Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

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: 10/22/2024 4:28:18 PM (Pacific)

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

Additional Contacts
none entered

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
UEI	HJS3TZHWWJX5
SAM Expires	7/8/2020

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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☑ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
□ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
□ Objective 3: Implement security protections commensurate with risk.
□ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.
☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local

governments within the state.

☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

☑ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

□ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.

□ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

□ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

□ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

☑ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

□ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

□ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

□ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

□ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.

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

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

□ Implement multi-factor authentication.

□ Implement enhanced logging.

□ Data encryption for data at rest and in transit.

□ End use of unsupported/end of life software and hardware that are accessible from the internet.

□ Prohibit use of known/fixed/default passwords and credentials.

□ Ensure the ability to reconstitute systems (backups).

☑ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.

□ Migration to the .gov internet domain.

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

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

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.

9. 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.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.

Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

The project location could be different than the sub-recipient address.
89101

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

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
☑ Yes
☐ No

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

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

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
☑ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
☐ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
☑ Equipment - Equipment, supplies, and systems that comply with relevant standards
☑ Training - Content and methods of delivery that comply with relevant training standards
☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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	1	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
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		1	**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	One-time purchase	System, Intrusion Detecti	05NP-00-IDPS

					covering 48,000 devices and Response covering 46,500 devices			
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 Master under 10k CPM will be needed for the deployment of UNLV and SNHD in Phase 1.	Recurring costs are shared by participating agencies	Hardware, Computer, Integ	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		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)	☑	Single Audit
Travel Policy	☑	Travel Policy

Payroll Policy	☑	Payroll Policy Payroll Narrative
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestones

Administrative Documents *

	Sole Source Request - Darktrace

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

Application ID: 483219

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	City of Las Vegas
	Project Name:	Dartrace - Unified View for Threat Intel - Southern Nevada Cyber Defense Project
	Project Funding Stream:	FY 2024 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 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

City of Reno

Backup and Disaster Recovery

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

$ 840,000.00 Requested

Submitted: 10/31/2024 4:34:40 PM (Pacific)

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

Additional Contacts
Phelpsa@reno.gov,hancockb@reno.gov,frandenc@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
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

☑ Objective 3: Implement security protections commensurate with risk.

☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

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

Projects may align with more than one element.

☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.

☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.

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

Implement a modern backup and disaster recovery platform following 3-2-1 priniciple that is backed by immutable storage to further increase resiliency and likelihood of recovery in the event of an attack. The current system in place is a legacy platform that does basic file and VM backups but is internet connected with no immutability or offsite/offiline replication. It was purchased with one time CARES Act funding and is approaching it End of Life and there is no funding currently to purchase a replacement.

The potential new platform would be using a best of breed vender and backup methodology not available with the current platform. This would consist on prem immutable storage appliances that don't allow data deletion even from administrator accounts. This protects against ransomware attackers that try to destroy backups first before launching the attack as even a super admin account is denied from removing the data. It would also support modern MFA/SAML protections for the admin console to make it significantly harder to tamper with settings and disrupt backup processes. The existing system is not compatible. Finally it will also support replication to any number of storage targets, our plan to do cloud off site as the long term archive repository so there is data in 2 locations in the event of disaster and the on prem appliances or data center is destroyed.

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

Having a modern immutable and replicated backup and recovery system is one of the only ways to successfully recover in the event of a cyber or infrastructure attack. A disaster recovery system that is able to survive an attack is the only way to restore government operations in a timely fashion if every other layer of cyber or phyiscal defenses failed. The risk of not having this is public safety, waste water treatment, and other critical government operations could have to revert to manual processes (if they exist) that could drag on for months or longer as evidenced by other CIty governments that have been attacked. This is major risk to life and financial stability of the organization.

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

3. Implementing a modern backup and disaster recovery systems prepares us for an attack ahead of time by ensuring the data protected and duplicated for restoration. It greatly speeds up the ability to respond and recover which plays into the resileance of the organization to continue operating.

5. Having a backup and recovery system that abides by the 3-2-1 principal is best practices in cybersecurity to ensure there are multiple redundancies to ensure recovery. Same if protecting the backup systems with strong MFA and immutability of the data incase all the other layers of defenses fall are best practice to have in place.

7. Being able to recover quickly after a disaster ensures continuty of operations able to continue or return to normal far quicker than if systems or data is unrecoverable.

10. The City hosts a number of major critical infrastructure systems that need to be operational 24/7 and available working with as little downtime as possible. These include all of the 911 CAD systems, Public Safety RMS and VPN platforms, GIS used for plowing routes priority based on Public Safety response times, Wastewater Treatment and SCADA/OT for tens of thousands of residents and many other daily functions.

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

☑ Implement multi-factor authentication.

☐ Implement enhanced logging.

☑ Data encryption for data at rest and in transit.

☐ End use of unsupported/end of life software and hardware that are accessible from the internet.

☐ Prohibit use of known/fixed/default passwords and credentials.

☑ Ensure the ability to reconstitute systems (backups).

☐ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.

☐ Migration to the .gov internet domain.

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

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

Project will be implemented by several IT staff along with vender implementation/PMs. The expected staff is Senior Server Admin and Server Admin as the primary individuals with the configuration and ongoing operation of backups, integrations with hypervisor integrations, and cloud replications. Senior Network and Network Analysts will be involved in the IP configuration and network connections for the equipment. Senior Cyber Security Analyst will be insuring critical security policies are in place for the platform like MFA/SAML, immutability, encryption of the back up data at rest, copies of data to multiple sites and/or cloud, and ongoing patches are applied.

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

A modern backup and disaster recovery system that has protections against all the modern threats faced by back up systems attackers and nation states do to destroy data before launching an attacks. It will be compatibile with most hypvervisor systems as more organizations move away from Broadcom. Backups will follow the 3-2-1 rule to ensure the ability to recovery is available in a worst case scenario. Other critical controls like MFA, multiple admin approvals for changes, encryption of the backups, etc are all implemented that do not exist with the current aging backup system.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.

Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89501

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

With a competitive process it is likely that the project costs would be lower. The identified dollar amount is to ensure a complete solution. The backup schedule and amount of data kept can be reduced to lower storage costs. Various software license lengths can be shortened if needed.

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

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

☐ Yes

☑ No

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

☑ Build

☐ Sustain

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

N/A

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

☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☐ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

☐ Training - Content and methods of delivery that comply with relevant training standards

☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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
Backup Solution	Complete backup solution, to be determined by RFP	1	$ 840,000.00	$ 840,000.00	The is the complete solution.	This funding is for a complete solution.	Applications SAAS,Hardwar	04AP-11-SAAS,04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	$ 840,000.00	$ 840,000.00				

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)	☑	Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll
Procurement Policy	☑	Procurement Policy Procurement Policy
Milestones download template	☑	Milestones

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

Application ID: 485243

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

Applicant Name	City of Reno
Project Name:	Backup and Disaster Recovery
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	RFP Creation and Release	2 Months
2	Contract Execution	1 Month
3	Project Implementation	2 Months
4	Project Closure	2 Weeks
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

City of Reno

Vulnerability Scanning and Remediation

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

$ 250,000.00 Requested

Submitted: 10/31/2024 4:33:53 PM (Pacific)

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

Additional Contacts
Hancockb@reno.gov,Phelpsa@reno.gov,frandenc@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
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☑ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☐ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.
☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☑ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
Purchase and implement a vulnerability scanning and monitoring platform for both On Prem devices like PCs and Servers as well as Cloud Posture management for SaaS applications. This will allow us to centrally track and prioritize CVE patching and remediation for 0/n days as well as implement hardening best practices to align with CIS benchmarks through GPOs, Intune, Entra, etc security policies.

Currently it's a disjoined manual process to track missing security patches and misconfigurations on thousands of machines. 1 platform only handles Microsoft patches, another handles ~50 3rd party patches and basic AD CIS benchmarking. Any applications outside of what those patching tools scan for there is no visability if present. Centralizing all of these data in a vulnerability platform will allow for a holistic view of overall organization risk and where limited man hours should spent to patch and harden systems.

5. How does your project align with the objective selected in Question 2?
Vulnerability scanners continuously scan devices and SaaS app configurations for missing patches, misconfigurations or exposed services. They typically produce an overall risk score that adjusts and tracks over time whether the overall risks and CVEs are increasing or decreasing. This allows us to continuously test and evaluate our environment and perform assessments on how closely we are meeting CIS Benchmarking.

6. How does your project align with the program element(s) selected in Question 3?
1. Vulnerability scanners typically offer the ability to scan entire IP ranges and discover all assets on the network that may be unknown or known to track and possibly enroll into management systems or block the rogue devices from accessing the network.

3. By patching and applying recommended security configurations we can greatly reduce the odds of an attack happening in the first place. If an attacker does manage to get a foothold, having no CVEs or strong default policies in place it becomes very difficult to move laterally and minimizes the blast radius.

4. A vulnerability scanner meets exactly what 4 is looking for.

5. Patching CVEs and implementing CIS Benchmark or vendor best practices enhance cybersecurity.

10. The scanner allows us to access and mitigate risks that are the most likely the easiest for an attacker to use to break in the environment.

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Project will be implemented by cybersecurity staff with assistance from vender. Agent based scanners will be deployed to all endpoints and servers. Unmanaged IP ranges will be input into the scanner VM to crawl IoT or network devices for risks. API key access to Office 365 or other SaaS apps will be created for the scanner to check settings and configurations.

9. Describe, in a few sentences, the desired outcome(s) of your project.
Deploy scanning agents to as many Windows PCs and Servers as possible along with most IP ranges for nonmanaged assests and SaaS environments where it makes sense. This will allow us to get a baseline of the entire network risk. Then over the course of the grant reporting period show continous reductions in Critical, High, Medium, etc risks with particular focus given on Critical and High findings. By the end we are hoping to have a significant reduction exploitable risks and also discover any unmanaged assests found during the scans and bring them into the Patching, Scanning, Intune, AV fold.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building’s structure, layout, systems, or critical aspects of a building’s safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89501

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

Additional money can be added to extend the length of time the licenses are valid for to allow for long tracking and reductions in risk through time. Or it could be used to apply towards additional modules around vulrenability management outside of the core endpoint and SaaS checks.

Money can be cut and would reduce the validity period the scanning agents are available for to track risks. Or modules for SaaS could be cut and only endpoint tracking implemented.

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

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

□ Yes

☑ No

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

☑ Build

□ Sustain

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

N/A

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

□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

□ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

□ Training - Content and methods of delivery that comply with relevant training standards

□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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**
Vulnerability and SaaS Scanner	Scanner to include VM for IoT and Network devices without agents, SaaS API connections to validate policy best practices or exposed data, web application vuln scanner, external exposure scanning, and benchmark compliance.	1	$ 250,000.00	$ 250,000.00		An additional funding request would submitted through the budget process.	Applications, SAAS	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	**$ 250,000.00**	**$ 250,000.00**				

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)	☑	Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy Purchasing
Milestones download template	☑	Milestones

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

Application ID: 485171

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

©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.

Logout | Browser

Applicant Name	City of Reno
Project Name:	Vulnerability Scanner
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	RFP Process	2 Months
2	Contract Execution	1 Month
3	Project Kickoff	1 Week
4	Project Implementation	3 Months
5	Project Closure	2 Weeks
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Clark County School District

Cybersecurity Digital Forensics

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

$ 581,875.00 Requested

Submitted: 10/28/2024 2:07:30 PM (Pacific)

Project Contact
Dirk Florence
floreda@nv.ccsd.net
Tel: 702-799-5272

Additional Contacts
blissm@nv.ccsd.net,abajiv@nv.ccsd.net,jonescv1@nv.ccsd.net

Clark County School District

5100 W Sahara Ave
Las Vegas, NV 89146
United States

Chief Information Officer
Marilyn Delmont
delmom@nv.ccsd.net

Telephone	702-799-2273
Fax	
Web	
UEI	SRBYQ7XFBYA6
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☑ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

- □ Objective 3: Implement security protections commensurate with risk.
- □ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

- ☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- ☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- ☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- □ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- □ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
- □ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- ☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- □ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
- ☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- □ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- □ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- □ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
- □ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- ☑ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- ☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
- □ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
Cybersecurity forensics tools in a K-12 school district can significantly improve cybersecurity by enabling the detection, investigation, and analysis of security incidents. These tools help IT staff identify the source and scope of cyberattacks, such as unauthorized access, data breaches, or malware infections. By collecting and analyzing digital evidence, forensics tools can reveal vulnerabilities in the network and user behavior, allowing the district to strengthen defenses, patch security gaps, and prevent future incidents. Additionally, these tools provide valuable insights for compliance with legal and regulatory requirements, ensuring a safer, more resilient digital environment for students and staff. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.

5. How does your project align with the objective selected in Question 2?
Cybersecurity forensics tools and services align closely with key security measures in a K-12 school district, such as managing, monitoring, and tracking information systems, applications, and user accounts. These tools provide real-time visibility into network activity, helping identify unusual or suspicious behavior that may indicate a security breach. By tracking user access patterns and system events, forensics tools ensure that incidents are quickly detected and thoroughly investigated, enabling the district to respond effectively. They also support the implementation of security protections that match the level of risk, as they provide critical insights into vulnerabilities and threats, allowing the district to adjust its defenses accordingly. This proactive approach ensures that cybersecurity measures are continually improved to safeguard student and staff data.

6. How does your project align with the program element(s) selected in Question 3?
Cyber forensics tools and services for K-12 school districts play a vital role in aligning with security measures like managing, monitoring, and tracking information systems, applications, and user accounts. By enabling continuous monitoring of network traffic, these tools help detect anomalies, intrusions, or potential threats in real time, allowing IT staff to respond swiftly to security incidents. Forensics tools enhance system resiliency by identifying vulnerabilities and weaknesses that can be addressed before they are exploited. They also ensure the district adopts and maintains best security practices by providing insights into security gaps and compliance requirements. Additionally, by mitigating cyber risks through detailed incident analysis and threat intelligence, these tools ensure the district has adequate access to cybersecurity services, helping to protect sensitive student and staff data while maintaining a secure digital learning environment. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Digital Forensics Supplier will build and test integrations with the District's enterprise email and productivity systems plus active directory data sources as detailed in the Digital Forensics Grant Milestones template. The team will then test the software configurations and integrations and move to implementation upon successful results. Accuracy and optimization of data will be constantly monitored. Standard procedures will be developed to address requests for information. Implementing cybersecurity forensic tools and services for a K-12 school district involves a strategic integration to enhance the district's ability to investigate and respond to cyber threats and information requests effectively. This approach will introduce comprehensive tools capable of monitoring and searching email communications, analyzing network traffic, and assessing various cybersecurity related environments. By integrating these tools, the district will streamline investigative processes, enabling rapid identification and response to security incidents while ensuring compliance with legal and regulatory standards. This implementation will not only bolster the District's overall cybersecurity posture but also provide a structured framework for ongoing training and support for staff, enabling the District to respond efficiently and appropriately to requests from law enforcement and other departments.

9. Describe, in a few sentences, the desired outcome(s) of your project.
Digital forensics managed services will provide for a timely, streamlined Security, Forensics Investigation workflow in support of Information Security and Forensics Discovery Identification, Preservation, Collection & Analysis and will be set up to allow CCSD to readily identify data sources for full indexing, analysis, forensic discovery, early case review, redaction, and export for across connected end points within the enterprise.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

- ☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses

the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89146

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

No

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

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

□ Yes

☑ No

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

☑ Build

□ Sustain

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

Not applicable.

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

□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

□ Training - Content and methods of delivery that comply with relevant training standards

□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Project Management	Blended average of Project management resources.	125	$ 175.00	$ 21,875.00	Oversight and project management to attain milestone delivery associated with: Deploy new capability to configure digital investigations software and integrations, develop standard operating procedure and documentation, coordinate with managed services provider throughout the project lifecycle as they provide support of Information Security and Forensics Discovery Identification, Preservation, Collection & Analysis and will be set up to allow CCSD to readily identify data sources for full indexing, analysis, forensic discovery, early case review, redaction, and export for across connected end points within the enterprise. Ensure continuity of communications to these key resources. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers.	Reduce funding to other district priorities.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
		125	$ 175.00	$ 21,875.00

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
Professional Services	Implementation services configuration and integrations for active directory and enterprise email and productivity systems.	1	$ 100,000.00	$ 100,000.00	Installation and configuration of digital forensics integrations.	This is a one time setup cost.	Consulting Services	21GN-00-CNST
Managed Services Subscription	3-year SaaS Infrastructure, Storage, Software and Managed Data Security and Forensic Services	1	$ 460,000.00	$ 460,000.00	Adopt and use best practices and methodologies to enhance cybersecurity through use of digital forensics.	Reduce funding to other district priorities.	Software as a Service	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		2	$ 560,000.00	$ 560,000.00				

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)	☑	Audit 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: 484819

©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.

	Applicant Name	Clark County School District
	Project Name:	Digital Forensics
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Software License Subscription	6 months after award
2	Configure and test initial system features	9 months after award
3	and to optimize the data	12 months after award
4	Deliver standard operating procedure and training documentation, and standardize requests for reporting for outputs on data management, workflow status, and security/forensic investigations	12 months after award
5	Managed services subscription transitions to Operations	36 months after award
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Clark County School District

DDOS Managed Services

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

$ 1,457,944.66 Requested

Submitted: 10/28/2024 2:03:21 PM (Pacific)

Project Contact
Dirk Florence
floreda@nv.ccsd.net
Tel: 702-799-5272

Additional Contacts
blissm@nv.ccsd.net,abajiv@nv.ccsd.net,jonescv1@nv.ccsd.net

Clark County School District

5100 W Sahara Ave
Las Vegas, NV 89146
United States

Chief Information Officer
Marilyn Delmont
delmom@nv.ccsd.net

Telephone	702-799-2273
Fax	
Web	
UEI	SRBYQ7XFBYA6
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
□ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
□ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

☑ Objective 3: Implement security protections commensurate with risk.
□ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

□ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
□ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
□ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
□ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
□ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
□ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
□ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
□ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
□ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
□ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
Implement managed services that monitor for Distributed Denial of Service (DDOS) attacks. A DDoS attack would target the District's internet connectivity and disrupt network services in an attempt to exhaust the network resources. The perpetrators behind these attacks flood the network with errant traffic, resulting in poor functionality or knocking it offline altogether. DDoS attacks are some of the most common cyberthreats. During a DDoS attack, a series of bots, or botnet, floods the network or service with HTTP requests and traffic. Essentially, multiple computers storm one computer during an attack, pushing out legitimate users. As a result, service can be delayed or otherwise disrupted for a length of time. DDoS attacks can exploit security vulnerabilities and target any endpoint that is reachable, publicly, through the internet. Denial-of-service attacks can last hours, or even days. These cyber assaults can also cause multiple disruptions throughout a singular attack. DDOS Managed services would benefit the 7.24% of rural communities where Clark County School District provides critical services.

There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.

5. How does your project align with the objective selected in Question 2?
Providing protection against a DDoS attack enables the District to provide increased security for our Internet connection. Modern classroom instruction is heavily reliant on Internet connectivity from student information systems to the actual instruction delivered to students, via an interactive flat panel or individual computing device. Using a managed service DDoS provider will allow the District to monitor and access the current threat landscape directed at the CCSD Internet. This can be done on a regular basis with an eye towards planning for future needs. A concentrated DDoS attack that negatively impacts the Internet bandwidth of the District would be very consequential. Depending on the length and timing of the attack, students would lose instruction time, attendance and grade recording would be delayed impacting state reporting requirements, and functions like school banking would be un available. In addition to school based issues, the district would also lose access to all it's cloud services and infrastructure including email and productivity systems, HR systems, and procurement systems.

6. How does your project align with the program element(s) selected in Question 3?
A DDoS protection service will monitor Internet traffic in and out of CCSD and abate it's systems against cyber-attacks. This monitoring and protection will enhance the resiliency of the District Internet connection in the face of ongoing cyber threats. The protection and mitigation efforts of DDoS protection will help ensure the District Intenret stays functional and helps ensure continuity of operations for instruction in CCSD. Keeping the District Intenret connection up ensures continuous data flow and communication to cloud resources and allows CCSD to update State Department of Education resources. The continual monitoring and response against a DDoS attack will allow the instant assessment of any new DDoS attacks and the mitigation to filter and provide clean internet traffic to the District. As all of CCSD uses the same internet circuits, this protection will not only be available for the urban center of Clark County, but also to all of the rural schools, about 7.24% of the schools in Clark County, throughout the roughly 8,000 square miles of Clark County that CCSD serves.

Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
A DDoS protection service provider will be chosen. After a provider is chosen network traffic from CCSD will be routed to the provider first before it gets to CCSD. The DDoS service provider would make these changes in conjunction with the Internet Service Provider. The DDoS provider would route the Internet traffic back to the CCSD Internet circuit and CCSD Internet staff would confirm they are receiving the traffic with no degradation or latency. Internal monitoring and routing would confirm all traffic is being received and properly routed. Once this is accomplished, the DDoS protection service provider will provide monitoring for the traffic that passes through their service and CCSD staff will monitor the Internet circuit to make sure all traffic is flowing as it should.

9. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome is for CCSD to have in place appropriate mitigation services against DDoS cyber attacks. The service would prevent a crippling DDoS attack against CCSD ensuring continuity of operations.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses

the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89146

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

Yes, we could reduce from three year to two years, although three years is optimal.

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

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

□ Yes

☑ No

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

☑ Build

□ Sustain

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

Not applicable.

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

□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

□ Training - Content and methods of delivery that comply with relevant training standards

□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Project Management	Blended average of Project management resources	250	$ 175.00	$ 43,750.00	Oversight and project management to attain milestone delivery associated with: Deploy new capability to monitor, audit, track network traffic and ensure continuity of communications to these key resources. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers.	Reduce funding to other district priorities.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

		$	$
		$	$
		$	$
	250	**$ 175.00**	**$ 43,750.00**

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
Professional Services	Professional Services to implement DDOS	1	$ 14,588.82	$ 14,588.82	Installation and configuration	This is a one time set up cost.	Consulting Services	21GN-00-CNST
Cloud Security	DDoS Protection for Networks - On-Demand Bandwidth	36	$ 38,877.94	$ 1,399,605.84	Deploy new capability to monitor, audit, track network traffic and ensure continuity of communications to these key resources. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers.	Recurring managed services is 38,877.94 monthly would need to be available in the sustainability budget.	Asset Management	05SM-00-ITAM
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		37	**$ 53,466.76**	**$ 1,414,194.66**				

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)	☑	Audit 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: 484545

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

Applicant Name	Clark County School District
Project Name:	DDoS Managed Services
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	Purchase Software as a Service	4 months after award
2	Configure and test network traffic routing	6 months after award
3	Deploy Managed Services	7 months after award
4	Complete Managed Services	36 months after award
5		
6		
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 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Clark County School District

Identity Management Access Governance

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

$ 524,447.00 Requested

Submitted: 10/28/2024 2:08:48 PM (Pacific)

Project Contact
Dirk Florence
floreda@nv.ccsd.net
Tel: 702-799-5272

Additional Contacts
blissm@nv.ccsd.net,abajiv@nv.ccsd.net,jonescv1@nv.ccsd.net

Clark County School District

5100 W Sahara Ave
Las Vegas, NV 89146
United States

Chief Information Officer
Marilyn Delmont
delmom@nv.ccsd.net

Telephone	702-799-2273
Fax	
Web	
UEI	SRBYQ7XFBYA6
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☑ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

□ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
□ Objective 3: Implement security protections commensurate with risk.
□ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☑ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
□ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
□ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
□ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
□ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
□ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☑ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
□ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
□ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
IAM Access Governance provides the following: 1) Visibility and Control Over Access including comprehensive visibility into who has access to what across our enterprise, spanning both cloud and on-premises environments. 2) Dynamic Access Control which enhances various access control models like attribute-based, policy-based, and role-based access control. These models allow for more granular and context-aware permissions, reducing the risk of unauthorized access by ensuring that access rights are aligned with business needs and security policies. 3) Access Reviews and Analytics insights-based access reviews, where access rights are periodically reviewed and certified by managers or system owners. This process, driven by analytics, helps in identifying anomalies or excessive permissions, which could be security risks. Currently, this is a manual process for our staff that requires heavy overhead. This will simplify the process, giving business owners, auditors, and leadership access to reviews on demand. 4) Policy Compliance by integrating with our current provisioning platform and sources of truth, it ensures that access policies are enforced consistently across the enterprise and helps in maintaining compliance with regulatory requirements by managing access in compliance with laws like FERPA, HIPAA, or internal policies. 5) Risk Mitigation Through Intelligence using machine learning and advanced analytics, the product can predict and mitigate risks by identifying patterns that might indicate potential security issues, such as dormant accounts with high privileges or unusual access patterns. 6) The intuitive user interface of Access Governance not only aids in better user management but also encourages adoption by making governance tasks less cumbersome. This user-centric approach indirectly improves security by ensuring that governance processes are followed more diligently. Access Governance would help reduce the attack surface by ensuring that access is least privileged, appropriate, and compliant, thereby significantly improving the District's cybersecurity posture. This product aligns with best practices in cybersecurity by automating, monitoring, and controlling access rights, which are fundamental in preventing unauthorized access and data breaches. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.

5. How does your project align with the objective selected in Question 2?
Identity Access Governance (IAG) establishes appropriate governance structures by managing identities and access rights, ensuring both compliance with regulatory standards and robust security measures. IAG syncs with the District’s Human Resources system (our source of truth) to create a unified identity profile, ensuring that all systems operate with accurate and consistent identity data. This synchronization pulls data from authoritative sources and correlates this data to fit into the governance framework. IAG supports our current models, including Role-Based Access Control (RBAC), where permissions are assigned based on roles, simplifying management for large user groups, and Attribute-Based Access Control (ABAC), allowing for more granular, dynamic control based on user or resource attributes, such as Student Information System. Policy-Based Access Control (PBAC), ensures that access rights can be adjusted dynamically according to predefined rules or changes in context, thereby aligning with evolving business needs or security policies. The system automates access reviews, triggering them based on events or schedules, ensuring that access rights are always appropriate for current roles and responsibilities. This extends to managing the entire identity lifecycle, from onboarding through role changes to offboarding, which is crucial for maintaining access integrity as personnel changes occur within the organization. By providing a single point of control for access governance, it reduces the risks associated with decentralized or misconfigured access settings, streamlines auditing processes, and facilitates compliance by ensuring visibility into who has access to what resources across the organization. This also reduces the overhead of managing access across multiple disparate systems which is a current challenge for the District. IAG's integration capabilities allow it to interface with our current provisioning system and third-party systems and applications. It ensures that governance policies are enforced uniformly across various applications and platforms. IAG incorporates analytics, providing insights for identifying potential risks, understanding access trends, and refining governance policies based on actual usage and threat data. The analytics support a proactive approach to security and compliance management, allowing the District to adapt our governance strategies dynamically. IAG provides a framework that addresses security and compliance, dynamically adapting to the changing landscape of cybersecurity threats and regulatory requirements. The comprehensive governance model ensures that access rights are appropriate, justified, and in line with the principle of least privilege, helping safeguarding our data integrity, enhancing operational efficiency, and maintaining a compliant posture, all of which are critical.

6. How does your project align with the program element(s) selected in Question 3?
Identity Access Governance (IAG) functions as an automated system for managing, monitoring, and tracking access to IT systems and user accounts. It aligns with operational requirements by:
Access Control: Implementing and maintaining access permissions aligned with user roles, dynamically adjusting as roles change or terminate. Additionaly adding the ability for electronic and automated account approval workflows. Network Surveillance: Utilizing logging mechanisms to monitor, audit, and track network activities for compliance and security purposes. Vulnerability Reduction: By enforcing least privilege access, IAG minimizes exposure to cybersecurity threats by reducing potential attack vectors within the IT infrastructure. Through continuous alignment with organizational policies and regulatory standards, IAG supports operational best practices, ensuring minimal disruption and rapid recovery in the event of system failures or breaches. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

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

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

Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
IAM Access Governance is a cloud native service thus eliminating the need for hardware or software setup. We will utilize our IAM supplier partner for configuration of the product and integration into our current provisioning systems. The team has intimate knowledge of our data flow architecture allowing us to configure and deploy the Active Directory and Enterprise Email and Productivity workspace data connectors fairly quickly. After those connectors are complete, the supplier will help us modify our current Student Information System connector to allow a two-way reconciliation.

The supplier team will work with the CCSD Identity and Access Management team to implement, configure, and train the development and support staff on the technical specification of the product.

The project will be managed by a CCSD project manager.

9. Describe, in a few sentences, the desired outcome(s) of your project.
IAM Access Governance will deliver outcomes centered around enhancing security, compliance, and operational efficiency in the District. By automating access reviews, managing user lifecycle, and providing centralized governance, it will reduce risk, support compliance with regulatory standards, and streamline operations. This product offers insights for better risk management, supports scalability through integration with various systems, and improves overall user experience by simplifying governance processes. Ultimately, it will help us maintain a secure, compliant, and efficient environment, adaptable to changing business needs while reducing staff overhead costs.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)
□ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89146

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
No.

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
□ Yes
☑ No

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

16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project.
Not applicable.

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
☑ Equipment - Equipment, supplies, and systems that comply with relevant standards
□ Training - Content and methods of delivery that comply with relevant training standards
□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Project Management	Blended average of Project Management Resources.	125	$ 175.00	$ 21,875.00	Oversight and project management to attain milestone delivery associated with: Adopt and use best practices and methodologies to enhance cybersecurity – Identity Management Access Governance.	Reduce funding to other district priorities.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		125	**$ 175.00**	**$ 21,875.00**		

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
Professional Services	Configuration to integrate with Student Information System, Active Directory and Enterprise Email and Productivity systems. Additionally, Student Information Systems requires additional development needed for the bi-directional functionality required for access reviews.	1	$ 300,000.00	$ 300,000.00	Installation and configuration three major systems to utilize IAM Governance.	This is a one time set up cost.	Consulting Services	21GN-00-CNST
Software Subscription	Monthly subscription fee	36	$ 5,627.00	$ 202,572.00	Adopt and use best practices and methodologies to enhance Identity Management by employing access governance.	Reduce funding to other district priorities.	Software as a Service	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				

	37	$ 305,627.00	$ 502,572.00

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)	☑	Audit 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: 484825

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	Clark County School District
	Project Name:	Access Governance
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Secure licensing & services	90 days after award
2	Product configuration	120 days after award
3	Config, test, roll out first 2 connectors (email, Identity Management)	165 days after award
4	Config, test, roll out 3rd connector (SIS)	240 days after award
5	Implement, configure and train development and support staff	240 days after award
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Clark County School District

Multi-Factor Authentication for Student Education Systems

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

$ 764,075.00 Requested

Submitted: 10/28/2024 2:05:46 PM (Pacific)

Project Contact
Dirk Florence
floreda@nv.ccsd.net
Tel: 702-799-5272

Additional Contacts
blissm@nv.ccsd.net,abajiv@nv.ccsd.net,jonescv1@nv.ccsd.net

Clark County School District

5100 W Sahara Ave
Las Vegas, NV 89146
United States

Chief Information Officer
Marilyn Delmont
delmom@nv.ccsd.net

Telephone 702-799-2273
Fax
Web
UEI SRBYQ7XFBYA6
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

☑ Objective 3: Implement security protections commensurate with risk.
□ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
□ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
□ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
□ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
□ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
□ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
□ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
□ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
□ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
□ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
□ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
□ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
□ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
Multifactor authentication (MFA) for students in a K-12 school district significantly enhances cybersecurity by adding an extra layer of protection beyond just a password. Given the potential vulnerabilities in student accounts, such as weak passwords or phishing attacks, MFA helps ensure that even if a password is compromised, unauthorized access is prevented by requiring a second factor, like a one-time code or biometric verification. This added security reduces the risk of data breaches, unauthorized access to sensitive information, and disruptions to learning systems, creating a safer digital environment for students and staff. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

5. How does your project align with the objective selected in Question 2?
Implementing multifactor authentication (MFA) for K-12 students aligns with the principle of applying security measures commensurate with risk by addressing the specific vulnerabilities associated with student accounts and the digital systems they access. In a school environment, student accounts are prime targets for cyberattacks, including phishing and credential theft. MFA provides a higher level of security proportional to these risks, ensuring that even if a password is compromised, additional authentication layers protect sensitive student and school data. By aligning security controls, like MFA, with the actual risk posed to the school’s digital infrastructure, administrators can create a balanced and effective cybersecurity strategy without overburdening students. Given that the District stores and manages critical information that falls under PII (Personally Identifiable Information) FERPA and Nevada’s NRS 603A, MFA ensures that security measures are proportional to the level of risk. By introducing MFA, we aim to significantly strengthen the security of user accounts by adding an additional layer of protection beyond passwords, which can be easily compromised through phishing or other social engineering attacks.

There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.

6. How does your project align with the program element(s) selected in Question 3?
Adopting Best Practices to Enhance Cybersecurity - Implementing MFA is a proven best practice in cybersecurity and aligns with industry standards such as NIST and CISA, ensuring our district adopts well-established methods to protect critical data. Mitigating Cybersecurity Risks to Critical Infrastructure - The Student education systems platform is essential to our district's daily operations, storing student data, personally identifiable information (PII), and educational records—all classified as high-risk assets. A compromise to this system would disrupt educational services and lead to violations of FERPA and Nevada’s NRS 603A. MFA effectively mitigates threats like phishing and credential theft, as it blocks 99% of phishing attacks, ensuring that even if passwords are compromised, unauthorized access is prevented. This project safeguards a critical part of our infrastructure, minimizing the impact of security breaches on information systems. Ensuring Access and Participation in Cybersecurity Services for Rural Areas - Our project includes rural areas, ensuring equitable access to cybersecurity protections. Approximately 7.24% of the Clark County School District serves rural communities, and by extending MFA to these areas, we provide enhanced security protections that might otherwise be harder to access. This ensures that rural students and staff benefit from the same high-level protections as the rest of the district, securing their access to educational resources while maintaining the integrity of digital learning tools. This MFA project supports the program elements by adopting best practices, mitigating risks to critical infrastructure, and ensuring that rural areas have equal access to cybersecurity services. This implementation will strengthen the district’s security posture and help create a secure, inclusive, and resilient digital environment for all students and staff.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Configure and test MFA (multi-factor authentication for students) features, develop communication plan for rollout to students and educational staff as required for training, deploy MFA, support MFA in production.

9. Describe, in a few sentences, the desired outcome(s) of your project.
Implementing multifactor authentication (MFA) in K-12 instructional applications enhances the security and privacy of student data by requiring additional verification steps beyond just passwords. The desired outcomes include reducing the risk of unauthorized access, protecting sensitive student information, and ensuring compliance with PII, FERPA, Nevada’s NRS 603A, and other privacy regulations. MFA also eliminates vulnerabilities from default or weak passwords, further strengthening the district's cybersecurity defenses. By implementing these protections, we are promoting a safer online learning environment, safeguarding digital resources from potential cyber threats, and ensuring the continuity of critical educational services. Additionally, this project ensures that rural communities, which make up 7.24% of the district, have equal access to these enhanced cybersecurity protections, helping create an inclusive and secure digital experience for all users.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building’s structure, layout, systems, or critical aspects of a building’s safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89146

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

No

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

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

☐ Yes

☑ No

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

☑ Build

☐ Sustain

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

Not applicable.

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

☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

☐ Training - Content and methods of delivery that comply with relevant training standards

☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Project Management	Blended average of Project management resources.	125	$ 175.00	$ 21,875.00	Oversight and project management to attain milestone delivery associated with: Adopt and use best practices and methodologies to enhance cybersecurity – Multifactor Authentication for student educational systems.	Reduce funding to other district priorities.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$
			$	$
			$	$
		125	**$ 175.00**	**$ 21,875.00**

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	Multifactor Authentication for student educational systems annual license subscription - approx 350,000 accounts	3	$ 242,400.00	$ 727,200.00	Adopt and use best practices and methodologies to enhance cybersecurity – Multi Factor Authentication.	Reduce funding to other district priorities.	Software as a Service	04AP-11-SAAS
Professional Services	Implementation Services	1	$ 15,000.00	$ 15,000.00	Installation and configuration of MFA for student technology.	This is a one time setup cost.	Consutling Services	21GN-00-CNST
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		4	**$ 257,400.00**	**$ 742,200.00**				

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)	☑	Audit 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: 484816

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

©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.

Logout | Browser

	Applicant Name	Clark County School District
	Project Name:	MFA for Student Education Systems
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Software License Subscription	4 months after award
2	Configure and test MFA features	6 months after award
3	Develop Communication & Training Plans	8 months after award
4	Deploy MFA features	9 months after award
5	Software License subscription transitions to Operations	36 months after award
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ *and*

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Clark County School District

Update Cybersecurity Incident Response and Tabletop Exercise

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

$ 94,000.00 Requested

Submitted: 10/28/2024 2:10:04 PM (Pacific)

Project Contact
Dirk Florence
floreda@nv.ccsd.net
Tel: 702-799-5272

Additional Contacts
blissm@nv.ccsd.net,abajiv@nv.ccsd.net,jonescv1@nv.ccsd.net

Clark County School District

5100 W Sahara Ave
Las Vegas, NV 89146
United States

Chief Information Officer
Marilyn Delmont
delmom@nv.ccsd.net

Telephone	702-799-2273
Fax	
Web	
UEI	SRBYQ7XFBYA6
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

1. Is this agency considered a rural area (an area encompassing a population of less than 50,000 people)?

If your agency is not considered a rural area, but your project will support rural communities, select "No" and indicate in your narrative what percentage of your project will directly benefit rural Nevadans.

☐ Yes
☑ No

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☑ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☐ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

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

Projects may align with more than one element.

☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☐ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.

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

An incident response (IR) plan is a set of tools and procedures that CCSD can use to identify, contain, and recover from cybersecurity threats. It is designed to help CCSD personnel respond quickly and uniformly against any type of external threat. An IR Standard will define the specific requirements CCSD will implement to ensure a sound IR plan and process. The IR Standard will define key roles and responsibilities for IR planning and response. Tabletop exercises will test and validate the IR team's ability to utilize and leverage the developed process and playbooks. Technology & Information Systems Services (TISS) created an IR plan in early 2023 prior to CCSD's October 2023 cybersecurity incident. We would like to update our Incident Response Planning based on lessons learned and other 2024 projects where we have created focused IR Plans for Distributed IT (DIT) Teams (IT groups outside of Technology and Information Services Division). Additionally, we also want to improve our communications with the schools during potential incidents. By applying lessons learned, we could greatly enhance our incident response planning and recovery. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.

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

Security Vendor will work with Clark County School District staff to update incident response plans, create additional departmental work aids, and facilitate a tailored tabletop exercise focused on the entire District and how to be prepared and respond to disruptions due to cyberattack. The concentration is on critical services to ensure continuity of operations and appropriate communication to relevant leadership district wide during potential incidents. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

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

Cybersecurity Incident Response Planning and Tabletop Exercises are crucial for strengthening the resilience of information systems by simulating real-world scenarios to identify vulnerabilities and improve recovery strategies. These exercises ensure continuity of operations by preparing teams to respond effectively to cyber incidents, minimizing downtime and preserving critical functions. They also reinforce the continuity of communication and data networks by testing protocols that maintain secure channels during disruptions. Additionally, tabletop exercises help assess cyber threats and risks by evaluating the organization's preparedness, response capabilities, and areas for improvement, enabling proactive risk mitigation. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.

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

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

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

Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Security vendor and CCSD Team would review lessons learned from 2023 cybersecurity incident plus DIT projects and then conduct a gap analysis of current TISS IR plan. Interviews of incident response leaders and participants would be conducted. IR plan documents and tools would be updated. An on-site table top workshop would be held to include TISS, DIT and school leaders that could be impacted by a possible incident. The real world example would allow stakeholders to react and learn from the elements of a potential attack. An after action report would be produced to document the table top workshop and final documents and reports for incident response planning would be delivered.

9. Describe, in a few sentences, the desired outcome(s) of your project.
A well prepared and exercised plan minimizes the potential impacts of a security incident and helps enable a return to normal operations as soon as possible. The Incident Response Plan describes the overall CCSD approach to identifying and managing security incidents, including the roles and responsibilities of key personnel and important communication protocols. More detailed guidance on the execution of IR processes and procedures are outlined in the CCSD IR Procedure document and IR Playbooks. The NIST SP 800-61 Rev. 2 Guide advises that, once your plan is approved, you should implement the plan. Importantly, you should review it at least once a year, if not more often, to ensure your organization is following the roadmap for maturing the capability and fulfilling incident response goals.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)
☐ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89146

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
No

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
☐ Yes
☑ No

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

16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project.
FY 2022 - Incident Response Planning and Tabletop Exercise

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
☑ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
☐ Equipment - Equipment, supplies, and systems that comply with relevant standards
☐ Training - Content and methods of delivery that comply with relevant training standards
☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Professional Services	Incident response plan and tabletop exercise.	1	80,000.00	$ 80,000.00	Enhance the preparation, response, and resilience of critical systems. Ensure the continuity of operations.	Reduce funding to other district priorities.
				$		
				$		
				$		
				$		

				$
				$
				$
				$
				$
				$
				$
				$
				$
		1	**80,000.00**	**$ 80,000.00**

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?
Project Management	Blended average of Project management resources	80	$ 175.00	$ 14,000.00	Oversight and project management to attain milestone delivery associated with: the preparation, response, and resilience of critical systems. Ensure the continuity of operations.	Reduce funding to other district priorities.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		80	**$ 175.00**	**$ 14,000.00**		

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
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		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)	☑	Audit 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: 484954

©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.

	Applicant Name	Clark County School District
	Project Name:	Cybersecurity IR Plan Update
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Procurement of Services	90 days after award
2	Gap analysis	120 days after award
3	Interviews	150 days after award
4	Update IR plan documents	180 days after award
5	Onsite workshop and final reports	210 days after award
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Clark County Water Reclamation District

Firewall Improvement for Clark County Water Reclamation District

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

$ 33,289.48 Requested

Submitted: 10/29/2024 2:07:57 PM (Pacific)

Project Contact
Angeline Szymanski
aszymanski@cleanwaterteam.com
Tel: 702-668-8066

Additional Contacts
none entered

Clark County Water Reclamation District

5857 E Flamingo Rd
Las Vegas, NV 89122
United States

Chief Financial Officer
Charles OCansey
cocansey@cleanwaterteam.com

Telephone	7026688066
Fax	
Web	www. cleanwaterteam.com
UEI	MSTUUDL7AEG5
SAM Expires	3/18/2025

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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

☑ Objective 3: Implement security protections commensurate with risk.

☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

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

Projects may align with more than one element.

☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☐ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.

☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

☐ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.

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

To enhance our organization's cybersecurity infrastructure, we seek grant funding to procure a new, advanced firewall. The firewall would be utilized at our primary data center, which supports critical components of the wastewater agency's operations. The firewall currently in use will be repurposed at our disaster recovery site, allowing the District to improve resilience to cybersecurity attacks and avoid operational interruptions.

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

This upgrade is critical for bolstering our primary internet firewall's capabilities, ensuring strong protection against evolving cyber threats, which aligns with Objective 3: Implement security protections commensurate with risk. The existing firewall will be repurposed to our backup data center, significantly strengthening our disaster recovery and business continuity plans. By implementing this dual-layered security approach, we will safeguard sensitive data, maintain uninterrupted operations during unforeseen events, and comply with industry standards for data protection. This strategic investment will not only mitigate risks but also enhance our overall resilience and operational integrity.

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

A firewall ensures network traffic is monitored, audited and tracks activity to ensure cyber intrusions are not occurring at the District, which serves unincorporated Clark County as a wastewater agency (Element 2). The new firewall will enhance and provide resiliency to block intrusions on the District network, and support similar protection on the District's disaster recovery site. This ensures the local government agency can continue its operations and mission of returning reclaimed water to Lake Mead (Element 3 and 7).

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

☐ Implement multi-factor authentication.

☑ Implement enhanced logging.

☑ Data encryption for data at rest and in transit.

☐ End use of unsupported/end of life software and hardware that are accessible from the internet.

☐ Prohibit use of known/fixed/default passwords and credentials.

☑ Ensure the ability to reconstitute systems (backups).

☐ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.

☐ Migration to the .gov internet domain.

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

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

Staff will install and configure the security appliance cluster with support from vendor to ensure the appliance is properly configured to the District's network, in alignment with industry best practices for cybersecurity.

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

Upgrading to a new, advanced firewall will significantly enhance our overall security posture in several ways:

1. Improved Threat Detection and Prevention: The firewall will include advanced features such as deep packet inspection, intrusion prevention systems (IPS), and real-time threat intelligence, to detect and block sophisticated cyber threats more rapidly.
2. Enhanced Network Performance: With better processing power and faster throughput, the new firewall will ensure that legitimate traffic flows smoothly while malicious activities are swiftly intercepted, reducing the risk of network slowdowns or breaches.
3. Increased Redundancy and Reliability: By repurposing the existing firewall to our backup data center, we create a robust failover mechanism. This ensures that in the event of a primary firewall failure, our backup can seamlessly take over, maintaining continuous protection and minimizing downtime.
4. Compliance and Risk Management: The upgrade will help us comply with industry standards and mandated requirements for data protection, reducing risk and enhancing our organizations security posture.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.

Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the

Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89122

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

Project is not scalable as this will support redundancy of the disaster recovery network, and is the minimum requirement to support firewall needs on the District primary network.

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

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

☐ Yes

☑ No

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

☑ Build

☐ Sustain

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

N/A

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

☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☐ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

☐ Training - Content and methods of delivery that comply with relevant training standards

☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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	Security Appliance Cluster	2	$ 16,494.28	$ 32,988.56	Prevents intrusions and allows monitoring of a critical infrastructure network.	One-time expense; products equipment replacement would be added to budget at the end of the product's useful life.	Firewall, Network	05NP-00-FWAL
Transceiver Module	Transceiver Module	4	$ 75.23	$ 300.92	Supports the receipt and transmission of data for the firewall. The above item would not work without this module.	One-time expense; products equipment replacement would be added to budget at the end of the product's useful life.	Components, Networking	04HW-03-NETD
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		6	$ 16,569.51	$ 33,289.48				

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 CAFR (2024 Not Available Until After Deadline) DRAFT 2024 ACFR
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Time and Attendance
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestone Schedule

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

Application ID: 484971

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	CLARK COUNTY WATER RECLAMATION DISTRICT
	Project Name:	Firewall Improvement for Clark County Water Reclamation
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	PROCUREMENT/PURCHASE	2/1/2025
2	INSTALLATION	4/1/2025
3	CONFIGURATION	5/1/2025
4	COMPLETE/PROJECT CLOSEOUT	6/30/2025
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

LVMPD

LVMPD Cyber Security Project FFY24

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

$ 148,000.00 Requested

Submitted: 10/28/2024 2:18:39 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	
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☑ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.
☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☑ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☑ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☑ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☑ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☑ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
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 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 KnownBe4 or something similar, which 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?
This 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. Does your project address any of the following Key Cybersecurity Best Practices?
☐ Implement multi-factor authentication.
☐ Implement enhanced logging.
☐ Data encryption for data at rest and in transit.
☐ End use of unsupported/end of life software and hardware that are accessible from the internet.
☑ Prohibit use of known/fixed/default passwords and credentials.
☐ Ensure the ability to reconstitute systems (backups).
☑ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.
☐ Migration to the .gov internet domain.

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
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.

9. 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.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building’s structure, layout, systems, or critical aspects of a building’s safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses

the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89106

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

No, to reduce this grant would pull capability away.

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

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

□ Yes

☑ No

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

□ Build

☑ Sustain

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

Currently this project is funded by UASI. If awarded FFY23 SLCGP funds, these would take the place of UASI FFY24 approved project. If both FFY23 and FFY24 SLCGP funds are awarded, the FFY24 SLCGP funds would sustain the FFY23 SLCGP project.

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

□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

□ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

□ Training - Content and methods of delivery that comply with relevant training standards

□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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
KnownBe4 Security Awareness Training	KnownBe4 Security Awareness Training	1	$ 62,000.00	$ 62,000.00	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	$ 28,000.00	$ 28,000.00	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	$ 148,000.00	$ 148,000.00

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	☑	LVMPD Cyber FFY24 SLCGP Milestones

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

Application ID: 485102

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

Applicant Name	LVMPD - Diana Clarkson
Project Name:	LVMPD Cyber Program - FY24
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
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		

*Please add additional rows as necessary for your project

Milestones will be expanded if project is awarded - AJ 11/06/24

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Nevada Department of Agriculture

Single Sign-on Implementation

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

$ 39,600.00 Requested

Submitted: 11/1/2024 6:03:37 PM (Pacific)

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

Additional Contacts
none entered

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	
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

1. Is this agency considered a rural area (an area encompassing a population of less than 50,000 people)?

If your agency is not considered a rural area, but your project will support rural communities, select "No" and indicate in your narrative what percentage of your project will directly benefit rural Nevadans.

☐ Yes
☑ No

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☑ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

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

Projects may align with more than one element.

☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☐ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☑ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☐ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.

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

The Nevada Department of Agriculture (NDA) plans to upgrade its current login system to the Nevada State Digital Identity System (NVDIS), a secure, unified login solution used by Nevada state agencies. This upgrade will make logging in safer and easier for users while ensuring stronger security for NDA's online applications.

Project Goals:

Migrate User Accounts: Transfer all existing user accounts to the new system, ensuring secure, continuous access.
Connect NDA Applications to NVDIS: Reconfigure NDA applications to work with NVDIS, so users only need a single login.
Add Extra Security Steps: Implement multi-step login, requiring a second form of verification for added security.
Ensure User Permissions: Configure the system to provide access based on each user's specific role, ensuring only authorized access to sensitive information.

Why This Project is Needed: Our current login system relies on outdated software, which increases security risks. The transition to NVDIS offers a reliable, state-supported solution that is both secure and flexible to meet NDA's needs.

How This Project Enhances Security:

Stronger Authentication: Extra verification steps will help ensure only the right users access sensitive applications.
Reduced Risk: Moving away from unsupported software reduces the risk of security breaches.
Centralized Monitoring: With NVDIS, NDA can more easily monitor and manage user access.
Increased Public Trust: A .gov domain provides users a trustworthy entry point for secure access to NDA's online services.

This project will improve NDA's security and create a safer, more user-friendly login experience, protecting both user data and NDA's digital resources.

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

Our project aligns closely with Objective 3: Implement security protections commensurate with risk by directly addressing critical security vulnerabilities and enhancing protections through a secure, modernized authentication framework.

The current login system relies on .NET Core 3.1, which reached its end-of-life on December 13, 2022, meaning it no longer receives security updates. This project mitigates the security risks associated with unsupported software by transitioning to the Nevada State Digital Identity System (NVDIS). Through this upgrade, we implement multi-factor authentication for stronger user verification, significantly reducing the risk of unauthorized access.

Additionally, NVDIS enables centralized management and monitoring of user access, allowing NDA to detect and respond swiftly to any security incidents. This modernization aligns with state cybersecurity standards, ensuring NDA's practices remain resilient against evolving threats. By using a .gov domain for login, NDA will also improve public trust, reinforcing the safety and reliability of its online services.

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

Our project aligns closely with the selected program elements by enhancing user account management, implementing cybersecurity best practices, and promoting a secure, trusted user experience.

Program Element 1: Managing, Monitoring, and Tracking Information Systems
By migrating from .NET Core 3.1, which reached end-of-life on December 13, 2022, to the Nevada State Digital Identity System (NVDIS), we are addressing the risks associated with outdated technology. NVDIS provides real-time monitoring and tracking capabilities, enabling NDA to manage user accounts, monitor access, and respond promptly to suspicious activity. This integration strengthens control over user access across NDA applications, ensuring secure, centralized management of user identities.

Program Element 5: Adopting Best Practices in Cybersecurity
The transition to NVDIS brings NDA in line with cybersecurity best practices, such as implementing multi-factor authentication and supporting secure identity protocols. This upgrade allows us to leverage modern security features to improve authentication and authorization, aligning with widely accepted standards for safeguarding digital identities and reducing unauthorized access risks.

Program Element 6: Promoting Secure and Trustworthy Online Services
By modernizing our existing SSO on a .gov domain through NVDIS, we maintain a secure and recognizable access point for NDA's online services. This enhances public trust and provides users with a consistent, reliable, and protected experience, reinforcing NDA's commitment to high security standards.

Overall, this project reduces vulnerabilities, strengthens access control, and ensures a trusted online environment for all users accessing NDA services.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
1. Project Planning and Analysis
Lead: Contracted Vendor, with input from NDA and OCIO
Activities: The vendor will begin by analyzing NDA's current SSO environment and determining the specific requirements for migrating user accounts and integrating NDA applications with NVDIS. The planning phase will include defining key project milestones, timelines, and a detailed migration strategy.
Outcome: Comprehensive project plan, including migration scripts, requirements for application updates, and a strategy for secure user account migration.

2. Preparation and Configuration of Environments
Lead: Contracted Vendor, supported by OCIO and NDA IT Staff
Activities: OCIO will configure the necessary Azure Entra ID and Azure AD B2C environments, including test, development, and production environments, to support the migration. The vendor will assist with setting up these environments, establishing connectivity with NDA's applications, and configuring authentication flows.
Outcome: Configured environments in Azure, ready for integration and testing with NDA's applications.

3. Migration of User Accounts
Lead: Contracted Vendor, with validation support from NDA IT Staff
Activities: The vendor will prepare scripts and tools to migrate user accounts from NDA's existing .NET Core 3.1 SSO to Azure Entra ID/B2C. NDA will provide access to user account data, which the vendor will use to test and validate the migration process in a development environment. Once tested, the migration will proceed in the production environment.
Outcome: Successful migration of all user accounts to the new NVDIS system, verified through validation and testing by NDA.

4. Integration of NDA Applications with NVDIS
Lead: NDA IT Staff, with support from Contracted Vendor
Activities: The NDA IT team will modify and reconfigure existing applications to authenticate users through NVDIS. This involves updating each application's login protocols to redirect users to Azure Entra ID/B2C for authentication, handle returned security tokens, and map them to existing NDA user profiles. The vendor will provide guidance, troubleshooting, and coding support as needed.
Outcome: NDA applications are fully integrated with NVDIS, enabling users to authenticate through the new, secure identity system.

5. Testing and Validation
Lead: NDA IT Staff, with oversight from Contracted Vendor and OCIO
Activities: In collaboration with OCIO, NDA staff will conduct user acceptance testing in development and quality assurance environments to verify the functionality and security of the integration. Tests will cover account login, multi-factor authentication, and the handling of user roles and permissions.
Outcome: Verified integration and functionality of NVDIS with NDA applications, ensuring smooth and secure user authentication.

6. Defect Remediation and Adjustments
Lead: Contracted Vendor, with involvement from NDA IT Staff
Activities: Any defects or integration issues identified duri

9. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcomes of this project are to provide a secure, modern single sign-on (SSO) solution that protects NDA's applications and user data. By transitioning to the Nevada State Digital Identity System (NVDIS), NDA will enhance user authentication with multi-factor security, streamline account management across applications, and reduce risks associated with outdated software. The project aims to ensure reliable, secure access for users while aligning with state cybersecurity standards and best practices.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-

ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
Yes, this project is scalable, allowing for expansion or reduction as needed.

Expansion Options: The project can extend to integrate additional NDA or state agency applications, moving toward a unified state identity system where a single login provides access to all state services. Enhanced user profile management could also be added, allowing more refined control over permissions.

Reduction Options: To conserve resources, only high-priority NDA applications can be integrated initially, with other applications added in phases. Similarly, user migration could start with active accounts, migrating less active accounts later.

This flexibility ensures the project aligns with NDA’s resources while laying groundwork for a comprehensive state-wide identity management system.

14. Is this project shareable or deployable to other jurisdictions?
Select “Yes” if the project supports multiple jurisdictions (e.g., multiple cities). Select “No” if the project primarily supports a single entity.

☐ Yes

☑ No

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

☑ Build

☐ Sustain

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

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

☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☐ Equipment - Equipment, supplies, and systems that comply with relevant standards

☐ Training - Content and methods of delivery that comply with relevant training standards

☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Vendor contract to implement SSO	Covers costs for vendor services, including planning, migration, application integration, configuration of	1	$ 39,600.00	$ 39,600.00	The vendor contract is essential for successfully implementing the secure single sign-on (SSO) system outlined in the application. The vendor will conduct the technical migration from the outdated .NET Core 3.1 SSO to Azure Entra ID and Azure AD B2C under the Nevada State	This is an implementation project. Sustaining licensing is part of NDA's existing

	security features, testing, and support for transitioning NDA’s single sign-on system to Azure Entra ID and Azure AD B2C under the NVDIS framework.				Digital Identity System (NVDIS). This includes migrating user accounts, reconfiguring NDA applications, and ensuring robust security through multi-factor authentication and user access tracking. By handling the project’s complex technical requirements, the vendor supports NDA’s goals of reducing cybersecurity risks, improving user account management, and providing secure, streamlined access to NDA services.	Microsoft licensing.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		1	$ 39,600.00	$ 39,600.00		

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

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

Application ID: 485415

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

Applicant Name	Nevada Department of Agriculture
Project Name:	Single Sign-on Implementation
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	Project Kickoff and Planning	3/31/2025
2	Migration Preparation and Setup	4/15/2025
3	User Account Migration and Application Integration	5/15/2025
4	User Acceptance Testing and Adjustments	6/15/2025
5	Production Deployment and Post-Launch Support	6/30/2025
6		
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 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Nevada Department of Transportation - Cybersecurity

FY 2024 SLCGP NDOT

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

$ 2,253,244.00 Requested

Submitted: 10/18/2024 4:09:52 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
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions top

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
□ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
□ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☑ Objective 3: Implement security protections commensurate with risk.
□ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

□ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.

□ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

□ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

☑ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

☑ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

□ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

☑ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
Enhance our Network Security by implementing NGFWs and NAC. Next-Generation Firewalls (NGFWs) and Network Access Control (NAC) work together to enhance network security through several key functions.
Next-Generation Firewalls (NGFWs)
Deep Packet Inspection: NGFWs analyze the content of packets rather than just their headers, allowing them to identify and block threats like malware and intrusion attempts that traditional firewalls might miss.
Application Awareness: They can identify and control applications rather than just ports and protocols, allowing organizations to enforce security policies based on the application level.
Intrusion Prevention Systems (IPS): NGFWs typically include IPS capabilities that can detect and block attacks in real-time.
Threat Intelligence Integration: Many NGFWs leverage threat intelligence feeds to stay updated on the latest threats and adapt their defenses accordingly.
SSL Inspection: They can inspect encrypted traffic, which is essential since a significant portion of internet traffic is now encrypted.
Network Access Control (NAC)
Device Authentication: NAC systems ensure that only authorized devices can access the network. They authenticate devices using various methods (e.g., 802.1X, certificates).
Posture Assessment: NAC evaluates the security posture of devices before granting access, checking for things like up-to-date antivirus software and security patches.
Segmentation: NAC can segment the network, isolating devices based on their role, security status, or user identity, which limits potential lateral movement by attackers.
Policy Enforcement: NAC enforces security policies dynamically, ensuring that devices comply with organizational standards before accessing network resources.
Guest Networking: NAC solutions often include guest access controls, allowing visitors to connect to the network securely without compromising overall security.
Security Cameras: Purchase, install, train users, to support visual vulnerability status of all NDOT critical infrastructure areas. This will serve as the monitoring feature of cybersecurity, and reduce primary weaknesses across NDOT's IT infrastructure.

5. How does your project align with the objective selected in Question 2?
The project aligns with Objective 3 - Implement security protections commensurate with risk by addressing some of the key issues of physical and logical cybersecurity and secure operations in the OSI Security Layers 1-3. As technology has evolved at the OSI Security Layers 4-7, vulnerabilities are being exploited by threat actors at layers 1-3 due to vulnerabilities in these areas. This equipment change will improve our capabilities in both daily operations and in an incident response recovery role as well, thereby helping to improve our state of cybersecurity.

The authentication devices will ensure that the higher requirements of MFA for service accounts are met, per NIST/FIPS guidance.

The forensics labs will help to identify and validate incident response actions with the Eradicate portion of the incident response plan be researched, analyzed, implemented and validated.

The Satellite Internet System, will ensure that the NDOT IT Infrastructure is available during the incident response period, should the established NDOT IT network or any portion of it become unavailable.

The security cameras will support Objective 3 - Implement security protections commensurate with risk by ensuring the security element 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" is monitored and recorded for all critical infrastructure across NDOT.

6. How does your project align with the program element(s) selected in Question 3?
• Network Switches w/ NAC: Elements 1, 2, 3, 5, 9, 10
• Network Routers: Elements 1, 2, 3, 4, 5, 9, 10
• NGFWs: Elements 1, 2, 3, 4, 5, 9, 10, 11
• Cellular Routers: Elements 1, 3, 7, 9, 15
• Wireless APs: Elements 1, 2, 3, 5, 9, 15
• WAN-in-a-Box: Elements 3, 7, 9, 10, 15
• Network Testing Tools: Elements 1, 2, 3, 4, 5, 9, 10
• Authentication Devices: Elements 1, 2, 3, 5, 7, 9, 11, 12, 14, 15
• Forensics Hardware: Elements 1, 2, 3, 5, 7, 9, 11, 12, 14, 15

1. Network Switches with Network Access Control (NAC) Policies
Aligned Key Elements:
• Element 1: System Management and Monitoring
o Explanation: NAC policies help manage and monitor devices and user accounts accessing the network, ensuring only authorized users and compliant devices connect.
• Element 2: Network Traffic Monitoring
o Explanation: Switches with NAC can track network activity, providing visibility into who is accessing the network and what they're doing.
• Element 3: Cybersecurity Preparedness and Resilience
o Explanation: Enforcing NAC policies strengthens the network's defense against unauthorized access and potential threats.
• Element 5: Adoption of Cybersecurity Best Practices
o Explanation: Implementing NAC is considered a best practice for network security management.
• Element 9: Communication Network Continuity
o Explanation: By preventing unauthorized access, NAC policies help maintain the integrity and availability of communication networks.
• Element 10: Critical Infrastructure Protection
o Explanation: Protecting network infrastructure from unauthorized devices mitigates risks to critical systems.

2. Network Routers
Aligned Key Elements:
• Element 1: System Management and Monitoring
o Explanation: Advanced routers allow for comprehensive management and monitoring of network systems.
• Element 2: Network Traffic Monitoring
o Explanation: This technology provides detailed insights into network traffic patterns and anomalies.
• Element 3: Cybersecurity Preparedness and Resilience
o Explanation: Enhances network resilience through dynamic routing and self-healing capabilities.

• Element 4: Continuous Vulnerability Assessments
o Explanation: Supports ongoing assessments by providing real-time data and analytics (Analytics).
• Element 5: Adoption of Cybersecurity Best Practices
o Explanation: Utilizing advanced routing technologies aligns with industry best practices for network security.
• Element 9: Communication Network Continuity
o Explanation: Ensures stable and continuous communication between state and local governments.
• Element 10: Critical Infrastructure Protection
o Explanation: Secures the backbone of critical network infrastructure against potential threats.
____
3. Next-Generation Firewalls (NGFWs)
Aligned Key Elements:
• Element 1: System Management

Authentication Devices ensure an extra layer of MFA for Service Accounts

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
NDOT IT Staff will accomplish the installation, purchase, training, implementation and maintenance of all the identified equipment listed below. The process will be ticketed and assigned through the NDOT IT Ticketing System, and prioritized by project managers for each department in Cyber Ops and Cyber Security for NDOT IT with the exception of the below item:

Security cameras will be purchased, and installed by contract workers who are NOT NDOT employees.

9. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome of the NDOT Equipment Purchase will reflect the following.

The Combined Benefits are:
Layered Security: The combination of NGFWs and NAC creates a multi-layered security approach, making it more difficult for attackers to breach the network.
Real-Time Response: Both systems can provide real-time alerts and responses to potential threats, enabling quicker remediation.
Comprehensive Visibility: Together, they offer enhanced visibility into network traffic and device behavior, aiding in the identification of anomalies.
In summary, NGFWs and NAC work together to create a robust security framework, protecting the network from a wide range of threats while ensuring that only authorized and compliant devices can connect.
Authentication Devices will help to ensure that only the holders of these devices will be authenticated to log into the network as Service Account Holders. These devices will serve as MFA keys, to keep service accounts secure from credential harvesting.
Forensics hardware will assist in researching the effects of viruses, cyber-attacks and insider threats across the NDOT IT infrastructure. In an incident recovery, the Satellite Internet System will help to meet the recovery time objective of the incident response plan, should any portion of the NDOT IT infrastructure become unavailable.

The purchase and installation of the security cameras will be used to continuously monitor the critical infrastructure and cybersecurity equipment across NDOT and ensures continuous availability.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
□ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)
☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89712

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
Yes, the project is scalable at the organization's desire once built and will be expanded.

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
☑ Yes
□ No

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

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

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
□ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

□ Training - Content and methods of delivery that comply with relevant training standards

□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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 Switches with Network Access Control (NAC) Policies	Network Access Control solutions provide organizations with control over the devices that are connected to the corporate network. With NAC, companies can block non-compliant devices entirely or restrict their access to corporate assets.	1	$ 23,304.00	$ 23,304.00	Support network security activity for NAC	Will maintain security operations at a reduced effectiveness	Switch, Network	04HW-03-SWCH
Network Routers	A router is a device that connects two or more packet-switched networks or subnetworks. It	1	$ 66,393.00	$ 66,393.00	Support network security activity for NAC, Provide Stealth Networking and Resiliency	Will maintain security operations at a reduced effectiveness	Router	04HW-03-ROUT

	serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.							
Next-Generation Firewalls (NGFWs)	A next-generation firewall (NGFW) is a network security device that provides capabilities beyond a traditional, stateful firewall12345. NGFWs are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall3. NGFWs evolve and expand upon the capabilities of traditional firewalls, combining a conventional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS)4.	1	$ 58,772.00	$ 58,772.00	Improves deep packet stateful inspection, with next gen features	Will maintain security operations at a reduced effectiveness	Firewall, Network	05NP-00-FWAL
Cellular Routers	Cellular routers are a type of router that uses cellular technology to provide internet access. They are an ideal solution for businesses, homes, and other locations that don't have access to wired internet services, such as cable or fiber.	1	$ 2,000.00	$ 2,000.00	The ability to secure remote locations for network traffic	Will maintain security operations at a reduced effectiveness	Router	04HW-03-ROUT
Wireless Access Points (APs)	A wireless access point (wireless AP) is a network device that transmits and receives data over a wireless local area network (WLAN), serving as the interconnection point between the WLAN and a fixed wire	1	$ 3,947.00	$ 3,947.00	Support network security activity for NAC, also to improve endpoint security and visibility	Will maintain security operations at a reduced effectiveness	Access Point, Wireless	04HW-03-WAP

	network.							
WAN-in-a-Box	A Wide Area Network (WAN) connects one or more local area networks (LAN) to form an extensive network of connected computers, devices, and hardware spanning a large geographical area – typically across cities, states and countries.	1	$ 5,100.00	$ 5,100.00	The ability to provide security connectivity for pop-up networks during emergency response	Will maintain security operations at a reduced effectiveness	Router	04HW-03-ROUT
Network Testing Tools	Tools used to assess and evaluate the performance, reliability, and security of computer networks. Measure network characteristics. Identify potential issues. Optimize network performance.	1	$ 26,395.00	$ 26,395.00	Identifies network vulnerabilities and Issues, increases Mean-Time-To-Repair (MTTR) for managing outages and incidents	Will maintain security operations at a reduced effectiveness	Tools, Vulnerability Scan	05NP-00-SCAN
Authentication Devices	FIPS 140-2 validated security keys	150	$ 115.00	$ 17,250.00	Will ensure Authentication and Validation of all Service Accounts by ensuring compliance of FIPS 140-2 validated (Overall Level 1 and Level 2, Physical Security Level 3) Meets the highest authenticator assurance level 3 (AAL3) of NIST SP800-63B guidance.	Will maintain security operations at a reduced effectiveness	Device, Biometric User Au	05AU-00-BIOM
Forensics Lab	Forensic Laptops, Imagers, and Media	1	$ 192,083.00	$ 192,083.00	Will allow for cybersecurity deep analysis of cybersecurity Incidents	Will maintain security operations at a reduced effectiveness	Forensics, Software	05HS-00-FRNS
Satellite Internet System	Satellite earth station transmitter and receiver, usually Ka,Ku, or V. Examples include, but are not limited to Starlink, Iridium and INMARSAT A and B.	6	$ 18,000.00	$ 108,000.00	Provides the ability to communicate and restore temporary communications until normal communications are restored in an incident	Incident Response Communications Will not be available	Equipment, Satellite Data	06CC-04-EQSD
Security Cameras with Installation	a camera that records images in or outside a building or in a public place, in order to prevent or help solve crime there:	1	$ 1,750,000.00	$ 1,750,000.00	Tools for maintaining and consolidating information about an organization's IT resources, including both hardware and software assets.	Will be unable to support continuous monitoring via video surveillance, which creates vulnerabilities of critical infrastructure	System, Information Techn	05SM-00-ITAM
			$	$				
			$	$				
			$	$				
		165	**$ 2,146,109.00**	**$ 2,253,244.00**				

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)	☑	Travel Policy Audit Nevada Single Audit Report Milestones NDOT Cybersecurity Equipment Needs
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestones FY 2024 NDOT Milestones NDOT Cybersecurity Equipment Needs Milestones NDOT Cybersecurity Equipment Needs

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

Application ID: 484405

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	Nevada Department of Transportation
	Project Name:	NDOT Cybersecurity Equipment Needs
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Network Switches with Network Access Control (NAC) Policies ; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
2	Network Routers; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
3	Next-Generation Firewalls (NGFWs); purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
4	Cellular Routers; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
5	Wireless Access Points (APs); purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
6	WAN-in-a-Box; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
7	Network Testing Tools; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
9	Authentication Devices; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
10	Forensics Lab; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
11	Satellite Internet System; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
12	Security Cameras with Installation; purchase equipment; train personnel and deploy equipment; and maintain equipment	Friday, November 28, 2025
13		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Office of the Chief Information Officer

Cyber Tool Tracking System 2.0 (CTTS).

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

$ 297,927.72 Requested

Submitted: 11/1/2024 2:00:19 PM (Pacific)

Project Contact
Tiffany Morelli
tiffanymorelli@it.nv.gov
Tel: 775-531-3078

Additional Contacts
daxtell@it.nv.gov

Office of the Chief Information Officer

100 N Stewart St Ste 100
Carson City, NV 89701
United States

Management Analyst III
Tiffany Morelli
tiffanymorelli@it.nv.gov

Telephone	775-531-3078
Fax	
Web	http://it.nv.gov/
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☑ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to

cybersecurity incidents and ensure continuity of operations.

□ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
□ Objective 3: Implement security protections commensurate with risk.
□ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
□ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
□ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
□ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
□ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
□ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
□ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
□ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☑ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
□ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
□ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☑ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
□ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☑ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
We wish to trial, refine, and deploy the Cyber Tool Tracking System (CTTS) that was successfully completed in 2024 but was unable to deploy due to a lack of state funding. This tool allows the sharing of information between Nevada political subdivisions to improve efficacy and efficiency with the use of cybersecurity tools leveraging tips, tricks, and warnings gained from direct experience.
To strengthen cybersecurity risk management for the State and for Nevada the CTTS was successfully designed and built to capture cybersecurity tool assets from Nevada's political subdivisions. This program is a crowdsourced asset management tool that provides a collaboration mechanism enabling visibility into and sharing of users' experiences with their cybersecurity tools. Sharing benefits and liabilities with individual tools provides efficiencies of use, visibility of assets, and invaluable assistance in disaster recovery efforts.

5. How does your project align with the objective selected in Question 2?
This project provides a collaborative tool for agencies to share their experiences in using cybersecurity tools and maintain a centralized asset repository to improve responsiveness and continuity of operations from tool failure, both internal user fails and external tool fails (e.g., SolarWinds, Crowdstrike). An additional benefit of this system is a governance committee to ensure best practices are employed.

6. How does your project align with the program element(s) selected in Question 3?
Creating a statewide tracking tool database builds a knowledge repository which enables cybersecurity planning, learning, and tabletop exercises will be invaluable. Sharing information between State agencies, counties, locals, and tribal entities will improve the security capabilities for all Nevada government organizations. This initiative could be a key component in bringing Nevada political subdivisions closer together.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
The bulk of the project will be accomplished by state FTE staff. Some training and integration will be executed by a service provider vendor.

Project Director David Axtell, Chief Deputy CIO/CTO, Office of the Chief Information Officer, State of Nevada; daxtell@it.nv.gov

Project Manager Lisa Jean, Enterprise Architect; Office of the Chief Information Officer, State of Nevada; ljean@it.nv.gov

Fiscal Manager Tiffany Morelli, CFO, Office of the Chief Information Officer, State of Nevada; 775-531-3078, tiffanymorelli@it.nv.gov

Grant Documentation Tiffany Morelli, CFO, Office of the Chief Information Officer, State of Nevada; 775-531-3078, tiffanymorelli@it.nv.gov

Darla Dodge, Senior Deputy CIO/COO, Office of the Chief Information Officer, State of Nevada, darladodge@it.nv.gov

9. Describe, in a few sentences, the desired outcome(s) of your project.
Provide a crowdsourced tool to leverage cybersecurity tool experiences made available to all state political subdivisions.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the

Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89701

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

This system is scalable, limited only by the license funding. It would be possible to reduce the costs by reducing the number of political subdivisions to be licenses. Initially, we've scoped funding for 35 entities.

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

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

☑ Yes

□ No

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

□ Build

☑ Sustain

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

FFY 2021 Homeland Security Grant Program

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

□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

□ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

☑ Training - Content and methods of delivery that comply with relevant training standards

□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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
Public Sector Digital Services Professional – Fulfiller User v2 (2 years)		35	$ 6,370.92	$ 222,982.20	These licenses will provide access to the tool which will allow agencies to share their experiences in using cybersecurity tools and maintain a centralized asset repository to improve responsiveness and continuity of operations	The current request will cover OCIO costs through the new biennium. OCIO intends to build the ongoing license costs into the upcoming budget through its rate development process.	AEL information to be completed if project is awarded (further information required) - AJ 11/06/24	
Business Stakeholder User V4 (2 years)		8	$ 664.65	$ 5,317.20	These licenses will provide access to the tool which will allow agencies to share their experiences in using cybersecurity tools and maintain a centralized asset repository to improve responsiveness and continuity of operations	The current request will cover OCIO costs through the new biennium. OCIO intends to build the ongoing license costs into the upcoming budget through its rate development process.	AEL information to be completed if project is awarded (further information required) - AJ 11/06/24	
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		43	**$ 7,035.57**	**$ 228,299.40**				

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?
Service deployment and training services		200	$ 242.31	$ 48,462.00	This training and deployment will assist state staff in developing the repository and maintaining the ongoing system.	Deployment and Training is a one-time cost that would not be required to fund after the successful completion of the project.	No
Impact Guided – public Sector (US) V2 (2 years)		1	$ 21,166.32	$ 21,166.32	This training and deployment will assist state staff in developing the repository and maintaining the ongoing system.	Training is a one-time cost that would not be required to fund after the successful completion of the project.	No
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

			$	$			
			$	$			
			$	$			
		201	$ 21,408.63	$ 69,628.32			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 Report 2022
Travel Policy	☑	OCIO Travel Policy
Payroll Policy	☑	NV Central Payroll Policity
Procurement Policy	☑	NV State Purchasing Policy
Milestones download template	☑	OCIO CTTS Milestones
Administrative Documents *		
		State Single Audit 2022

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

Application ID: 485403

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

©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.

Logout | Browser

Applicant Name	Office of the Chief Information Officer
Project Name:	Cyber Tool Tracking System 2.0 – (CTTS)
Project Funding Stream:	FY 2024 SLCGP
Milestone Description*	Date of Expected Completion
1. Review and refined detailed requirements for the CTTS 2.0 program.	TBD
2. Coordinate with the Office of Cyber Defense Coordination (OCDC) to create a trial and deployment of the CTTS 2.0 program.	TBD
3. Create a detailed project plan and program charter for CTTS 2.0.	TBD
4. Procure necessary licenses for CTTS 2.0.	TBD
5. Execute training for project staff.	TBD
6. Refine CTTS application to create the CTTS 2.0 application.	TBD
7. Deploy trial CTTS 2.0, test, and integrate community feedback.	TBD
8. Coordinate solution deployment with OIS and OCDC.	TBD
9. Create an operational playbook based on the trial experiences.	TBD
10. Create a funding model for individual political subdivisions to support the CTTS 2.0 program.	TBD
11. Deploy Cyber Tool Tracking System 2.0 to the licensed community.	TBD
12. Close out project/project measurement/project evaluation and transition to a sustainable program.	TBD

Dates to be updated if project is awarded - further information required - AJ 11/06/24

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Office of Cyber Defense Coordination
Incident Response Team Staffing

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

$ 559,998.00 Requested

Submitted: 11/1/2024 11:51:50 AM (Pacific)

Project Contact
Adam Miller
amiller@ocdc.nv.gov
Tel: 7754316381

Additional Contacts
amiller@ocdc.nv.gov,Lhicks@dps.state.nv.us

Office of Cyber Defense Coordination

100 N Carson St Ste 100
Carson City, NV 89701
United States

Administrator
Adam Miller
amiller@ocdc.nv.gov

Telephone	7754316381
Fax	
Web	
UEI	MAXGJADTHWV7
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to

cybersecurity incidents and ensure continuity of operations.

☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☐ Objective 3: Implement security protections commensurate with risk.
☑ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☑ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☐ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☑ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☑ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☑ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☑ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☑ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☑ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
Sustain our Incident Response Team which was created using FY23 grant funds. This team will be available to assist SLTT partners in the state of Nevada, including the rural entities. This will serve as the functional base for assisting SLTT partners in creating workable Incident Response Plans and facilitate these plans in the event of a cyber threat and/or an attack. The team will implement security protections to counter these threats and attacks. An IRT will also enable the State to be aware of more incidents within the state, therefore better able to monitor traffic and activity. Additionally, part of the aim of the project is to allow entities to easily share information with each other to enhance the state’s capabilities to react across the board to threats detected within an entity, and have a good, centralized resource for cyberthreat activity indicators. We are focusing our efforts on what would most benefit rural areas with a minimum 80% of the funds awarded to be invested solely in those rural areas through IRT collaboration and response efforts, however, our work is open to non-rural entities as well should they choose to use it.

5. How does your project align with the objective selected in Question 2?
Sustaining the IRT will enable us to continue to be available to assist our SLTT partners and continue to assist all agencies to work together to 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. Smaller entities, with limited budgets, will continue to benefit by receiving assistance when faced with a cyber threat and/or attack.

6. How does your project align with the program element(s) selected in Question 3?
Allowing all partner entities in the state access to this project, we are enabling them to 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, to protect them against threats and/or attacks.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
The project will allow the OCDC to sustain staffing and continue to have an IRT available for SLTT’s within the state. The IRT will be available in assisting with creating and implementing Incident Response Plans.

9. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome of this project would be to proactively assist SLTT partners with their tailored incident response plans so that they are able to quickly and efficiently react to a malicious cyber attack. The IRT would be able to advise SLTT partners where their current deficiencies are and how to improve. Additionally, the IRT will be able to come in immediately after a malicious cyber incident to help with remediation, backup, and recovery if necessary of SLTT networks and data. The project will also assist the state's partner agencies, including those in the rural areas, work together in sharing information with each other in order to enhance the state's capabilities to react across the board to threats detected within an entity, and have a good, centralized resource for cyber threat activity indicators.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building’s structure, layout, systems, or critical aspects of a building’s safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page:

https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89711

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

We can scale by expanding or reducing the number of staffing hired and the positions needed based on the needs of our partner entities.

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

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

☑ Yes

☐ No

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

☐ Build

☑ Sustain

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

FY23 Support Staff Kickstart

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

☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

☐ Training - Content and methods of delivery that comply with relevant training standards

☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Sustain Hires/New Hires	Staffing to support SLTT entities and create an incident response team.	3	$ 184,666.00	$ 553,998.00	By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We can provide immediate assistance when any entity is experiencing a cyber threat or attack. Additionally, an IRT can advise and assist SLTT partners in creating a robust IRP pre-attack so they are better prepared to deal with an attack if/when one happens.	We may look to subsidize the IRP efforts from other sources within the State government. The most likely approach if grant funding is reduced or discontinued is we would either seek alternate sources of funding or wait until the next legislative appropriations cycle.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$
		3	$ 184,666.00	$ 553,998.00

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
Staff Support Hardware/Software	Hardware and Software that the IRT staff will need to assist with their work for the state.	3	$ 2,000.00	$ 6,000.00	This line item will support both the hardware and software needs of the IRT as they assist SLTT partners.	If grant funding was reduced or discontinued, OCDC would not be able to sustain the project in its current form. We would look to maximize the impact of the IRT while on contract before the contract ultimately expired.	Hardware, Computer	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		3	$ 2,000.00	$ 6,000.00				

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)	☑	A-133 FY22
Travel Policy	☑	DPS Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	IRT Grant Milestones

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

Application ID: 485178

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	Office of Cyber Defense Coordination
	Project Name:	Incident Response Team Staffing
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Policy/Planning: Incident response plans (IRPs) created for majority of counties (10/17)	11/30/2027
2	Operation: IRT able to assist in remediation and recovery after attack in majority of incidents	11/30/2027
3	Equipment: Provide state-approved equipment to contracted employees to ensure they are able to work on state systems and with SLTT partners	1-month after receiving grant funding.
4		
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Office of Cyber Defense Coordination

Statewide SOC/ISAC

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

$ 400,000.00 Requested

Submitted: 11/1/2024 11:53:39 AM (Pacific)

Project Contact
Adam Miller
amiller@ocdc.nv.gov
Tel: 7754316381

Additional Contacts
amiller@ocdc.nv.gov,Lhicks@dps.state.nv.us,,D.boyter@dps.state.nv.us

Office of Cyber Defense Coordination

100 N Carson St Ste 100
Carson City, NV 89701
United States

Administrator
Adam Miller
amiller@ocdc.nv.gov

Telephone	7754316381
Fax	
Web	
UEI	MAXGJADTHWV7
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

☐ Yes
☑ No

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☑ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☐ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☑ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☑ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☑ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☑ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☑ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☑ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☑ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
A statewide Security Operations Center will benefit both rural and urban entities, but a focus will be on using the allocated grant money to allow rural entities to use the SOC service to increase their cybersecurity and become aware of threats they may not have previously been aware of. Rural entities, because of their minimal resources and potentially minimized cybersecurity staff, are at greater risk for malicious cyber incidents that can ultimately have a greater impact on whole of state operations. We are focusing our efforts on rural areas, with a minimum 80% of the funds awarded to be invested solely in those rural areas, however, our work is open to non-rural entities as well should they choose to use it. We anticipate rural funding allocation to exceed 80%. The needs of the rural areas will drive our products direction.

5. How does your project align with the objective selected in Question 2?
A security operations center will allow entities to provide data to highly trained professionals that will be able to highlight and respond to potentially malicious cyber incidents and indicators of compromise on entity networks. Because a SOC is staffed 24-7, entities can feel confident that an organization is constantly monitoring their cybersecurity and cyber risk for any malicious cyber incidents.

6. How does your project align with the program element(s) selected in Question 3?
A SOC will not only ensure that entities that provide information are being constantly monitored for malicious cyber incidents, but a SOC can be one of the first steps in flagging an indicator of compromise that can then be shared not only with the victim network but also a vast organization of connected entities that will find the information useful to begin scanning their own networks for potential indicators of compromise. At the very least, a SOC benefits the single entity that is maliciously attacked, at most, a SOC can uncover a malicious cyber incident that can be found and remediated and increase the cybersecurity posture of all other state networks. Finally, the cybersecurity training courses and certifications that can be taken as a result of the grant funding will potentially allow rural entities to become better trained and qualified to perform incident response/handling when they receive notifications from the SOC that there is an indicator of compromise or an active malicious cyber incident.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
At this point in time, the State is looking to contract with a 3rd party vendor to manage the security operations center for the State. The SOC will receive data and information from entities that wish to contribute and the licenses that are provided to the rural and urban entities to submit data to the SOC will be paid for with money from the SLCGP grant.

9. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome is a large percentage of public entities from rural, urban, and SLTT partners that provide information and data to the SOC. The SOC would then be able to scan for vulnerabilities and indicators of compromise and alert the effected entity. This ensures a more robust cybersecurity posture and a whole-of-state approach to protecting and defending the network. Finally, the grant would provide a number of training opportunities for SLTT partners that would ensure they are able to adequately address any issues raised by the SOC.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
□ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)
☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89711

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
Depending on grant resourcing, the project will be scalable. If the grant funding is fully appropriated, OCDC will be able to provide more licenses to more entities, allowing the SOC to review more data for malicious cyber incidents or indicators of compromise. The less resourcing that is appropriated for the SOC, the less licenses OCDC will be able to provide to entities and the more at-risk networks could be.

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
☑ Yes
□ No

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

16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project.
FY23 OCDC Statewide SOC/SIEM/ISAC Program

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
□ Equipment - Equipment, supplies, and systems that comply with relevant standards
☑ Training - Content and methods of delivery that comply with relevant training standards
□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Direct Partner Outreach	Working with all state entities, including rural, to ensure smoother deployments of support projects.	1	$ 20,000.00	$ 20,000.00	Would be used to directly support the deployment of the project with partner entities and provide hands on support for the technical needs required to get the project online. This would include travel to relevant rural entities for direct support.	Any reduction or discontinuation of grant funding for partner outreach runs the risk of SLTT partners not having the information and hands on setup necessary to join in on SOC services. Reducing the number of entities that opt-in to SOC services poses a risk for the cybersecurity of the state as a whole due to the vastness of connected networks.
SLTT Collaboration	Used to bring together SLTT entities and vendor analysts to describe the benefits of using SOC services.	1	$ 15,000.00	$ 15,000.00	This grant funding would be directly used to create a conference or symposium to bring together entities across the state to show them the value of opting-in to a managed SOC that is contracted with the State. By bringing them together in-person, they can see first hand the benefits of their organization or entity participating in SOC services.	Reduction or discontinuation of this grant funding will decrease the likelihood that entities will have the knowledge or understanding of the services that a SOC will provide. Statewide cybersecurity would be at an increased risk with entities unknowing of the risks on their networks.
Contractor/Consulting Services	Contract with a 3rd-party vendor to run a Security Operations Center to review, analyze, and report on SLTT systems	1	$ 330,200.00	$ 330,200.00	This particular line item would go directly towards funding a third-party SOC and the licenses necessary for entities to have to provide the information needed to the SOC for review and analysis. The greater the award appropriation, the greater number of licenses and entities that the SOC can cover in a given fiscal year.	Any reduction or discontinuation in grant funding for contracted SOC services or license will directly impact the amount of support that the SOC can provide and the amount of licenses that can be provided to entities that need them.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		3	$ 365,200.00	$ 365,200.00		

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?
Cybersecurity Training Courses	Training vouchers	4	$ 8,700.00	$ 34,800.00	Continuing education and training is a very useful resource when dealing with how to provide, interpret, and respond to the data that is providing to the SOC. Rural and underserved entities would most likely not have access to this training due to the resource intensive nature.	If funding for training was reduced or discontinued that would directly effect the success of the information that entities are providing to the SOC and how they are handling the outcomes of the reports the SOC provides.	No
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		4	**$ 8,700.00**	**$ 34,800.00**			**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 FY22
Travel Policy	☑	DPS Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestones Document

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

Application ID: 485184

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

Applicant Name	Office of Cyber Defense Coordination
Project Name:	Statewide SOC/ISAC
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	Increase enrolled entities to the SOC by 50% from previous year.	30-Nov-26
2	Purchase training vouchers in DEC or JUL, whichever comes first after appropriation of award.	7/30/2025, 12/30/25
3	Dissemination of 50% of training vouchers to rural entities to increase awareness and response to malicious cyber incidents uncovered by the SOC	7/30/2025, 12/30/25
4		
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Washoe County

Vulnerability Management Tool

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

$ 275,000.00 Requested

Submitted: 10/28/2024 10:27:49 AM (Pacific)

Project Contact
Christopher Bower
cbower@washoecounty.gov
Tel: 7758585935

Additional Contacts
none entered

Washoe County

1001 E. 9th St.
Reno, NV 89512
United States

IT Manager
James Wood
jawood@washoecounty.gov

Telephone	(775) 328-2200
Fax	
Web	www.washoecounty.gov
UEI	GPR1NY74XPQ5
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
□ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to

cybersecurity incidents and ensure continuity of operations.

☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☑ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☑ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☑ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
As a governmental organization, Washoe County must adhere and comply with Nevada Revised Statutes (NRS) Chapter 603A.210. In this policy, it is stated that governmental organizations must “comply with the current version of the Center for Internet Security (CIS) Controls as published by the Center for Internet Security, Inc.” CIS Control 7 specifies assessing and tracking vulnerabilities in enterprise assets, which can be completed using a vulnerability management tool. This process is crucial because unaddressed vulnerabilities can be exploited by attackers, leading to data breaches and significant financial loss. Additionally, an effective vulnerability management tool would be advantageous for the county's rural communities, as having such a tool would enhance the security of all network devices county-wide. Approximately 36% of the total funding request will be dedicated to rural communities in Washoe County.

5. How does your project align with the objective selected in Question 2?
Implementing a vulnerability management tool helps Washoe County proactively identify and assess specific risks associated with their systems and applications. By regularly assessing vulnerabilities and prioritizing them based on potential impact, organizations can allocate resources more effectively, focusing on high-risk areas first. This targeted approach ensures that security measures are proportional to the threats, enhancing overall protection while optimizing costs.

6. How does your project align with the program element(s) selected in Question 3?
Implementing vulnerability management enhances the preparation, response, and resilience of information systems by establishing a proactive approach to identifying and addressing potential threats. Continuous assessments allow organizations to stay ahead of emerging vulnerabilities and adapt their defenses accordingly, minimizing the risk of exploitation. By prioritizing vulnerabilities based on their risk levels, organizations can focus resources on the most critical areas, ensuring a more effective response to cybersecurity threats.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Washoe County will source a suitable vendor to provide a vulnerability management tool, a dedicated team from within Washoe County's Infrastructure, Systems Administration, and Security group will work with the vendor to deploy the solution.

9. Describe, in a few sentences, the desired outcome(s) of your project.
The primary outcome of the project is to comply with the CIS Controls and Chapter 603A of the NRS statute. Additionally, implementing a vulnerability management tool ensures Washoe County can effectively prepare for and respond to evolving cybersecurity threats.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building’s structure, layout, systems, or critical aspects of a building’s safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during

the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

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

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

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
Washoe County Technology Services will hire a vendor that implements a vulnerability management tool. This project can be scaled to the extent that the cost of available solutions varies from vendor to vendor, while still satisfying the requirements stipulated by the referenced CIS controls.

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
☐ Yes
☑ No

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

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

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
☐ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
☑ Equipment - Equipment, supplies, and systems that comply with relevant standards
☐ Training - Content and methods of delivery that comply with relevant training standards
☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	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
Vulnerability Management Tool	A software tool for Vulnerability Management	1	$ 275,000.00	$ 275,000.00	This is the only purchase associated with this project. It will provide Washoe County with a process to protect enterprise assets and abide by CIS Controls.	Washoe County will submit for budget funding and if denied, we would cease using the product.	System, Patch/Config MGT	05PM-00-PTCH
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	**$ 275,000.00**	**$ 275,000.00**				

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)	☑	A-133 Audit
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: 484898

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

Applicant Name	Washoe County Technology Services
Project Name:	Vulnerability Management Tool
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	Source a suitable vendor	29-Jan
2	Receive quotes from vendors	21-Oct
3	Implement the vulnerability management tool	4-Mar
4		
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Washoe County Emergency Management & Homeland Security Program

Washoe County - Second Judicial District Court: Cyber Security and Network Strengthening

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

$ 566,251.40 Requested

Submitted: 10/31/2024 10:45:48 AM (Pacific)

Project Contact
Francisco Ceballos
FCeballos@washoecounty.gov
Tel: 7752244109

Additional Contacts
Valerie.Moser@washoecourts.us,chris.long@washoecourts.us

Washoe County Emergency Management & Homeland Security Program

5195 Spectrum Blvd
Reno, NV 89512
United States

Emergency Manager
Kelly Echeverria
KEcheverria@washoecounty.gov

Telephone	7753994811
Fax	
Web	www.readywashoe.com
UEI	
SAM Expires	11/10/2021

Pre-Application *top*

1. Is your organization one of the following types of entities?: County, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of government, regional government entity, agency or instrumentality of a local government, rural community, unincorporated town or village, or other public entity, tribe, or authorized tribal organization.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☑ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

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

Projects may align with more than one element.

☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.

☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.

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

The Second Judicial District Court (SJDC) is seeking funding to be able to enhance and secure their enterprise network systems. As a separate branch of government, SJDC is funded within Washoe County but must maintain completely separate networks and database systems from the Executive Branch. SJDC plans to implement this funding to improve its cyber-secure wireless and filtering systems by purchasing wireless access points since wireless points are a common target and known point for cyber intrusion and exploitation. In addition to purchasing the access points, SJDC would like to purchase up to date and secure network switching this would enable the creation of virtualized networks that automate network operations, simplify network provisioning, and enhance security, all while reducing the strain on network and IT personnel. SJDC would also hire a consultant to assist with ensuring proper installation and compliance with latest cyber security recommendations. SJDC would like to enhance password security by purchasing a system that allows sharing to applicable Tech Services Administrative personnel without having to expose passwords. SJDC would like to purchase a multi-factor authentication for entire enterprise environment for all personnel. Additional software to preempt infrastructure issues with automated trending and capacity planning graphs and proactive alerts. The last added component to enhance the security would be additional security for the end users. By purchasing end-point protection for all users against malware, viruses, and anomalies with 24/7 monitoring, the SJDC Court Tech team could be notified immediately upon a potential risk or breach of security and be able to close off that user prior to the risk of infecting the whole system. If awarded, funding will benefit not only the Cities of Reno and Sparks, but would also benefit rural, unincorporated Washoe County which encompasses 22% of the population.

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

SJDC's project would implement multi point security protections in hardening access from external users, in addition to bringing internal systems up to current standards in the cyber security field. This project would benefit not only SJDC's Court Technology but enhance protection for all end users and judicial data and systems. With this project, SJDC's ultimate goal is to mitigate risk throughout the entire enterprise.

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

SJDC's project aligns with enhancing the preparation, response, and resilience of information systems, applications, and user accounts by enabling multi factor on all systems for all users. With 24/7 monitoring and response for anomalies, ransomware, alerts and risks associated with dangerous cyber threats, SJDC will be able to be more resilient to respond to quickly issues and threats. MFA enhancements will bring SJDC up to current best practices in addition to having constant mobile devices VPN ability. With the modernization of network equipment this will enhance security and resiliency to a critical component of the criminal justice system, the judicial system. If the Courts are not assessable, trials are delayed, jail populations increase, and citizen safety greatly impacted. With automating alert notifications and capacity planning the risk of reduced operations is mitigated. By having secured wireless equipment this will give SJDC the ability to add enterprise level devices with the range of authentication options and granular network policies that can be applied globally or customized for local access.

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

☑ Implement multi-factor authentication.

☑ Implement enhanced logging.

☑ Data encryption for data at rest and in transit.

☑ End use of unsupported/end of life software and hardware that are accessible from the internet.

☑ Prohibit use of known/fixed/default passwords and credentials.

☐ Ensure the ability to reconstitute systems (backups).

☐ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.

☐ Migration to the .gov internet domain.

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

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

SJDC, Court Tech team will be responsible for acquiring necessary quotes and purchasing the equipment. This project will be led by Court Tech Manager, Celina Galindo. Assessment review and follow up will be conducted by all and reported to the Second Judicial District Court Leadership Team.

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

Second Judicial District Court strives to provide the timely, fair, and efficient administration of justice under the law, in a matter that instills and sustains the public's confidence in the judicial system. In order to provide this justice, a strong, safe, network backbone must be in place. Without the security of the justice documents and its users, the public's confidence would be eliminated. With this funding, SJDC strives to enhance the cybersecurity of the entire District Courts enterprise network to provide faith in the justice system for everyone.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.

Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
If necessary, the Second Judicial District Court could eliminate part of the equipment requests, but that would decrease the level of security for the Court and keep that area of the network at a higher risk for cyber-attacks and intrusions.

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
☐ Yes
☑ No

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

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

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
☑ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
☑ Equipment - Equipment, supplies, and systems that comply with relevant standards
☐ Training - Content and methods of delivery that comply with relevant training standards
☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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?
Consultant Services	consult to assist with always on VPN activation and monitoring	1	$ 30,000.00	$ 30,000.00	Consultant services would assist with 24/7 monitoring as well as always on VPN configuration development. Consultant will verify configuration and compliance with current security standards.	Above base funding would be requested.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		1	$ 30,000.00	$ 30,000.00		

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	How would your organization sustain this project if grant funding was	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

					the Application Questions section.	reduced or discontinued?		
Password protection/manager	Secure Passwords	1	$ 14,000.00	$ 14,000.00	Securely stores passwords and allows system administration sharing without having to write out.	Small yearly fee would be requested as an above base request for general funding.	Information Tech - risk	04AP-04-RISK
MFA platform	enterprise Multi Factor Authentication	1	$ 6,251.40	$ 6,251.40	Enforces enterprise Multi Factor Authentication on login to computers to ensure secure authentication and authorization of users.	Small yearly fee would be requested as an above base request for general funding.	Cyber Security En Ntwk	05NP-00-IDPS
Cyber Security platform	Enhanced investigation and remediation all threats.	1	$ 50,000.00	$ 50,000.00	Cynet keeps your servers, and mobile devices safe from malware, ransomware, and other dangerous cyberthreats.	SJDC will continue to request budget authority from Washoe County for this item.	Cyber Security En Host	05HS-00-MALW
Software - proactive alerting, trending and planning	Software	1	$ 20,000.00	$ 20,000.00	Preempt infrastructure issues with automated trending and capacity planning graphs and proactive alerts.	Above base funding would be requested.	Cyber Security En Ntwk	05NP-00-IDPS
Network Switches	network switches	1	$ 410,000.00	$ 410,000.00	Enable the creation of virtualized networks that automate network operations, simplify network provisioning, and enhance security	Requested funding would be requested once switch would need to be replaced.	Information Tech Hardwar	04HW-01-INHW
New Wireless Access Points	Wireless systems are known point for cyber intrusion and exploitation.	45	$ 800.00	$ 36,000.00	This add-on provides additional insight into cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.	SJDC would submit a request to the County for additional budget authority to carry out this project. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available.	Information Tech Hardware	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		50	**$ 501,051.40**	**$ 536,251.40**				

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 2023
Travel Policy	☑	WC Travel Policy
Payroll Policy	☑	SJDC Personnel Manual
Procurement Policy	☑	Washoe County Purchasing Manual
Milestones download template	☑	Milestones

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

Application ID: 485279

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	Second Judicial District Court
	Project Name:	SJDC's Cyber - Security
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Acceptance of Funding by Washoe County Board of County Commissioners (BCC), Setting up of separate grant tracking of fiscal expenses within financial system	Assume award notification by 10/1/2025. Within 90 days of receipt of Award notification. By end of December 2025
2	Obtain necessary updated quotes from vendors for all equipment	within 90 days of receipt of Award notification. By end of December 2025
3	Issue of Purchase Orders for equipment	within 45 days of acceptance of funds by BCC. By February 15, 2025
4	Install of equipment	within 90 days of receipt of equipment. May vary depending on product backlog/shipment issues.
5	Final review and report of project to DEM	By end of December 2026
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Washoe County School District

WCSD Cyber Forensic Suite

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

$ 60,000.00 Requested

Submitted: 10/31/2024 1:04:08 PM (Pacific)

Project Contact
Austin Smith
austin.smith@washoeschools.net
Tel: 7757893422

Additional Contacts
lohlin@washoeschools.net,radrake@washoeschools.net,radrake@washoeschools.net

Washoe County School District

425 E 9th St
Reno, NV 89512
United States

Director of Grants
Lauren Ohlin
austin.smith@washoeschools.net

Telephone	7757893435
Fax	775-333-5012
Web	www.washoeschools.net
UEI	DEA6NNBHBTV3
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions top

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☑ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☐ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☐ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☑ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
This project is to improve Washoe County School District's Cyber Forensic capability. Cyber attacks have increasingly targeted K12 organizations and open source tooling offers a poor capability to investigate breaches and collect endpoint artifacts. By improving our cyber forensic capability, WCSD will have an increased capacity to respond to cyber incidents, collect indicators, and share them with partner agencies.

5. How does your project align with the objective selected in Question 2?
Objective 3: Implement security protections commensurate with risk. Investigations are a key component of digital forensics and incident response. This project aligns with the objective by improving our capability to respond to attacks by quickly and accurately investigating attacks and performing root cause analysis. Investigation findings can be shared and quickly accelerate the wider communities' capability to prevent or react to an attack.

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

Ensures that WCSD can investigate compromised systems and identify root causes of cyber intrusion. This will prevent future compromises by allowing systemic analysis and measures to be put in place.

11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

Digital Forensics and Incident Response (DFIR) tooling would allow our organization to investigate breaches, gather indicators, and share them with other agencies.

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

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
The project would be implemented by WCSD's internal IT staff in concert with vendor-provided implementation partners. The project would involve a current needs assessment, solution formation, compare potential options, and technical implementation and integration with existing WCSD systems.

9. Describe, in a few sentences, the desired outcome(s) of your project.
Implement a cyber forensic system to improve WCSD's ability to investigate cyber breaches.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service

assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
This project could be expanded to include additional functions or capabilities of the forensic software.

14. Is this project shareable or deployable to other jurisdictions?
Select “Yes” if the project supports multiple jurisdictions (e.g., multiple cities). Select “No” if the project primarily supports a single entity.

☐ Yes

☑ No

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

☑ Build

☐ Sustain

16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project.
This project was not a previously awarded SLCGP project.

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

☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☐ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

☐ Training - Content and methods of delivery that comply with relevant training standards

☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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
Cyber Forensic Infrastructure	Infrastructure required for cyber forensic investigations includes software, hardware, and licensing	1	$ 60,000.00	$ 60,000.00	In order to investigate systems in the event of a cyber attack, this system would be used to perform in-depth analysis of an intrusion.	The organization would need to support the software internally.	Software, Forensic	05HS-00-FRNS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	$ 60,000.00	$ 60,000.00				

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)	☑	FY 22 Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy Procurement Procedure
Milestones download template	☑	Forensic System Milestones

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

Application ID: 485352

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	Washoe County School District
	Project Name:	WCSD Email Security System
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Software	45 days after award
2	Receive license	60 days after award
3	Perform installation with vendor support	90 days after award
4	Ensure operation and validation	120 days after award
5	Review system usage and confirm operation	150 days after award
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ *and*

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Washoe County School District

WCSD Disaster Recovery

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

$ 250,000.00 Requested

Submitted: 10/24/2024 9:36:13 AM (Pacific)

Project Contact
Austin Smith
austin.smith@washoeschools.net
Tel: 7757893422

Additional Contacts
lohlin@washoeschools.net,radrake@washoeschools.net

Washoe County School District

425 E 9th St
Reno, NV 89512
United States

Director of Grants
Lauren Ohlin
austin.smith@washoeschools.net

Telephone	7757893435
Fax	775-333-5012
Web	www.washoeschools.net
UEI	DEA6NNBHBTV3
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
□ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.

☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☑ Objective 3: Implement security protections commensurate with risk.
☐ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.
☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☑ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
☐ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
☑ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)
☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
This project is to improve Washoe County School District's Disaster Recovery infrastructure. Cyber attacks have increasingly targeted K12 organizations with destructive cyber attacks (data wipers, ransomware). By improving our backup infrastructure, WCSD will have an increased capability to respond to cyber incidents and quickly restore services.

5. How does your project align with the objective selected in Question 2?
Objective 3: Implement security protections commensurate with risk. Destructive cyber attacks are increasingly common amongst K12 organizations. This project aligns with the objective by improving our capability to respond to destructive attacks by quickly and reliably restoring data and services.

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

Ensures the confidential storage of backups and enables rapid recovery in the event of a destructive cyber attack.

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.

Disaster Recovery specifically targets high value assets belonging to WCSD. Improving the Disaster Recovery system will enhance our capability to restore systems supporting school district operations.

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.

Destructive cyber attacks can only impact victims if there is no valid backup.

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
The project would be implemented by WCSD's internal IT staff in concert with vendor-provided implementation partners. The project would involve a current needs assessment, solution formation, compare potential options, and technical implementation and integration with existing WCSD systems.

9. Describe, in a few sentences, the desired outcome(s) of your project.
Implement a school district-wide disaster recovery system to improve cyber resilience and readiness.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend

ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89502

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

Building out backup infrastructure requires a significant up front capital expenditure (capex). This project could not be reduced due to the size and volume of the data that our agency processes. If we were to pursue a smaller solution, it may not fulfill our storage capacity needs. In contrast, backup and storage infrastructure can continuously expand.

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

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

□ Yes

☑ No

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

☑ Build

□ Sustain

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

This project was not a previously awarded SLCGP project.

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

□ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

□ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

□ Training - Content and methods of delivery that comply with relevant training standards

□ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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
Disaster Recovery Infrastructure	All infrastructure required for data backups, storage, security, and recovery.	1	$ 250,000.00	$ 250,000.00	In order to restore systems in the event of a cyber attack, this system would be used to securely backup, store, and restore data.	This project is tied to a large up front expenditure to acquire the hardware for improved backup infrastructure.	Hardware, Computer, Integ	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	$ 250,000.00	$ 250,000.00				

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)	☑	Audit FY22
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Payroll
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Implementation Plan

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

Application ID: 484936

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

Applicant Name	Washoe County School District
Project Name:	WCSD Disaster Recovery
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	Review existing backup infrastructure	Award date + 0
2	Identify solutions and enhancements	Award date + 30
3	Request purchase approval	Award date + 45
4	Get all approvals	Award date + 90
5	Complete purchase	Award date + 120
6	pilot implementation	Award date + 150
7	production implementation	Award date + 180
8	integration	Award date + 210
9	finalize and complete project	Award date + 240
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Washoe County School District

SUSTAIN WCSD Email Security System

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

$ 275,000.00 Requested

Submitted: 10/31/2024 3:21:20 PM (Pacific)

Project Contact
Austin Smith
austin.smith@washoeschools.net
Tel: 7757893422

Additional Contacts
lohlin@washoeschools.net,radrake@washoeschools.net,radrake@washoeschools.net,lohlin@washoeschools.net

Washoe County School District

425 E 9th St
Reno, NV 89512
United States

Director of Grants
Lauren Ohlin
austin.smith@washoeschools.net

Telephone	7757893435
Fax	775-333-5012
Web	www.washoeschools.net
UEI	DEA6NNBHBTV3
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to

cybersecurity incidents and ensure continuity of operations.

□ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

☑ Objective 3: Implement security protections commensurate with risk.

□ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.

□ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

□ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

□ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

□ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

□ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.

□ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

□ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

□ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

□ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

☑ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

□ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

□ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

☑ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

□ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

□ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
This project will sustain licensing for email security software that Washoe County School District (WCSD) will use to protect internal and external email traffic. Email security is critical because it is the main avenue for cyber attacks to occur with over 91% of cyber attacks starting with a phishing email. This project will provide licensing and a vendor-supported implementation. From a technical perspective, this will accomplish Objective 3: "Implement security protections commensurate with risk" because it supports secure email and prevents bad actors from gaining a foothold in the environment using targeted phishing. WCSD is a large, geographically-dispersed public entity. However, the internal IT department has only one dedicated staff member supporting email security. Implementing this system will prevent malicious email and also free up the existing personnel to implement more advanced cybersecurity needs. This software is necessary to support WCSD's daily business operations, and provide a safe and secure learning environment for our 62,000 students, including those in rural areas of Washoe County.

5. How does your project align with the objective selected in Question 2?
This project aligns with Objective 3: "Implement security protections commensurate with risk" because email is the most common initial vector for cyber breaches. Industry statistics demonstrate that 91% of breaches start with a phishing email. Email security also protects against other forms of attack like business email compromise or conventional fraud that cause major losses to all entities. WCSD currently relies on vendor-provided email security solutions that do not use advanced techniques to identify and prevent email fraud. This project will greatly improve WCSD's capability to prevent and respond to a breach.

6. How does your project align with the program element(s) selected in Question 3?
This project aligns with the selected program elements as follows:
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." This system will actively monitor, audit, and track network traffic (email/SMTP traffic) as it enters and leaves the WCSD email system. This will allow IT staff to investigate and identify anomalous activity occurring on the system.
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." This system will greatly improve WCSD's ability to prepare for and respond to email-based 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." Modern email security systems integrate with threat intelligence feeds to gather information on threats in other customers' environments. Using an email security suite will directly address cyber risk where it is most likely to damage the District and other state/local agencies.
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." In modern cyber attacks, bad actors typically compromise legitimate accounts before pivoting to other resources. Email is the most common initial entry vector. An email security system will help stop these attacks and feed threat intelligence systems for other state agencies.

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

□ Implement multi-factor authentication.

☑ Implement enhanced logging.

□ Data encryption for data at rest and in transit.

□ End use of unsupported/end of life software and hardware that are accessible from the internet.

□ Prohibit use of known/fixed/default passwords and credentials.

□ Ensure the ability to reconstitute systems (backups).

□ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.

□ Migration to the .gov internet domain.

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
This project will be implemented by WCSD's internal IT staff. Because WCSD's enterprise email system is hosted, we will integrate the environment with a vendor solution that is provided by their isolated cloud environment. This project will primarily be performed by internal staff working in coordination with a vendor to ensure mail flow is not impacted while ensuring their system gains visibility to our organization's email system. This work is performed in a centralized console and does not require on-hands installation of new equipment, systems, or software.

9. Describe, in a few sentences, the desired outcome(s) of your project.
Implement an email security solution to protect all users from internal and external email threats including malware, phishing, and business email compromise.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

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

89502

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

This project will support ingress/egress, as well as intra-organization email security. This is critical because most email threats come from outside the organization, but internal threats, such as business email compromise, come from inside the organization (intra-org). This project will cover all staff and student accounts. Limiting implementation to just staff members, rather than including student accounts, would drastically degrade WCSD's capabilities in the event of a compromise of student accounts.

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

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

☐ Yes

☑ No

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

☐ Build

☑ Sustain

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

FY2022 - "Email Security System"

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

☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information

☐ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure

☑ Equipment - Equipment, supplies, and systems that comply with relevant standards

☐ Training - Content and methods of delivery that comply with relevant training standards

☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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
Email Security Software License	Software licensing for email security product, including cloud portal and vendor support	1	$ 275,000.00	$ 275,000.00	$275,000 is the total cost for this licensing based on current estimates. This item will allow WCSD to implement an integrated email security suite for all accounts and mailboxes. Email compromise is a common vector for bad actors and often results in financial loss for victims, as well as serving as a springboard to compromise other organizations. If one entity in the State of Nevada gets compromised and they regularly work with others, they can serve as an avenue to compromise other organizations.	WCSD will sustain this project through multiple mechanisms. This project will result in reallocated budget priorities and ensure that the level of continued support for these products are necessary. WCSD will potentially switch to other products due to cost savings.	Applications, Software AS	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	$ 275,000.00	$ 275,000.00				

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)	☑	FY22 Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll
Procurement Policy	☑	Procurement Policy Procurement Procedure
Milestones download template	☑	Email Security milestones

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

Application ID: 485374

Applicant Name	Washoe County School District
Project Name:	SUSTAIN - Email Security System
Project Funding Stream:	FY 2024 SLCGP

	Milestone Description*	Date of Expected Completion
1	Solicit competetive quotes	date of award + 30
2	get board of trustees approval	date of award + 90
3	complete purchase	date of award + 120
4	complete installation and validation	date of award + 150
5	begin monitoring	date of award + 151
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 11/1/2024

Washoe County Sheriff's Office

WCSO 2024 Cybersecurity

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

$ 309,495.81 Requested

Submitted: 10/31/2024 3:16:47 PM (Pacific)

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

Additional Contacts
svanderwall@washoecounty.gov

Washoe County Sheriff's Office

911 Parr Blvd
Reno, NV 89512
United States

Sheriff
Darin Balaam
sogrants@washoecounty.us

Telephone	7753283013
Fax	
Web	
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.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.
☑ Yes
☐ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
☑ Yes
☐ No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the 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.
☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2024 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Division of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

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

2. There are four (4) objectives for FY 2024 SLCGP. Please select the objective with which your project most closely aligns.
☐ Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☐ Objective 3: Implement security protections commensurate with risk.
☑ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

3. Please select which of the SLCGP program elements your project addresses.
Projects may align with more than one element.
☐ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

☐ 2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☐ 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

☐ 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

☑ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.

☐ 6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

☐ 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

☐ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

☐ 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

☐ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

☐ 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

☐ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

☐ 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

☐ 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
The Northern Nevada Cyber Center is requesting equipment and training to ensure personnel are appropriately trained in cybersecurity, increase their ability to respond to cybersecurity threats, and decrease vulnerability to these threats.

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?
Primary Objective: Personnel Cybersecurity Training

Training Courses:
- Cybersecurity Risk Assessment: Equips managers with skills to assess and mitigate risks, ensuring compliance.
- Foundations: Computers, Technology & Security: Builds foundational knowledge for two members, progressing to advanced cybersecurity concepts.
- Introduction to Cybersecurity: Covers network attacks, malware, and cryptography for one member.
- Security Essentials: Teaches core defense skills for networks, endpoints, and cloud security.
- Practical OSINT: Trains three experts in OSINT for law enforcement and intelligence work.
- Reverse-Engineering Malware: Provides three experts with tools to analyze malware targeting Windows systems.
- Outcome: Enhances Cyber Center personnel’s skills to effectively handle cybersecurity risks.

Objective: Implementing Security Protections Commensurate with Risk

Cellebrite Software:
- Inseyets & Inseyets Unlocks: Provides digital forensics capabilities for extracting and managing data, supporting cybersecurity threat response.
- Guardian: Manages digital evidence securely and efficiently.
UPS Replacement: Upgrades power supply for the Cyber Center’s server, ensuring data integrity and system availability.
Risk-Based Security Enhancements: Strengthens system resilience through monitoring, encryption, and secure evidence management.

Overall Alignment:

Training and infrastructure: Training develops essential cybersecurity expertise, and new equipment bolsters system resilience, directly addressing the grant's primary and additional objectives.

% 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.

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

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Project Implementation and Execution:

1. Training Implementation:
• Training Provider:
Instructors from the training vendor will facilitate the training courses.
• Participants:
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.

2. 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.

3. 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:
A Grant Manager from the Washoe County Sheriff's Office will oversee the project, ensuring compliance with grant requirements and proper allocation of funds.

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.

9. 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.

10. FY 2024 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2024 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)
☐ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

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

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

14. Is this project shareable or deployable to other jurisdictions?
Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
☑ Yes
☐ No

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

16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project.
Potentially FY24 SLCGP, which as of this submission date, has not been awarded yet.

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
☐ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
☐ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
☑ Equipment - Equipment, supplies, and systems that comply with relevant standards
☑ Training - Content and methods of delivery that comply with relevant training standards
☐ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

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 - ($8221.05/License - Total = $57,547.35), 150 Inseyets Unlocks - ($228.38/Unlock - Total = $34,257.00), 7 Guardian Licenses ($10,667.78/License - Total = $74,674.46)	1	$ 166,478.81	$ 166,478.81	The purchase of Cellebrite software and Cellebrite Guardian supports the project by enabling the Cyber Center to monitor, audit, and track network traffic and device activities, enhancing its oversight capabilities. Additionally, the Cellebrite tools bolster the Center's resilience, preparation, and response efforts, while Guardian specifically enhances secure evidence management, fostering trust in online services. These tools also improve the Center's ability to share cyber threat information securely with state and local entities, while targeted training and software extend cybersecurity support to rural areas, ensuring equitable access and participation.	The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on	Software, Forensic	05HS-00-FRNS

the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities.

Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives.

Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services.

By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing

						financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada.		
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	The Liebert EXS UPS enhances cybersecurity operations by providing reliable backup power, ensuring continuous monitoring and response capabilities. This supports Cellebrite software's role in tracking network activity and reinforces system resilience alongside personnel training for effective threat response. Together with secure evidence management by Cellebrite Guardian and the extension of cybersecurity services to rural areas, the UPS helps maintain robust, uninterrupted cybersecurity operations across northern Nevada.	This is a one-time purchase and would not need to be renewed.	Components, Networking, D	04HW-03-NETD
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		2	**$ 206,478.81**	**$ 206,478.81**				

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 $8,951, GOSI Certification $1,028)	3	$ 9,979.00	$ 29,937.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of	NO

					workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities. Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives. Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services. By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada. "	
1 - Training Course Travel	San Diego, Start May 5, 2025 - Airfare ($450 = $1,350), Lodging ($194 x6 Nights = $3,492), M&IE 5 Days ($74 + 2 Travel Days @ $55.50 = $1,443), Misc Travel $194 x6 Nights	3	$ 2,270.00	$ 6,810.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities. Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives. Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services. By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the	NO

						project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada. "	
2 - Training Coure Registration	Performing a Cybersecurity Risk Assessment - On Demand - (Registration $3,575)	1	$ 3,575.00	$ 3,575.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities. Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives. Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services. By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada. "	NO
3 - Training Course Registraion	Foundations: Computers, Technology, & Security - Web-Based - (Registration $3,171, GFACT Certification $399 x2)	2	$ 3,570.00	$ 7,140.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities. Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives. Revenue Generation Strategies: Investigating revenue generation strategies, such as providing	NO

						digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services. By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada. "	
4 - Training Course Registration	Introduction to Cyber Security - On Demand - (Registration $7,801, GSIF Certification $1,028)	1	$ 8,829.00	$ 8,829.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities. Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives. Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services. By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada. "	NO
5 - Training Course Registration	Reverse-Engineering Malware: Malware Analysis Tools and Techniques - (Registration $8,951, GREM Certification $1,028)	3	$ 9,979.00	$ 29,937.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities.	NO

						Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives. Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services. By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada. "	
5 - Training Course Travel	Las Vegas, Start Sep 4, 2024 - Airfare ($450 = $1,350), Lodging ($194 x6 Nights = $3,492), M&IE 5 Days ($74 + 2 Travel Days @ $55.50 = $1,443), Misc Travel $194 x6 Nights	3	$ 2,270.00	$ 6,810.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external funding sources. Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities. Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives. Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services. By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada. "	NO
6 - Training Course Registration	Security Essentials - Network, Endpoint, and Cloud - On Demand - (Registration $8,951, GSEC Certification $1,028)	1	$ 9,979.00	$ 9,979.00	The purchase of training courses is integral to enhancing the Cyber Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively. Courses like these support continuous vulnerability assessment and threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments.	"The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace hardware, and to maintain proficiency through periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of strategies: Budget Allocation within Participating Agencies: As the project progresses and agencies reap the benefits of enhanced capabilities, it may be feasible to allocate funds from their respective budgets to cover ongoing expenses associated with license renewals, hardware updates, and occasional training updates. This approach ensures continued access to essential tools and resources without relying solely on external	NO

funding sources.

Grant Renewal or Extension: Depending on the success and impact of the project, there may be opportunities to seek grant renewals or extensions to cover ongoing expenses beyond the initial funding period. This could involve applying for additional funding from the Department of Emergency Management or other relevant grant-making entities, highlighting the project's continued importance in addressing cybersecurity threats and protecting communities.

Partnerships and Collaborations: Exploring partnerships with other agencies, organizations, or industry stakeholders could provide avenues for cost-sharing or securing additional funding support for ongoing expenses. Collaborative efforts could include sharing resources, leveraging collective purchasing power for software licenses, or jointly applying for grants aimed at sustaining cybersecurity initiatives.

Revenue Generation Strategies: Investigating revenue generation strategies, such as providing digital forensic services on a contractual basis, could potentially generate additional funds to offset ongoing expenses. This approach would require careful consideration of legal and ethical considerations, as well as market demand for such services.

By implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing financial obligations beyond the initial grant funding period. This ensures the longevity and effectiveness of the project's efforts in enhancing cybersecurity capabilities and protecting against cyber threats in Northern Nevada.
"

			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
		17	$ 50,451.00	$ 103,017.00	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)	☑	SAM.gov Reg Single Audit
Travel Policy	☑	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: 485357

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com
©2002-2024 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	WCSO
	Project Name:	Northern Nevada Cyber Center
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
1	BCC Approval - Receive BCC approval to utiliz	October 1 2025
2	Equipment/Hardware - Purchase and install r	November 1 2025
3	Equipment/Software - Renew/Upgrade Celle	June 8 2026
4	Training - Identify training needs; develop tra	October 1 2027
5	Close Out	End of Project
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project