

Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)

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

Deadline: 11/1/2024

City of Las Vegas Southern Nevada Cyber Defense Project

Soutr	iern Nevada Cyber Defense Project	
Jump to: Pre-Application	Application Questions Line Item Detail Budget Document Up	<u>ploads</u>
\$ 649,704.00 Requested	City of Las Vegas	
Submitted: 10/22/2024 4:28:18 PM (Pacific)	495 S. Main Street Las Vegas, NV 89101	Telephone 7022290313 Fax
Project Contact	Mayor	Web www.lasvegasnevada.gov UEI HJS3TZHWWJX5
Carolyn Levering <u>clevering@lasvegasnevada.gov</u>	Carolyn G. Goodman	SAM Expires7/8/2020
Tel: 702220313	cievering@iasvegasnevada.gov	
Additional Contacts none entered		
Pre-Application top		
1. Is your organization one of the following types of entities?: Councouncil of government, regional government entity, agency or instruauthorized tribal organization. Be advised that state agencies receiving SLCGP funds will have to obtaive yes. No 2. All funds granted under the State and Local Cybersecurity Grant	Imentality of a local government, rural community, uninc in consent for their project from local jurisdictions. A template	orporated town or village, or other public entity, tribe, or for obtaining this consent will be provided.
this goal? (If not, the project is not eligible for SLCGP funding). ✓ Yes □ No		
 In order for your application to be considered, you must attend of do not send representation to the required meetings, your application Meeting dates are to be determined and will be communicated to SLCGiv I understand and agree. 	on will not be considered.	ecurity Task Force. This is a requirement of the grant. If you
4. All procurement is required to be compliant with Nevada Revised legal opinion, locals may NOT use NRS 332.115 because it has been justification).** All procurement must be free and open competition, women's business enterprises, and labor surplus area firms per 2 C provide a preference for the purchase, acquisition, or use of goods be pre-approved in writing by the Division of Emergency Managemy You may view FEMA's written legal opinion on NRS 332.115, along with I understand and agree.	n determined that NRS 332.115 is less restrictive than 2 C Applicants are also required to follow the socioeconomic LF.R. Part 200.321. All non-federal entities should also, to products, or materials produced in the United States, pe ent (DEM) in advance of the procurement.	.F.R. Part 200 (see Resources section for further cateps in soliciting small and minority businesses, the greatest extent practicable under a federal award, or 2 C.F.R. Part 200.322. Any sole source procurement must
 Supplanting is prohibited under this grant. Supplanting occurs we expected to be available) to fund that same activity. I attest that funding for this project does not currently exist within our age. 		r an activity because federal funds are available (or
6. Entities applying as a subgrantee must meet a 30% cost share reI understand and agree.	quirement for FY 2024 SLCGP. Please acknowledge your	understanding and agreement of this requirement.
 Each jurisdiction must complete its own application. The submitt Subgrantees may not pass through or subgrant funds to other age: I understand and agree. 		Vithout an application, DEM is unable to issue a grant.
8. Subrecipients (i.e., agencies receiving this funding through the N I understand and agree	levada Division of Emergency Management) may not use	this funding to administer their own subawards.
Application Questions top		
I. Is this agency considered a rural area (an area encompassing a p If your agency is not considered a rural area, but your project will suppor Nevadans.		what percentage of your project will directly benefit rural
2. There are four (4) objectives for FY 2024 SLCGP. Please select th ☑ Objective 1: Develop and establish appropriate governance structure:	, , , , , ,	plans, to improve capabilities to respond to cybersecurity
incidents and ensure continuity of operations. Objective 2: Understand their current cybersecurity posture and areas		
☐ Objective 3: Implement security protections commensurate with risk.		อแนงเนเอน สออตออเทตาแอ.
 Objective 4: Ensure organization personnel are appropriately trained in 	n cybersecurity, commensurate with responsibility.	

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 or 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.)
	12. Leverage cyclesecurity services oriented by Cloxi. (See Application Question 10 for futner details on triese 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.
	Describe your project in detail.
Wh The to n	At would you like to do? Why? How does this project improve cybersecurity protection for your agency? 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 ininimizing 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 pened, giving us little time to prepare/safeouard our organization.
and from Dar Dar Out	ution: 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 insymized 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 in 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, ktrace 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 ktrace can effectively facilitate the connection to the Unified Cloud Master we aim to promote. come: 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 preemptivel tect against threats that have not yet hit their systems and infrastructure.
Dar thre gov Cur acre Fute sub ave	Now does your project align with the objective selected in Question 2? It ktrace Al-driven approach to Cyber-Threat Detection autonomously monitors traffic detecting and investigating anomalous or suspicious behavior indicating potential cyber relates. This proactive approach allows for rapid containment of incidents and provides valuable insights for strengthening overall cybersecurity posture, ultimately reducing these participating emment agencies exposure to cyber risks and cost. Tent 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 best the agencies and spot abnormal behavior proactively. The 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 Al to identify the 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 range 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), improves efficiencies (5-10% reduction of actionable insights).
Bus opti	improves enticencies (3-10% reduction in action later insignities), insigness Outcomes: Save resources (Al 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 mized 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 tinuity (incident closure rate improved by 20%).
	How does your project align with the program element(s) selected in Question 3? e to space limitations in this application, please refer to response to this question in the Document Uploads section.
	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 energy in hidirectional charing between CISA and SLT actition in other relevant time frames to drive down other risk.
	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.
Des The cyb	Describe, in detail, how, and by whom, the proposed project will be implemented. Scribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work. 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 the er 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 aring from and how they can best prepare.
The hav sen	Describe, in a few sentences, the desired outcome(s) of your project. © City of Las Vegas would like to create a threat intelligence ecosystem through the implementation of Darktrace's Cyber Al network solution. The idea would be that every government entity should e 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 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 ring 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

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/msisac/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

The project to 89101	ocation could be	e different tha	an the su	ub-recipi	nt address.				
Yes, this proje like to reduce	ect with Darktrac visibility, it is as	ce is scalable s simple as re	as it is i	industry a subnets t	nd size agnostic. Da decrease the cover	rktrace can scale age. If a client w	e up or down seamlessly in ac	cordance with the distrib	nded, or the reasons why it cannot. ution of any digital environment. If a client would al appliances to the deployment scope. Scalability eir platform.
	oject shareable if the project sup					Select "No" if the	e project primarily supports a	single entity.	
15. Build or maintains a	Sustain: Select					w capability, o	r the intent of the project is	to close a capability g	ap. Select "sustain" if the project strictly
✓ Build☐ Sustain									
16. If this pro	oject is sustain	ning a previo	ously av	varded S	LCGP project, plea	se provide the	fiscal year and project nam	e of the original projec	t.
✓ Planning☐ Organiza✓ Equipme✓ Training	- Development ation - Individual ent - Equipment, - Content and m	of policies, pl teams, an ov supplies, and ethods of del	lans, pro erall org d system livery tha	cedures anizatior as that co at comply	mutual aid agreeme al structure, and lead nply with relevant sta with relevant training	nts, strategies, a ership at each le andards standards	vel in the structure	olves the collection and	ught for this project. analysis of intelligence and information b improve capabilities to respond to real events
Line Item Detail Budge	et <u>top</u>								
PLANNING COSTS	;								How would your organization sustain this
Planning Cost Name	Line Item Description	Quantity	COSI	l otal the	Application Quest	ions section.	this element tie into the pr		project if grant funding was reduced or discontinued?
Development of Unified View for Threat Intel	Quarterly meetings	1	0.00	0.00 the		entities, recent fir	n to discuss Unified View. This ndings, threat intel from Unifie ase 1		e N/A
				\$					
				\$					
				\$ \$					
				\$					
				\$					
				\$					
				\$					
				\$					
		1	0.00	0.00					
ODC ANIZATION C	0576								
ORGANIZATION Corganizational Cost	Line Item	Quantity	Unit						our organization sustain this project if grant
Name I	Description		Cost \$: a	s described in the A	Application Que	estions section.	funding was	reduced or discontinued?
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
		0	\$ 0.00	\$ 0.00					
EQUIPMENT COS	тѕ								
					Describe how the				
					purchase (s) within this	How would your organization			
Equipment Cost Name	Line Itei ^e Descrip	m Quantit	ty Unit	Cost	element tie Total into the project as described in the Applicatio Questions	sustain this project if gran funding was reduced or discontinued	equipment-list to find AL	ants/tools/authorized-	AEL Number - Search https://www.fema.gov/grants/tools/authorized equipment-list to find AEL info
DETECT_RESPOND/N	letwork Al Powe Detectio			\$ 61.60 62	section. \$ Al Powered 1,561.60 Detection	d One-time purchase	System, Intrusion Detecti		05NP-00-IDPS

			covering 48,000 devices and Response covering 46,500 devices		
Darktrace Deployment Usage Fees	Bundled 1 usage fee	\$ 28,142.40 28,1	42.40 (DCIP-XA) appliance, 2	Recurring costs Hardware, Computer, Integ are shared by participating agencies	04HW-01-INHW
		\$	\$		
		\$	\$		
		\$	\$		
		\$	\$		
		\$	\$		
		\$	\$		
		\$	\$		
		\$	\$		
		\$	\$		
		\$ \$	\$		
		\$ \$	\$		
	2	· · · · · · · · · · · · · · · · · · ·	\$		
	2	649,704.00 649,7			
		,			

TRAINING COSTS

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 tradition discontinued?	o you plan to coordinate this aining with the State Training Officer?
Services/Training/eLearning (Hosted)	Recorded video	\$	0.00		Complimentary online training video modules via N/A Darktrace Customer Portal	N/A
Services/Training/Public	Live online	\$	0.00	0.00	Complimentary access to live online training sessions N/A covering the full breadth of Darktrace's product suite and capabilities.	N/A
Services/Training/Private/Remote	Private remote	\$	0.00		Darktrace will include 2 x free of charge personalized N/A remote private trainings for City of Las Vegas	N/A
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		0 \$	0.00	\$		0
				0.00		

EXERCISE COSTS

-/											
Exercise Cost Name	Line Item Description	Quantity	Unit T	Describe I otal into the pr Questions	how the purchase(s roject as described is s section.) within this eleme in the Application	project	ould your organiz if grant funding w tinued?		Do you plan to co ercise with the S	
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
			\$	\$							
		0	\$ 0.00	\$							0
				0.00							
Total		0	\$ 0.00 \$	0.00							0

Document Uploads \underline{top}

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * Single Audit	
Travel Policy	✓	<u>Travel Policy</u>	

Payroll Policy	Payroll Policy Payroll Narrative
Procurement Policy	✓ Procurement Policy
Milestones download template	✓ <u>Milestones</u>
Administrative Documents *	
	Sole Source Request - Darktrace

 $^{^*\}mbox{\it ZoomGrants}^{\mbox{\tiny TM}}$ is not responsible for the content of uploaded documents.

Application ID: 483219

Become a <u>fan of ZoomGrants</u> on Facebook
Problems? Cortact us at <u>Questions? Excendinates com</u>
2002-2024 Grantshapts com. All rights reserved.
"ZoomGrants' and the ZoomGrants togs are trademarks of Granthrabyst.com, LLC.
Local Effections."

	Applicant Name	City of Las Vegas
		Dartrace - Unified View for Threat Intel - Southern
	Project Name:	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.



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

\$8	40,	000	.00	Req	uested
-----	-----	-----	-----	-----	--------

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

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 prinicipal 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.
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 prinicipal 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
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 prinicipal 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
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 prinicipal 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 could have to revert to manual processes (if they exist) that could drag on for months or not having this is public safety, waste water treatment, and other critical government operations could have to rev
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 prinicipal 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 r
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 prinicipal 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 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 physical defenses failed. The risk of not having this is public safety, waste water treatment, and other critical government operations in a timely fashion
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 principal 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 physical defenses failed. The risk of not having this is public safety, waste water treatment, and other critical government operations ould have to reve
What would you like in do? Why? How does this project improve cybersecurity protection for your agency? Implement a modern backup and disaster recovery platform following 3-2-1 principal 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/offliline 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 ransonware 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. Show 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 physical defenses failed. The risk of not having this is public safety, waste water treatment, and other critical government operations could have to reve

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 hyporevisor 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.

prohi struc costs Pleas	bition does not i	nclude mino ems, or crition Section D.13 anderstanding	r building cal aspect 3 of the FY	modifications no s of a building's 2024 SLCGP NO	cessary to install safety, or otherwi	and connect gra	nt-purchased ed	s of buildings or other physical facilitie: _l uipment that do not substantially affec r useful life of a building). For a full list	t a building's
Cybe and a asset ways exect regist body https annu. Techi MS-IS https	rsecurity and Inf pproval of a grain sees the "health" to enhance secuting continuous ter for these servior your email that "I/www.cisa.gov/ all self-assessme enology Cybersec SAC, during the facility www.cisecurity our agency is alread	rastructure s nt but is a po of of your pub urity in accou of scans of pu vices, email v at you are rec topics/cyber ent designed curity Frame irst year of tl y.org/ms-isa ndy participation	Security A ost-award olicly acce rdance with oblic, station rulnerability rulnerabilit	gency (CISA). For requirementC ssible web appli in hindustry and go less for accessify in a city in a	r these required solver Hygiene Servations by checking overnment best pole services and volument of the SLGCP. If the SLGCP, if	ervices and mem vices— Web Appling for known vulr ractices and stan ulnerabilities. Thi bject line "Reques for more informatices. —Nationwide cybersecurity pr ISAC. Entities and annually. For the e Cybersecurity Re	berships, pleas cation Scanning nerabilities and vidards. Vulneral is service provice sting Cyber Hygi tion, visit CISA's e Cybersecurity rograms. It is ba d their subrecipi more information	pate in a limited number of free service enote that participation is not required is an "internet scanning-as-a-service." weak configurations. Additionally, CISA billty Scanning evaluates external netwises weekly vulnerability reports and adiene Services – SLCGP" to get started. Cyber Hygiene Information Page: Review (NCSR)- The NCSR is a free, as sed on the National Institute of Standar ents should complete the NCSR, admirin, visit Nationwide Cybersecurity Review (NCSR) and the National Institute of Standar ents should complete the NCSR, admirin, visit Nationwide Cybersecurity Review (NCSR) and the Nationwide Cybersecurity Revi	for submission This service Can recommend ork presence by hoc alerts. To Indicate in the monymous, ds and histered by the ew (NCSR)
12. Pi	roject is awarded rovide the 5-digit roject location col								
		loablo? Can	any nart c	f it ha raducad a	ovnandad? Dasa	riho tho wave in t	which the projec	ct can be reduced or expanded, or the r	oacone why it
canno With a	ot. a competitive proc	ess it is likely	that the pro	oject costs would b	•	ied dollar amount is		plete solution. The backup schedule and a	•
Selec □ Y	es					t "No" if the project	primarily suppor	ts a single entity.	
▽ N	lo								
	ct strictly mainta					pability, or the int	ent of the projec	ct is to close a capability gap. Select "s	ustain" if the
	ustain								
16. If N/A	this project is su	ıstaining a pı	reviously	awarded SLCGP	project, please pr	ovide the fiscal ye	ear and project I	name of the original project.	
□ P ir □ C ☑ E □ T □ E	lanning - Develop Information Organization - Indiv quipment - Equipr raining - Content a	ment of policion ridual teams, a ment, supplies and methods o	es, plans, p an overall c s, and syste of delivery t	orocedures, mutual organizational structures orms that comply with research	aid agreements, st ture, and leadership th relevant standard evant training stand	rategies, and other o at each level in the ds dards	r publications; also	which funding is being sought for this o involves the collection and analysis of integration in the collection and analysis of integration in the collection and identify opportunities to improve capacity.	elligence and
Line Item Deta	il Budget <u>top</u>								
PLANNING (Planning Cost	Line Item	Quantity	Unit Tot			rithin this elemen		How would your organization sustain	
Name	Description		Cost	project as des	cribed in the Appl	ication Questions	s section.	grant funding was reduced or discont	inued?
				\$					
				\$					
				\$					
				\$					
				\$ \$					
				\$					
				\$					
				\$ \$					
				\$					
		0	0.00	\$ \$					
		U	0.00						
ORGANIZAT									
Organizationa Name	LUST LINE ITEM		11,		how the sureling	o(c) within this - !	amont tie late th	o How would your argent-sties suct-	in this project if
	Description	on Quan	tity Cos			e(s) within this ele Application Ques		e How would your organization susta grant funding was reduced or disco	
		on Quan	Cos	t sproject a					
		on Quan	Cos	t project a					

			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
		0 :	\$ 0.00	\$					
				0.00					
EQUIPME	ENT COSTS								
				Describe					
				how the					
				purchase (s) within	How would				
				this	your				
Equipment	Line Item Quantity			element tie	organization sustain this	L Name - Sear	ch	AEL Number -	Search
Cost Name	Line Item Quantity Description	Unit Cost		into the project as described in the Application Questions	funding was reduced or	ps://www.rem uipment-list to	a.gov/grants/tools/auti find AEL info	equipment-list	search ma.gov/grants/tools/authoriz to find AEL info
				section.					
Backup Solution	solution, to	\$ 40,000.00 840	,000.00	The is the complete solution.	This funding is Ap for a complete solution.	plications SAAS	S,Hardwar	04AP-11-SAAS	04HW-01-INHW
	be determined by RFP								
	•	\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
	1	\$	\$						
	8	40,000.00 840	,000.00						
'R AINING	G COSTS								
raining	Line Item Quan	tity Unit To	tal elen	nent tie into	e purchase(s) with the project as des stions section.	hin this cribed in the	How would your orga project if grant funding discontinued?	anization sustain this ng was reduced or	Do you plan to coordinate training with the State Train Offic
		\$	\$						Oille
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		\$	\$						
		0 \$ 0.00	\$						
		0.	.00						
KERCIS	E COSTS				he nurchase(s) wi				Do you plan to coordinate

Exercise Line Item Cost Name Description Quantity Unit Cost Unit Cost Describe how the purchase(s) within this project as described in the Application Questions section. How would your organization sus project if grant funding was reduced discontinued?

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?

Ψ	Ψ
\$	\$
\$	\$
•	Φ.

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

Document Uploads top

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

 $^{^{\}star}\textit{ZoomGrants}^{\textsc{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 485243

Become a fain of ZoomGrants 1" on Facebook
Problemer Contact us at Questions RoomGrants com
Problemer Contact us at Questions RoomGrants com
Victoria Contact us at Questions RoomGrants
Victoria Contact us de Victoria Vi

	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



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	Rec	uested
----	-----	------	-----	-----	--------

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.

Ubjective 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.
S. Ensure that the state of local governments within the state, adopt and use best practices and methodologies to enhance cycles ecuny. S. Ensure that the state of 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.
A Describe your project in detail
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

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.

and bring them into the Patching, Scanning, Intune, AV fold.

	I understand and a	igree				
	Cybersecurity and In and approval of a grassesses the "health ways to enhance see executing continuou register for these ser body of your email th https://www.cisa.gov annual self-assessm Technology Cyberse MS-ISAC, during the https://www.cisecuri our agency is alree	frastructure ant but is a p " of your pu urity in acces s scans of p vices, email aat you are ro //topics/cybe ent designe curity Fram first year of ty.org/ms-is ady participa ot yet signed	Security ost-awa blicly acordance rublic, stavulneral equestiner-threated to mea ework at the awar ac/servicing in the	Agency rd require recessible with indu atic IPs fo collity_info g this ser s-and-adv sure gapend is sport d/subawates/ncsr (e Cyber Hy	Il SLCGP recipients and subrecipients are required to parti (CISA). For these required services and memberships, pleatementCyber Hygiene Services Web Application Scanning web applications by checking for known vulnerabilities and stry and government best practices and standards. Vulner or accessible services and vulnerabilities. This service prove @ cisa.dhs.gov with the subject line "Requesting Cyber Hyvice as part of the SLGCP. For more information, visit CISA risories/cyber-hygiene-servicesNationwide Cybersecurity and capabilities of a SLT's cybersecurity programs. It is be as and capabilities of a SLT's cybersecurity programs. It is be as a property of the MS-ISAC. Entities and their subrecified period of performance and annually. For more informaticisecurity.org). Giene Services and Nationwide Cybersecurity Review (NCSR), but giene Services or Nationwide Cybersecurity Review (NCSR), but	use note that participation is not required for submission on its an "internet scanning-as-a-service." This service it weak configurations. Additionally, CISA can recommend ability Scanning evaluates external network presence by ides weekly vulnerability reports and ad-hoc alerts. To giene Services – SLCGP" to get started. Indicate in the 's Cyber Hygiene Information Page: y Review (NCSR) – The NCSR is a free, anonymous, assed on the National Institute of Standards and pients should complete the NCSR, administered by the ion, visit Nationwide Cybersecurity Review (NCSR)
	12. Provide the 5-dig <i>The project location co</i> 89501					
	cannot. Additional money can be	oe added to e	xtend the	length of	reduced or expanded? Describe the ways in which the projectime the licenses are valid for to allow for long tracking and reducutside of the core endpoint and SaaS checks.	•
	Money can be cut and	would reduce	the valid	ity period	the scanning agents are available for to track risks. Or modules for	or SaaS could be cut and only endpoint tracking implemented.
	14. Is this project sha Select "Yes" if the proj ☐ Yes ☑ No				jurisdictions? is (e.g., multiple cities). Select "No" if the project primarily supp	orts a single entity.
	15. Build or Sustain: project strictly maint ✓ Build ☐ Sustain				ocuses on starting a new capability, or the intent of the proj sting/current level.	ect is to close a capability gap. Select "sustain" if the
	16. If this project is s	ustaining a _l	orevious	ly awarde	ed SLCGP project, please provide the fiscal year and projec	t name of the original project.
Line Item	✓ Equipment - Equip☐ Training - Content	ment, supplie and methods	es, and sy of delive	stems tha	tional structure, and leadership at each level in the structure t comply with relevant standards aply with relevant training standards wledge of plans, allow members to improve their own performan	ce, and identify opportunities to improve capabilities to respond
	ING COSTS G Cost Line Item Description	Quantity	Unit -		cribe how the purchase(s) within this element tie into the ect as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				\$, , , , , , , , , , , , , , , , , , , 	gram ramaning man recursor on an accommission
				\$		
				\$		
				\$		
				\$ \$ \$		
				\$ \$		
				\$ \$ \$ \$ \$ \$ \$ \$ \$		
				\$ \$ \$ \$ \$ \$ \$ \$ \$		
				\$ \$ \$ \$ \$ \$ \$ \$ \$		
		0	0.00	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		
		0	0.00	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		
ORGAN	IIZATION COSTS	0	0.00	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		
Organiza	ational Cost Line Item	Qua	ntity (\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Describe how the purchase(s) within this element tie into project as described in the Application Questions section.	
		Qua	ntity (\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Describe how the purchase(s) within this element tie into project as described in the Application Questions section.	
Organiza	ational Cost Line Item	Qua	ntity (\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		
Organiza	ational Cost Line Item	Qua	ntity (\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		
Organiza	ational Cost Line Item	Qua	ntity (\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		

				\$	\$					
				\$	\$					
				\$	\$					
				\$	\$					
				\$	\$					
				\$	\$					
				\$	\$					
			0	\$ 0.00	\$					
					0.00					
EQUIPME	NT COSTS	3								
					Describe					
					how the					
					purchase	How would				
					(S) WILLIIII	your				
					this element tie	organization	AEL Name - Sea	rch	AEL Number -	Search
Equipment Cost Name	Line Item	Quantity Uni	t Cost		into the	sustain this	https://www.fem	a.gov/grants/tools/authorized-	https://www.fe	ma.gov/grants/tools/authorized- to find AEL info
Cost Name	Description	•			project as	funding was	equipment-list to	find AEL info	equipment-list	to find AEL info
					described	reduced or				
					in the Application	discontinued?	•			
					Application Questions					
					section.					
Vulnerability	Scanner to	1	\$	\$		An additional	Applications, SAA	AS	04AP-11-SAAS	
and SaaS	include VM	250,0	000.00 250	0,000.00		funding request				
	for IoT and Network					would submitted				
	devices					through the				
	without					budget				
	agents,					process.				
	SaaS API									
	connections to validate									
	policy best									
	practices or									
	exposed data, web									
	application									
,	vuln									
	scanner,									
	external									
	exposure scanning,									
	and									
	benchmark									
	compliance.									
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
		1 250 (\$ 100 00 350	\$ 000 00						
		250,0	00.00 250	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,						
TRAINING	COSTS									
Training	Line Item	0	Unit _	Des	cribe how th	ne purchase(s)	within this	How would your organization		Do you plan to coordinate this
Cost Name		n Quantity	Cost	otal elem	nent tie into	the project as o estions section.	described in the	project if grant funding was i discontinued?	reduced or	training with the State Training Officer?
			¢	\$ \$	ncadon wde	ວດບາເວ ວະບົດປົກ.		aiscommutu :		Officer?
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
		0	\$ 0.00	\$						0
				.00						

EXERCISE	COSTS					
Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Describe how the purchase(s) within Total element tie into the project as describe Application Questions section.	this How would your organization bed in the project if grant funding was re discontinued?	
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		0	\$ 0.00	\$		0
				0.00		
Total		0	\$ 0.00 \$	50.00		0

Document Uploads top

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

 $^{^{\}star}$ ZoomGrants $^{\tau_{M}}$ is not responsible for the content of uploaded documents.

Application ID: 485171

Become a <u>fan of ZoomGrands</u>** on Facebook Problema** Contact us at <u>Questions WoomGrands com</u> <u>Contact us at Questions WoomGrands com</u> <u>"ZoomGrands** and the ZoomGrands top on texthemate or Grand-Analyst com</u>, LLC. <u>Locolal Browners</u>

	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



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: <u>Pre-Application</u> <u>Application Questions</u> <u>Line Item Detail Budget</u> <u>Document Uploads</u>

¢	581	875	nn	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

JEI 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.

Dijective 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 applied of the coordinate strategies to address the state should be applied to the coordinate strategies to address the state should be applied to the coordinate strategies to address the state should be applied to the state should be a
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 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

enhar contific service you a adviss capaat the M and a are service you. It is a service you a adviss capaat the M and a are service you are service you are service you will be stricted. If you will be serviced you will be serviced you will be you	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									
PLANNING O			Unit ,	Desc	cribe how the purchase(s) within this element tie into the How would your organization su	stain this project if grant				
Name	Description	Quantity	Cost		ect as described in the Application Questions section. funding was reduced or disconti					
				\$						
				\$						
				\$						
				\$						
				\$						
				\$ \$ \$ \$						
				\$ \$ \$ \$						
				\$ \$ \$ \$ \$ \$						
			0.00	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$						
		0	0.00	\$ \$ \$ \$ \$ \$						
ORGANIZAT	ION COSTS	0		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$						
ORGANIZAT Organizational Cost Name		0 Quantity		\$ \$ \$ \$ \$ \$ \$ 0.00	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?				
Organizational	Line Item	Quantity	Unit Cost \$ 175.00 2	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Application Questions section.	organization sustain this project if grant funding was reduced or				
Organizational Cost Name	Line Item Description Blended average of Project management	Quantity	Unit Cost	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Application Questions section. 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	organization sustain this project if grant funding was reduced or discontinued? Reduce funding to other				

\$ \$ \$

					\$	\$					
					\$	\$					
					\$	\$					
					\$	\$					
					\$	\$					
					\$	\$					
			125		\$	\$					
				1/5.	00 21,87	5.00					
EQUIPME	NT COSTS										
Equipment Cost Name	Line Item Description	Quantity	Unit C	ost	Tot	project as	How would your organization sustain this project if grant funding was reduced or discontinued?	equipment-list			Search ema.gov/grants/tools/authorized- t to find AEL info
						section.					
Professional Services	Implementation services configuration and integrations for active directory and enterprise email and productivity systems.		100,000	\$ 0.00 1		\$ Installation and 0 configuration of digital forensics integrations.		Consulting Servi	ces	21GN-00-CNS	Т
Managed Services Subscription	3-year SaaS Infrastructure, Storage, Software and Managed Data Security and Forensic Services		460,000	\$ 0.00 4		00 best practices and methodologies to enhance cybersecurity through use of digital	to other district priorities.	Software as a S	ervice	04AP-11-SAA\$	5
						forensics.					
				\$		\$					
				\$		\$ \$					
				\$		\$					
				\$		\$					
				\$		\$					
				\$		\$					
				\$		\$					
				\$		\$					
				\$		\$					
				\$		\$					
		2		\$ \$		\$ \$					
			560,000		560,000.0						
TRAINING	COSTS										
Training	Line Item		., Un	:4	Desc	cribe how the pu	ırchase(s) with	n this element	How would your organization	sustain this	Do you plan to coordinate this
	Description	Quanti	ity Cos			to the project a	s described in t	he Application	project if grant funding was rediscontinued?	educed or	training with the State Training
	•			<u></u>		stions section.			aiscontinuea?		Officer?
				\$ \$	\$						
				\$	\$						
			(\$	\$						
				\$	\$						
				\$	\$						
				\$ \$	\$						
				Ф \$	\$						
				\$	\$						
			(\$	\$						
				\$	\$						
				\$	\$						
				\$.n	\$						0
			0 \$ 0.0		\$ 0.00						U
EXERCIS	E COSTS										
Exercise	Line Item Description	Quant		nit ost	Total tie i		as described in		How would your organization project if grant funding was r 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
1		

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required?	Attached Documents * Audit Report
Travel Policy	✓	<u>Travel Policy</u>
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	Milestones

 $^{^{\}star}\textit{ZoomGrants}^{\, \textsc{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 484819

Become a fan of ZoomGrants ¹¹⁰ 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:	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		36 months after award
7		
8		
9		
10		

^{*}Please add additional rows as necessary for your project



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.

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.
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. ✓ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state. ✓ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state. ✓ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state. ✓ 16. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state. ✓ 16. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state. ✓ 16. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state. ✓ 16. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state. ✓ 16. Ensure adequate access to 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 tinning 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 Internet stays functional and helps ensure continuity of operations for instruction in CCSD. Keeping the District Internet 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

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

capabilit the MS-IS	requesting this es/cyber-hygier ties of a SLT's c SAC. Entities ar	bility_info@ service as ne-service: ybersecur nd their su	© cisa.d part of sNation ity prog brecipie	accessi hs.gov v the SLG onwide grams. It ents sho	nd government best practices and standards. Vulnerability Scanning evaluates external network presence sible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To re with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of GCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber Cybersecurity Review (NCSR)-– The NCSR is a free, anonymous, annual self-assessment designed to meal to based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsol ould complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period wide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).	your email that er-threats-and- isure gaps and red by DHS and
	agency has not y		•	-	Hygiene Services and Nationwide Cybersecurity Review (NCSR) Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for ther	n if our project is
					t will be executed. recipient address.	
cannot.					e reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reason	ns why it
Yes, we c	could reduce from	n three year	to two y	ears, alth	though three years is optimal.	
			-		er jurisdictions? ions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.	
☑ No						
	naintains a core				t focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustair Acurrent level.	" if the project
16. If this Not applic		taining a p	revious	ly award	ded SLCGP project, please provide the fiscal year and project name of the original project.	
☑ Equip □ Train □ Exerc	pment - Equipme ning - Content and cises - Hands-or events	ent, supplies d methods o	s, and sy of delive	stems th ry that co	izational structure, and leadership at each level in the structure hat comply with relevant standards omply with relevant training standards inowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilitie	es to respond to
Line Item Detail Bu						
PLANNING COS Planning Cost Lii	STS	Quantity	Unit Cost		escribe how the purchase(s) within this element tie into the How would your organization sustain thi funding was reduced or discontinued?	s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity				s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$ \$		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$ \$ \$		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$ \$		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$ \$ \$ \$ \$ \$ \$		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		s project if gran
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		S S S S S S S S S S		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		S		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		S S S S S S S S S S		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item	Quantity		Property Property		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item		Cost	Property Property		s project if grant
PLANNING COS Planning Cost Lii	STS ne Item escription		Cost	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	roject as described in the Application Questions section. funding was reduced or discontinued?	
PLANNING CO: Planning Cost Lii Name De ORGANIZATIOI Organizational	STS ne Item escription	0	Cost	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		rganization t if grant

\$ \$ \$

\$ \$

\$

\$

				\$ \$						
				\$						
			25		\$ 43,750.00					
					,.					
EQUIPME	NT COSTS									
Equipment Cost Name	Line Item Description Qu	uantity 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 gran funding was reduced or discontinued	equipment-list			- Search ema.gov/grants/tools/authorized- t to find AEL info
Services	Professional Services to implement DDOS	1 14,58		14,588.82	Installation and configuration	This is a one time set up cost.	Consulting Servi	ces	21GN-00-CNS	Т
Cloud Security	DDoS Protection for Networks - On- Demand Bandwidth	36 38,87	\$ 7.94 1,4 1,4 1,4 1,4 1,4 1,4 1,4 1,4 1,4 1,		Deploy new capability to monitor, audit, track network traffic and ensure continuity of communication 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 s sustainability budget.	Asset Managem	ent	05SM-00-ITAN	
			\$ \$ \$	\$						
			\$ \$	\$						
			\$	\$						
		37	\$ \$	\$ \$						
				414,194.66	5					
TRAINING	COSTS			Doc	oribo how the n	urahasa(s) with	in this alament	How would your ora	anization custain this	Do you plan to goordinate this
Training Cost Name	Line Item Description	Quantity	Unit Cost	Total tie in	nto the project a stions section.	urchase(s) with	the Application	project if grant fundi discontinued?	anization sustain this ng was reduced or	Do you plan to coordinate this training with the State Training Officer?
			\$	\$						
			\$ \$	\$						
			\$	\$						
			\$ \$	\$						
			\$	\$						
			\$ \$	\$						
			\$	\$						
			\$	\$						
			\$ \$	\$						
		0 \$	0.00	\$						0
				0.00						
EXERCISE	E COSTS									
Exercise Cost Name	Line Item	Quantity	Unit Cost	Total tie		as described in		How would your org project if grant fund discontinued?	anization sustain this ing was reduced or	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 * A-133 Audit (Most Current)	Required?	Attached Documents * Audit report
Travel Policy	✓	<u>Travel Policy</u>
Payroll Policy	✓	Payroll policy
Procurement Policy	~	Procurement policy
Milestones download template	~	Milestones

 $^{^{\}star}ZoomGrants^{\intercal\!\!M}$ is not responsible for the content of uploaded documents.

Application ID: 484545

Become a <u>lan of ZoomGrans</u>, on Facebook
Problems? Confact us at <u>Questions 2 ZoomGrans com</u>
Problems? Confact us at <u>Questions 2 ZoomGrans com</u>
2 ZoomGrans of the <u>ZoomGrans com</u>
2 ZoomGrans and the <u>ZoomGrans logo</u> are <u>Indehenate</u> of GrantAnalyst.com, LLC.
<u>Local Elements</u>

	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



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

\$ 524,447.00 Requested	Clark County School District		
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	5100 W Sahara Ave Las Vegas, NV 89146 United States Chief Information Officer Marilyn Delmont delmom@nv.ccsd.net	Telephone Fax Web UEI SAM Expire	702-799-2273 SRBYQ7XFBYA6 es
1. Is your organization one of the following types of entitic district, council of government, regional government entit public entity, tribe, or authorized tribal organization. Be advised that state agencies receiving SLCGP funds will hat Yes No 2. All funds granted under the State and Local Cybersecu achieving this goal? (If not, the project is not eligible for S	y, agency or instrumentality of a local governm we to obtain consent for their project from local juri	nent, rural community, ui	nincorporated town or village, or other obtaining this consent will be provided.

□ 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.

- ✓ Lunderstand 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.

- 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 cybersecuri	ty posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
☐ Objective 3: Implement security protections comm	nensurate with risk.
Objective 4: Ensure organization personnel are a	ppropriately trained in cybersecurity, commensurate with responsibility.
3. Please select which of the SLCGP program ele	ements your project addresses.
Projects may align with more than one element.	
	is, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the ation systems, including legacy information systems and information technology that are no longer supported by the manufacturer of
_ ,	tivity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the
 3. Enhance the preparation, response, and resilie within the state, against cybersecurity risks and c 	ence of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments ybersecurity threats.
cybersecurity threats on information systems, app	rity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and blications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
<u> </u>	nin the state, adopt and use best practices and methodologies to enhance cybersecurity.
, , , ,	I 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 I a cybersecurity incident. 	ocal governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to
workforces of the state or local governments with	lucation (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity in the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of a the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
 9. Ensures continuity of communication and data involving those communications or data networks 	networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident
•	ossible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which
_ , , ,	dicators and related information between the state, local governments within the state, and CISA.
· · · · · · · · · · · · · · · · · · ·	ISA. (See Application Question 10 for further details on these services.)
13. Implement an information technology and operational technology cybersecurity objectives.	erational technology modernization cybersecurity review process that ensures alignment between information technology and
☐ 14. Develop and coordinate strategies to address	s cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be hould 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.
IAM Access Governance provides the following: 1) Victoud and on-premises environments. 2) Dynamic Acmodels allow for more granular and context-aware per policies. 3) Access Reviews and Analytics insights-badriven by analytics, helps in identifying anomalies or ethis will simplify the process, giving business owners and sources of truth, it ensures that access policies are in compliance with laws like FERPA, HIPAA, or intermitigate risks by identifying patterns that might indicat Access Governance not only aids in better user mana security by ensuring that governance processes are fappropriate, and compliant, thereby significantly imprecontrolling access rights, which are fundamental in precritical services to.	isibility and Control Over Access including comprehensive visibility into who has access to what across our enterprise, spanning both cess Control which enhances various access control models like attribute-based, policy-based, and role-based access control. These missions, reducing the risk of unauthorized access by ensuring that access rights are aligned with business needs and security ased access reviews, where access rights are periodically reviewed and certified by managers or system owners. This process, excessive permissions, which could be security risks. Currently, this is a manual process for our staff that requires heavy overhead, auditors, and leadership access to reviews on demand. 4) Policy Compliance by integrating with our current provisioning platform re enforced consistently across the enterprise and helps in maintaining compliance with regulatory requirements by managing access al policies. 5) Risk Mitigation Through Intelligence using machine learning and advanced analytics, the product can predict and e potential security issues, such as dormant accounts with high privileges or unusual access patterns. 6) The intuitive user interface of agement but also encourages adoption by making governance tasks less cumbersome. This user-centric approach indirectly improves belowed more diligently. Access Governance would help reduce the attack surface by ensuring that access is least privileged, owing the District's cybersecurity posture. This product aligns with best practices in cybersecurity by automating, monitoring, and eventing unauthorized access and data breaches. Benefits the 7.24% of rural communities that Clark County School District provides
There are 373 school programs in SY 2023-24. 27 (7.	.24%) of which are considered rural schools.
security measures. IAG syncs with the District's Huma consistent identity data. This synchronization pulls dat Role-Based Access Control (RBAC), where permissis allowing for more granular, dynamic control based on can be adjusted dynamically according to predefined triggering them based on events or schedules, ensuri lifecycle, from onboarding through role changes to off point of control for access governance, it reduces the ensuring visibility into who has access to what resoun challenge for the District. IAG's integration capabilities are enforced uniformly across various applications an governance policies based on actual usage and threa governance strategies dynamically. IAG provides a fre regulatory requirements. The comprehensive governa	rate governance structures by managing identities and access rights, ensuring both compliance with regulatory standards and robust an Resources system (our source of truth) to create a unified identity profile, ensuring that all systems operate with accurate and a from authoritative sources and correlates this data to fit into the governance framework. IAG supports our current models, including one are assigned based on roles, simplifying management for large user groups, and Attribute-Based Access Control (ABAC), user or resource attributes, such as Student Information System. Policy-Based Access Control (PBAC), ensures that access rights rules or changes in context, thereby aligning with evolving business needs or security policies. The system automates access reviews, ng that access rights are always appropriate for current roles and responsibilities. This extends to managing the entire identity boarding, which is crucial for maintaining access integrity as personnel changes occur within the organization. By providing a single risks associated with decentralized or misconfigured access settings, streamlines auditing processes, and facilitates compliance by sea across the organization. This also reduces the overhead of managing access across multiple disparate systems which is a current so allow it to interface with our current provisioning system and third-party systems and applications. It ensures that governance policies of platforms. IAG incorporates analytics, providing insights for identifying potential risks, understanding access trends, and refining that. The analytics support a proactive approach to security and compliance management, allowing the District to adapt our amework that addresses security and compliance, dynamically adapting to the changing landscape of cybersecurity threats and ance model ensures that access rights are appropriate, justified, and in line with the principle of least privilege, helping safeguarding 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. Additionally 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 syste failures or breaches. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.
tallules of bleaches. Behicits the 1.24% of full communities that old in County Octoor District provides unload 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 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 nublic static IPs for accessible services and vulnerabilities. This service provides w

	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-servicesNationwide 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
n	n Detail Budget <u>top</u>

Line Ite

Planning Cost Name	Line Item Description	Quantity	Unit Tota	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?
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		

Cost Name Cost Cos			0 0.	.00 \$ 0.00					
Court Name Project Section Pro	ORGANIZAT	ION COSTS							
Management Line Remote Secretary Configuration of Proportions of P	Organizational Cost Name	Line Item Desc	ription Qu	antity					this project if grant funding was
Section of the properties of t	Project Management	Project Manager			\$ 9 75.00 21,875.0	0 associated with	n: Adopt and use best practices and me	thodologies to	Reduce funding to other district priorities.
S S S S S S S S S S					\$))	· · ·		
Second S					\$	3			
Section Sect					\$	3			
SEQUIPMENT COSTS Equipment Line teem Cost Name Description Cost of integrate Cost Name Description Cost of integrate Cost Name Description Cost Name Desc					\$ \$	3			
Securior 175.00 21,875.0					\$	3			
Equipment Line Item Cost Name Description Co				125	\$	3			
Cost Name Description Cost Name Description Desc									
Cost Name Line Item Cost Name Cost Name Line Item Line	EQUIPMENT	COSTS							
Continue					purchase(s)				
Services with Student information System. Systems of Control Productivity Systems requires additional development of the Productivity required for access reviews. Software Monthly Subscription fee Signal and functionally required for access reviews. Software Subscription fee Signal and functionally required for access reviews. Software Subscription fee Signal and functionally required for access reviews. Software Subscription fee Signal and functionally required for access reviews. Software Subscription fee Signal and functionally required for access reviews. Software Subscription fee Signal and functionally required for access reviews. Software Subscription fee Signal and functionally required for access reviews. Software Subscription and functionally required for access greaters for the biddle for access reviews. Software Subscription access greaters for the district and functionally required for access greaters for the fairfield functionally required for access greaters for access greaters for the fairfield functionally required for access greaters for acces			Unit Cost	Tota	element tie into the project as described in the Application Questions	organization sustain this project if grant funding was reduced or	https://www.fema.gov/grants/tools/ equipment-list to find AEL info	authorized- https	://www.fema.gov/grants/tools/authorized-
Subscription subscription fee 202,572.00 best practices to other district priorities. methodologies to enhance Identity Management by employing access governance. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Services to i with life Sy: Acc Dirr En En Pro Sy: Add Stull Infe Sy: rec add devene the dirri fun rec acc rev	ntegrate h of Student ormation stem, tive ectory and terprise nail and oductivity stems. ditionally, ident ormation stems juires ditional velopment eded for beigetional ctionality juired for cess eiews.	300,000.00 3	00,000.00	configuration three major systems to utilize IAM Governance.	time set up cost.			
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Subscription sub	oscription	2	02,572.00	best practices and methodologies to enhance Identity Management by employing access governance.	to other district priorities.	Sumware as a Service	U4AF	-11-SAAS
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$			\$	\$					
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$			\$ \$	\$					
\$ \$ \$ \$ \$ \$			\$	\$					
\$ \$			\$	\$					
			\$	\$					

	37 \$ \$ 305,627.00 502,572.00								
TRAINING COSTS									
Training Cost Name	Line Item Description	Quantity	Unit . Cost	Total tie	scribe how the purchase(s) within this element into the project as described in the Application estions 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	Tota	Describe how the purchase(s) within this element. How would your organization sustain this tie into the project as described in the Application project if grant funding was reduced or Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		0	\$ 0.00	\$		0
				0.00		
Total		0	\$ 0.00	\$0.00		0

Document Uploads top

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

 $^{^{\}star}$ ZoomGrants $^{\text{\tiny{TM}}}$ is not responsible for the content of uploaded documents.

Application ID: 484825

Become a f<u>an of ZoonGrants</u>¹⁰ on Facebook
Problema® Confact us at <u>Questions ® ZoonGrants com</u>
Confact us at <u>Questions ® ZoonGrants com</u>
Confact Office Search Confact
"ZoonGrants" and the ZoonGrants bogo us to defendats of GrantAnalyst.com, LLC.
Lancial | Brometin

	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,	
5	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



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	nn	Requested

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

Project Contact Dirk Florence 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

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: France appropriate appropriately topically trained in other particular appropriately appropri
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.
I. 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.
Systems of reclaimings. 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.
It also be the state of the state of the state of the state of the state. It also be seen 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

Coperating this service as part of the SLOCO (CRSA). For these regular derivations and incompletely and provided the service for submissional control of the service of the	sperved of a grant but is a paste service. This paste service assessment of policies and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides sealing and the service and evidence for the service provides and the service and evidence for the service for the service provides and evidence seal sealing and the service and evidence for the service and evidence seal sealing and the service and evidence seal sealing and the service and evidence seal sealing and the sealing and evidence and evidence sealing and the sealing and evidence sealing and the sealing and evidence sealing and the sealing and evidence could be an evidence of the sealing and evidence sealing and the sealing and evidence sealing and the sealing and evidence of the sealing and	11. RE	EQUIRED SERV	ICES AND M	IEMBERS	SHIPS: All S	SLUGP	recipients a	and subrec	ipients are	required to	participate	e in a limited n	umber of free	services by the	ie
the "health" of your policy accessable wisk applications by children's price from our unbrainabilities and wask configurations. Additionally, Citiz As on accommend ways in a configuration of the con	the "health" of your publish accessible who applications by relecting for thrown vulnerabilities and vesal configurations, Additionally, CIBA can recommend ways to continuous areas or outside, scatter for the continuous areas or outside, scatter for the continuous areas or outside, scatter for the continuous and advanced that is, and a services provides very ulmerability report of the services, email vulnerability, refor Ross dha gave with the subject live. "Requesting Cyber Hypiera Services—SLCOP" to get stated, indicate in the body of your email that send on the continuous and advanced the "Requesting Cyber Hypiera Services—SLCOP" to get stated, indicate in the body of your email that send of the continuous and advanced the "great statements" (Services — SLCOP" to get stated, indicate in the body of your email that send of continuous and advanced the "great statements" (Services — SLCOP" to get stated, indicate in the body of your email that and capabilities of a BLT is operate circly program. It is is based on the National Institute of Blandards and Technology Cyberaccurity Previews (ACIB). If the provision of the property is described the "great statements" (Services and Services — SLCOP" or get stated, indicate in the large property and the services of the property is described by the statement of the property of the services of t	Cyber	security and In	frastructure	Security	Agency (C	ISA). Fo	r these rec	uired serv	ices and me	emberships	, please no	te that particip	oation is not re	equired for su	bmission and
continuous scario de public, static IPs for excessible services and visiones and visiones provides weekly uninvisibility reports and all hole and its hard of your small half services and visiones of the control of the public o	continuous scale of public, state IPs to accessible survises and valurabilities. This services provides veicely variability properts and a disconsist To register for this or provided the state of the continuous parts and the provided of the continuous parts and the continuous parts and the continuous parts and the continuous parts and the state and	the "h	ealth" of your p	oublicly acce	essible w	eb applicat	ions by	checking f	or known v	vulnerabiliti	es and wea	k configur	ations. Additio	nally, CISA ca	an recommen	d ways to
services, earnick stuministicity, incloy class aftis, gover with the subject lives "Requesting Cyber Psychians Services." Significant Confidence in this body of your small that you are required in the service of the SLT of the SLDE, The Psychians Services and SLT or potential that you are required in the Service of the SLT of the SLDE, The Psychians Services and SLT or potential and the SLPE SLDE, clinical and earlier considerable and Technology Cybersecurity Flamework and its epone on the SLT of the SLT or potential and Technology Cybersecurity Flamework and its epone on the SLT or potential and the SLPE SLDE, clinically slde scales and the SLPE SLDE, clinically and the SLPE SLDE, clinically slde scales and the SLPE SLDE SLDE SLDE SLDE SLDE SLDE SLDE SLD	services, email studinicality, into glocise chiese you with the subject for. Requesting Cyber Hygiene Services. —St.COP* to get stands indicate in the body of your email and subject for. Requesting Cyber Hygiene Services. —St.COP* to get stands and the stands of the common stands of s															
you are requesting this service as part of the SLCEP. For more information, visit (EBA's Opine) hylgener information of page https://www.cis.ago-viological-polar-protects and solid products of the product of the prod	you are requesting this service as part of the SLCP. For more information, visit CSBA is Cyber hygiene information Page: https://www.csa.gov/billips/cbb/page/page/page/page/page/page/page/page															
compatibilities of is S. If is operaneutry organization in the based on the National Institute of Stundards and Technology Operaneutry Framework and is appositionally plant and an expensional public and the control of the property of the	capabilities of a SLT's operacutary programs. It is based on the National Institute of Stunder's and Technology Cybersceruly Programs and an annual for the programs of the pr															
## WB-SI-SAC. Entities and that subvisciplems should complete the NCSR, administered by the MS-SAC, during the first year of the average content country. For from a information, while failurement of preformance and memority. For from a information, while failurement of preformance and memority. For from a protection will be required to sign up for the Cyber Hygiens Services or Nationwake Cybersecutily Review PICSR), but understands we will be required to sign up for them flour project is sometiment. The project states are subvised to the S-digit size pools where the project will be executed. The project content on the S-digit size pools where the project will be executed. The project content on the S-digit size pools where the project will be executed. The project content on the S-digit size pools where the project will be executed. The project content on the S-digit size pools where the project will be executed. The project content on the S-digit size pools where the project will be executed. The project content on the S-digit size pools where the project will be executed. The project content on the S-digit size pools where the project will be executed. The project districts of the project states and or of the project states are supported and the second of the	the MS-SACE. Entities and thater subrice/pleases beholds complete the NSCS, administered by the MS-SACE, during the first year of the average content of the ave															
Usuagency is streetly antifying the project in Hygiene Streetly and Materials Cybernous (NCSR). That understands we will be required to sign up for them? Your project in smethal in the project should be executed. 12. Provide the 5-digit sign code where the project will be executed. 13. It is this project scalesable? 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. 14. It is this project scalesable? 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. 15. It is this project sharpable or deployable to other particlictions? 16. It is this project sharpable or deployable to other particlictions? 17. It is this project sharpable or deployable to other particlictions? 18. It is project sharpable or deployable to other particlictions? 19. It is allow or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project is outcome a capability gap. Select "sustain" if the project sustains a core capability as the extensing extreme level. 19. Station 19. Station 19. It is project is sustaining a previously searched SLCOP project, please provide the fiscal year and project name of the original project. 19. These select all applicable planning, organization, equipment, training, and searcies (POETE) elements for which funding is being acquired for this project. 19. The project is sustaining a previously searched search, members of project is intended to the control of	Our agency activately participating in the Cyber Hygeres Bervies and Materials Cybernocutils Review (NCSR)	the M	-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													
Our agency has not up to graded up for the C-Deer Hygiene Servoso or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is consistent to the project that is designed to the 5-flight product that is the 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 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 flat if the 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 flat if the 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 15. It flat or Sustain Salect *build! If this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Salect *sustain!" If the project strictly maintains a core capability at its existing/current level. 16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project. No special is the project of sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project. No special is understand to sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project. No special is understand to sustaining a previously awarded SLCGP project, please provide the fiscal year and project and original project. No special is understand to sustaining a previously awarded SLCGP project, please provide the fiscal year and project and original project. No special is project or sustaining a previously awarded SLCGP project, please provide the fiscal ye	Cur againty has not yet aligned up for the Cyber Higher Section of National Section of National Section (National Section of National Section could be different than the sub-recipient address. The regional state of the Sedigit species where the project will be executed. The project scale belief Cost 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 be set that it is project stateable? 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 be set to the project and the project scale belief to the project scale belief to the project scale and project scale												isac/services/i	ncsr (cisecurit	y.org).	
2. Provided the 5-digit also pools where the project will be executed. The project location could be different dent for authorized authorized. The project scalebable? Can any part of it be treduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot. 14. It is this project shar-able or deployable to other jurisdictions? Solice! "First if the project approximation project for a project authorized by a project	13. Is this project scaleable? Can any part of it be reduced expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot fine. 14. Is this project scaleable? Can any part of it be reduced expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot fine. 15. Is this project shareable or deployable to other jurisdictions? Discribe the ways in which the project can be reduced or expanded, or the reasons why it cannot reduce the project shareable or deployable to other jurisdictions? Discribe the ways in which the project can be reduced or expanded, or the reasons why it cannot reduce the project shareable or deployable to other jurisdictions? Discribe the ways in which the project is or close a capability gain to the project is used in the project of the project is or close a capability gain. Select "fine" if the project is used in the project is used in the project of the project is used in the project is		0 ,	,, ,	•	, , , ,					,	,	stands we will b	e required to s	ign up for them	if our project is
The project location could be different them this sub-incoport advises. 11. 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? Secrit rife project subprote supports multiply jurisdictions (e.g., multiple critical). No 15. Build or Sustain. Schort "hold" 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 sicrity multiple project. Studio 16. If this project is sustaining a previously awarded SLCOP project, please provide the fiscal year and project name of the original project. No supports 17. Please select all supplicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Planning — Description— Description of the project planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Planning— Description— Supplicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Planning— Description— Supplicable planning, organization districture, and is advantaged, and the purchase of the project planning organization and the project planning organization districture, and is advantaged, and the purchase of the project and project and reduced or discontinued? Planning— Contract and reduced to dislayer, that comply with districture and project and information. Planning— Contract and reduced to discontinued? Planning— Contract and r	The project location could be different than the use in requires address. 69146 13. It this project excelled a displayable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" if the project supports installable to other jurisdictions? Select "Yes" in the project supports installable to other jurisdictions? Select "Yes" in the project supports installable to other jurisdictions? Select "Yes" in the project supports installable project supports in such jurisdictions. Select "Yes" in the project supports in such jurisdictions in such jurisdictions. Select all supports such jurisdictions. Select "Yes" in the project supports in such jurisdictions. Select "Yes" in the project supports in such jurisdictions. Select "Yes" in the project supports in such jurisdictions. Select "Yes" in the project such jurisdictions. Select "Yes" in the proj	av	warded	, ,		, ,,				•	,			·	•	
13. Is the project cacleable? 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 sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions? Solicit "Yes" if the project sharmable or deployable to other jurisdictions. The project sharmable or deployable to the project sharmab	and side 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 not not the project shareable or deployable to other particulations? Silect "rive" if the project shareable or deployable to other particulations? Silect "rive" if the project shareable or deployable to other particulations? 15. Build or Statistic Select "Mult" if this project to success on atterting a new capability, or the intent of the project is to close a capability gap, Select "sustain" if the project study warman as core capability at its entiregeneral local. Statistic Statistic Select "Mult" if this project is sustaining a previously awarded SLCOP project, please provide the fiscal year and project name of the original project. To Please "Statistic Select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. To Please "Statistic Select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. To Please "Statistic Select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. To Please "Statistic Select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. To Please "Statistic Select all applicable planning, organization, equipment training, and exercise (POETE) elements for which funding is being sought for this project. To Please "Statistic Select all applicable planning, organization, equipment training, and exercise (POETE) elements for which funding is being sought for this project. To Please "Statistic Select all applicable planning, organization, equipment training, and exercise (POETE) elements for which funding is being sought for this project is a stat	12. Pr	ovide the 5-digi	t zip code w	here the	project will	be exe	cuted.								
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 sharable or deployable to other purisdictions? Solical "No" if the project supports a single entity." 15. Bulls 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. 16. If this project is sustaining a previously awarded SLCOP project, please provide the fiscal year and project name of the original project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Planning-Constituted and organization is a subject to the project and inference and elements of the project and elem	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 be considered to the project shareable or deployable to other jurisdictions? 14. Is this project shareable or deployable to other jurisdictions? 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 extrictly maintains a core capability at its existing/current level. 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 extrictly maintains a core capability at its existing/current level. 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 extraction in the project is sustaining a previously awarded SLCOP project, please provide the fiscal year and project name of the original project.			ould be differe	ent than th	he sub-recip	ient add	ress.								
15. Build or Sustain: Select "build" if this project apports multiple jurisdictions (e.g., multiple cities). Select "7to" if the project paramy supports a angle entity. 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 sixthy maintains a core explainty at its existing current level. 16. If this project is sustaining a previously awared SLCOP project, please provide the fiscal year and project name of the original project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project in project and interest an	14. Is this project shareable or deployable to other pirisdictions? Solved "Yes" if the project supports multiple paradictions (a.g., multiple cline). Solved "No" if the project apports a single onthly. 15. Build of 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 satisfy maintains a corte capability at its existing current level. 15. Build of 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 satisfy maintains a corte capability at its existing current level. 16. If this project is sustaining a proviously awerded SLCGP project, please provide the fiscal year and project name of the original project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please select all applicable planning, organization, and organization an	89146	•													
14. Is this project shareable or deployable to other jurisdictions? the project properly appoints multiple jurisdictions (e.g., multiple cities). Select "Yio" if the project primarily supports a single entity. 15. Build or Question 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 multiplication (e.g., multiple cities). Select "yio" if the project is to close a capability gap. Select "sustain" if the project strictly multiplication. 16. If this project is sestaining a previously swarded SLCGP project, please provide the fiscal year and project name of the original project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project is recommendation. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project in the project is gap. T	A is n'is project shareable or deployable to other jurisdictions?	13. Is	this project sca	leable? Can	any part	t of it be rec	luced o	r expanded	l? Describe	e the ways i	n which the	project ca	in be reduced	or expanded,	or the reason	s why it cannot.
Select "Yes" if the project supports multiple jurnalisations (e.g., multiple cities). Select "No" if the project primarily supports a single entity. 15. Build of 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 "austain" if the project strictly maintains a core capability at its existing/current level. 18. Build of 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 "austain" if the project strictly maintains a core capability at its existing/current level. 18. Build of Sustain: Select "build" if this project is sustaining a previously awarded SLCGP project, please provide the fliscal year and project name of the original project. 18. Build of Sustain: Select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Planning - Device planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Planning - Device planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Planning - Device planning, organization and exercise planning, organization and exe	Solicit - Yes's' if the project supports multiple pursolations (e.g., multiple critics). Solicit 1/6/ if the project primarely supports a single unity. 15. Bull of Sustain: Select 1 build! if this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is an occasion of the control of the project in a new capability or this project. 16. If this project is sustaining a previously awarded SLCOP project, please provide the fiscal year and project name of the original project. 17. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 17. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POET	No														
Select "Yes" if the project supports multiple jurnalisations (e.g., multiple cities). Select "No" if the project primarily supports a single entity. 15. Build of 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 "austain" if the project strictly maintains a core capability at its existing/current level. 18. Build of 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 "austain" if the project strictly maintains a core capability at its existing/current level. 18. Build of Sustain: Select "build" if this project is sustaining a previously awarded SLCGP project, please provide the fliscal year and project name of the original project. 18. Build of Sustain: Select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Planning - Device planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Planning - Device planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Planning - Device planning, organization and exercise planning, organization and exe	Solicit - Yes's' if the project supports multiple pursolations (e.g., multiple critics). Solicit 1/6/ if the project primarely supports a single unity. 15. Bull of Sustain: Select 1 build! if this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is to close a capability gap. Select 1 sustain' if the project starting in a new capability or the intent of the project is an occasion of the control of the project in a new capability or this project. 16. If this project is sustaining a previously awarded SLCOP project, please provide the fiscal year and project name of the original project. 17. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 17. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 18. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. 19. Please-select all applicable planning, organization, equipment, training, and exercise (POET	14 ls	this project sha	reable or de	nlovable	to other iu	risdictio	ns?								
15. Built 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 select and sustain as core capability at its existing/current level. Planta P	15. Build of 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 "austain" if the project study merchant of the project is under the project study merchant of the project is sustain. 16. If this project is sustaining a previously awarded SLCOP project, please provide the fiscal year and project name of the original project. Not applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Please select all supplicable planning, organization and elements of the original project. Please select all supplicable planning, organization and elements of the project as a supplicable planning, organization and elements or a selection and entropy and elements of the project and exercise (POETE) elements for which funding is being sought for this project. Please selected and reduced or delivery but correlated to the project and exercise (POETE) elements for which funding as a please selected and reduced and reduced or delivery but correlated and reduced or delivery but correlated and reduced by a second to reduce and project and project as described in the Application Questions section. Please Pleas								. Select "No	o" if the proje	ect primarily	supports a	single entity.			
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.	15. Build or Sustain: Salect "build" if this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Safect "sustain" if the project articly maintains a core capability at its soliding/current level. Sustain															
strictly maintains a core capability at its existing/current level. Budd	strictly maintains a core capability at its existing/current level. Sustain Susta	✓ No	0													
Bladd Sustain	Build Sustain								new capab	ility, or the i	ntent of the	project is	to close a cap	ability gap. Se	elect "sustain'	if the project
Sustain	Sustain			ore capability	y at its ex	xisting/curr	ent leve	l.								
16. If this project is sustaining a proviously awarded SLCGP project, please provide the fiscal year and project name of the original project. Not applicable. 17. Pleases select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Planning - Content and methods of delivery but a comply with elevent training attached as a described in the Application of vertice. Training - Content and methods of delivery but comply with elevent training almost standards Planning - Content and methods of delivery but comply with elevent training almost standards or real content and methods of plans, allow methods to amply with elevent training almost standards or real content and methods of plans, allow methods to improve their own performance, and identify opportunities to improve capabilities to respond to real control. Planning - Content and methods of delivery but comply with elevent training almost standards or real control of control. Planning - Content and methods of delivery but comply with elevent training almost standards or real control.	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. Pleases select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Plearning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information. Policidation in the project of the project is pleased by the project of the project as described in the Application Questions section. Please															
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 other publications. Also intelligence and other publications are involved to the structure	Not applicable. 17. Please select all applicable planning, organization, equipment, training, and exercise (POETs) elements for which funding is being sought for this project. Potential Provided the sense of the project sense of the pro															
17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. Planning P	1. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.			ustaining a p	reviousl	ly awarded	SLCGP	project, ple	ease provid	de the fiscal	year and p	roject nam	e of the origina	al project.		
Planning- Development of policies, plans, procedures, mutual aid agreements, stratagies, and other publications; also involves the collection and analysis of intelligence and information inclination inclination and incli	Planning - Development of policies, plans, procedures, and tale daysements, strategies, and other publications; also involves the collection and analysis of intelligence and information individual teams, an overall organizational structure, and leadership at each level in the structure Experiment - Equipment - Equipment, supplies, and systems that compsy with relevant standards	·														
Information Individual teams, an overall organizational structure, and leadership at each level in the structure	information Comparisation Individual teams, an overall organizational structure, and leadership at each level in the structure Equipment Equipment Supplies, and systems that comply with relevant standards Carling Comparisation Comparisat				_	-			-	-			_			
Pulsarium - Equipment - Equipment, supplies, and systems that comply with relevant training alreadards 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	Continue of members of believes that comply with relevant standards and advanced or meal events and solve the members of believes that accomply with relevant standards and delivers. It is not a clivities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events. Planning Cost Line Item Detail Budget March Cost Cos			inent of polici	ies, piaris	s, procedures	, mutua	i alu agreen	ieriis, siraie	gies, and our	iei publicatio	nis, also liiv	olves the collec	lion and analys	is of filtelligeno	e and
Training - Content and methods of delivery that comply with relevant training standards	Training - Content and methods of delivery that comply with relevant training standards reactives: substitute in the project is secured by the purchase of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events PLANNING COSTS Planning Cost Line Item Quantity Cost Total Describe how the purchase(s) within this element tie into the Planning Cost Line Item L		-			-			-	each level in	the structure	:				
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 Planning Cost	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				-					c						
Line Item Detail Budget face PLANNING COSTS Planning Cost Line Item Name Description Quantity Cost S S S S S S S S S S S COGANIZATION COST Organizational Cost Cost S S S S S S S S S S S S S S S S S S S	Line Item Detail Budget 100 PLANNING COSTS Planning Cost Line Item Name Description Ouanity S S S S S S S Oversight and project As project management to line the Application Questions section.		-						-		eir own perfo	rmance, an	d identify oppor	tunities to impr	ove capabilities	s to respond to
PLANNING COSTS Planning Cost Line Item Name Description Quantity Cost S	PLANNING COSTS Planning Cost Line tem Name Description Quantity 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 gran funding was reduced or discontinued? S						3	,					, . , . , . , . , . , . , . , .	,		
PLANNING COSTS Planning Cost Line Item Name Description Quantity Cost S	PLANNING COSTS Planning Cost Line tem Name Description Quantity 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 gran funding was reduced or discontinued? S															
PLANNING COSTS Planning Cost Line Item Name Description Quantity Cost S	PLANNING COSTS Planning Cost Line tem Name Description Quantity 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 gran funding was reduced or discontinued? S															
Planning Cost Name Description Quantity Obscription Planning Cost Cost	Planning Cost Line Item Name Description Quantity Cost Total persistent of the purchase(s) within this element tie into the funding was reduced or discontinued? S	Line Item Detail	Budget top													
Planning Cost Name Description Quantity Obscription Planning Cost Cost	Planning Cost Line Item Name Description Quantity Cost Total persistent of the purchase(s) within this element tie into the funding was reduced or discontinued? S	Line Item Detail	Budget top													
Name Description Cost Co	Name Description Cost First Project as described in the Application Questions section. funding was reduced or discontinued?															
CORGANIZATION COSTS Organizational Cost Name Line Item Description Quantity Cost Solution Cost Name Project Blended average of Project management resources. Solution Cost Name Project Project Ranagement Project Ranagement Project Solution Cost Name All 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 Project management and project management to attain milestone delivery associated Project in management on the project if grant funding was reduced or discontinued? Reduce funding to other district priorities. Solution Cost Name Solution Cost Name Solution Cost Name Project management project management to attain milestone delivery associated and methodologies to an metho	CORGANIZATION COSTS Organizational Cost Name Describe how the purchase(s) within this element tie into the project management resources. Total as described in the Application Questions section. How would your organization sustain this project if grant funding was reduced or discontinued?	PLANNING C	costs		11-7											
ORGANIZATION COSTS Organizational Cost Name Line Item Description Quantity Cost Total as described in the Application Questions section. Project Blended average of Project management Project management resources. S S S S S S S S S S S S S S S S S S S	CRGANIZATION COSTS Organizational Cost Name Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. Project Blended average of Project management Project managem	PLANNING O	COSTS Line Item	Quantity												s project if grant
ORGANIZATION COSTS Organizational Cost Management Project Management Project Management Project Management Project Management Project Management Resources. S S S S S S S S S S S S S S S S S S S	ORGANIZATION COSTS Organizational Cost Name Line Item Description Quantity Cost Management Project management resources. 125 \$	PLANNING O	COSTS Line Item	Quantity		projec										s project if grant
CRGANIZATION COSTS Organizational Cost Name Line Item Description Quantity Cost Total as described in the Application Questions section. Project Management Project management resources. S S S S S S S S S S S S S S S S S S S	ORGANIZATION COSTS Cost Name Project management Project managemen	PLANNING O	COSTS Line Item	Quantity		\$ \$										s project if grant
ORGANIZATION COSTS Organizational Cost Name Project Management Project management resources. Blended average of Project management resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	SCORGANIZATION COSTS Organizational Cost Name Line Item Description Quantity Cost 7175.00 21,875.00 with: Adopt and use best practices and methodologies to enhance cybersecurity – Multifactor Authentication for student educational systems. S S S S S S S S S S S S S S S S S S S	PLANNING O	COSTS Line Item	Quantity		project \$ \$ \$										s project if grant
ORGANIZATION COSTS Organizational Cost Name Blanded average of Management resources. Blanded average of Project management resources. S S Oversight and project management to attain milestone delivery associated resources. S S S Oversight and project management to attain milestone delivery associated best practices and methodologies to enhance cybersecurity – Multifactor Authentication for student educational systems. S S S S S S S S S S S S S S S S S S S	SORGANIZATION COSTS Organizational Cost Name Project Management Project management resources. Blended average of Management Project management resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING O	COSTS Line Item	Quantity		\$ \$ \$ \$										s project if grant
ORGANIZATION COSTS Organizational Cost Name Project Management Project management resources. S S Oversight and project management resources. S S S S S S S S S S S S S S S S S S S	ORGANIZATION COSTS Organizational Cost Name Blended average of Management Project Management resources. S S S S S S S S S S S S S S S S S S S	PLANNING O	COSTS Line Item	Quantity		\$ \$ \$ \$ \$ \$										s project if grant
ORGANIZATION COSTS Organizational Cost Name Project Management Project management resources. Project management resources. S S S S S S S S S S S S S S S S S S S	ORGANIZATION COSTS Crganizational Cost Name Project Management Project management resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING O	COSTS Line Item	Quantity		\$ \$ \$ \$ \$ \$										s project if grant
ORGANIZATION COSTS Organizational Cost Name Project Management Project management resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	ORGANIZATION COSTS Organizational Cost Name Project Management Project management resources. Blended average of Management resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING O	COSTS Line Item	Quantity		s \$ \$ \$ \$ \$										s project if grant
ORGANIZATION COSTS Crganizational Cost Name Project Management Project management resources. \$ 175.00 21,875.00 with: Adopt and project management to attain milestone delivery associated resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	CORGANIZATION COSTS Cost Name Cost Name Cost Nam	PLANNING O	COSTS Line Item	Quantity		s s s s s										s project if grant
ORGANIZATION COSTS Crganizational Cost Name Project Management Project management resources. S \$ \$ \$ Oversight and project management to attain milestone delivery associated Project management resources. S \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	ORGANIZATION COSTS Organizational Cost Name Project Management resources. \$ \$ \$ Oversight and project management resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING O	COSTS Line Item	Quantity		s s s s s s										s project if grant
ORGANIZATION COSTS Organizational Cost Name Blended average of Management resources. \$ 125	ORGANIZATION COSTS Cost Name Line Item Description Project Management resources. Blended average of Management resources. \$	PLANNING O	COSTS Line Item	Quantity		project										s project if grant
ORGANIZATION COSTS Organizational Cost Name Line Item Description Cost	ORGANIZATION COSTS Organizational Cost Name Blended average of Project management resources. \$ 125	PLANNING O	COSTS Line Item	Quantity		project										s project if grant
ORGANIZATION COSTS Organizational Cost Name Line Item Description Project Management Project management resources. S S S S S S S S S S S S S S S S S S S	ORGANIZATION COSTS Organizational Cost Name Line Item Description Project Management M	PLANNING O	COSTS Line Item	Quantity		project										s project if grant
Organizational Cost Name Line Item Description Quantity Unit Cost Total Sescribe 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 Management resources. 125 \$ 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. \$	Organizational Cost Name Line Item Description Quantity Unit Cost 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 Management Management Project Management Project Management Project management Project management to attain milestone delivery associated Project management or sudent educational systems. Reduce funding to other district priorities. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING O	COSTS Line Item		0.00	project										s project if grant
Organizational Cost Name Line Item Description Quantity Unit Cost Total Sescribe 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 Management resources. 125 \$ 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. \$	Organizational Cost Name Line Item Description Quantity Unit Cost 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 Management Management Project Management Project Management Project management Project management to attain milestone delivery associated Project management or sudent educational systems. Reduce funding to other district priorities. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING O	COSTS Line Item		0.00	project										s project if grant
Cost Name Line Item Description Cost Blended average of Management resources. Blended average of Project management resources. Solversight 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. Solversight 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. Solversight and project management to attain milestone delivery associated with a dopt and use best practices and methodologies to enhance cybersecurity – Multifactor Authentication for student educational systems. Solversight and project management to attain milestone delivery associated methodologies to enhance cybersecurity – Multifactor Authentication for student educational systems.	Cost Name Line Item Description Cost Name Discription Project Management Ma	PLANNING C Planning Cost Name	COSTS Line Item Description		0.00	project										s project if grant
Management Project management resources. 175.00 21,875.00 with: Adopt and use best practices and methodologies to enhance cybersecurity – Multifactor Authentication for student educational systems. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Management Project management resources. 175.00 21,875.00 with: Adopt and use best practices and methodologies to enhance cybersecurity – Multifactor Authentication for student educational systems. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING C Planning Cost Name	COSTS Line Item Description		0.00	project								educed or dis	continued?	
resources. cybersecurity – Multifactor Authentication for student educational systems. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	resources. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational	COSTS Line Item Description	0	0.00	Project Proj	t as des	Describe	he Applica	rchase(s) w	vithin this e	lement tie i	funding was r	t How would this project	d your organi	zation sustain ling was
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave	0 escription	0.00	s s s s s s s s s s s s s s s s s s s	Tota	Describe as descril	how the puned in the A	urchase(s) w Application	vithin this e Questions t to attain m	lement tie i section. lestone deli	into the project	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	s s s s s s s s s s s s s s s s s s s	Tota	Describe as descril	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	Project Proj	Tota \$1,875.00	Describe as descril	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
\$ \$ \$ \$ \$ \$	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	Project Proj	Tota \$1,875.00	Describe as descril Oversight Oversecu	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
\$ \$ \$ \$	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	Project S S S S S S S S S	Tota \$1,875.00	Describe as described in the second of the s	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
·	\$ \$ \$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	Project Proj	Tota \$1,875.00	Describe as described in the second of the s	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
	\$ \$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	y Unit Cost \$ 175.00 2 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Tota \$1,875.00	Describe as describe oversight with: Adop	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
·	• • • • • • • • • • • • • • • • • • • •	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	Project Proj	Tota \$1,875.00 \$\$ \$\$	Describe as descril Oversight with: Adop cybersecu	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?
·	\$	PLANNING OPlanning Cost Name ORGANIZATI Organizational Cost Name Project	COSTS Line Item Description HON COSTS Line Item D Blended ave Project mana	0 escription	0.00	Project Proj	Tota \$1,875.00	Describe as descril Oversight with: Adop cybersecu	how the pu ped in the A	urchase(s) w Application managemen est practices	vithin this e Questions t to attain m and method	lement tie isection.	funding was re	t How would this project reduced o	d your organiating grant fund or discontinued	zation sustain ling was d?

					\$	\$					
					\$	\$					
					\$	\$					
				125	\$	\$					
				•	175.00	21,875.00					
QUIPME	NT COSTS										
Equipment Cost Name	Line Item Description	Quantity	Unit Cost	т	h p w el Irotal p d th A Q	vithin this ' lement tie nto the roject as	How would your organization sustain this project if grant funding was reduced or discontinued?	equipment-list	earch ma.gov/grants/tools/authorized to find AEL info	AEL Number - S I- https://www.fen equipment-list t	na.gov/grants/tools/authorize
	Multifactor Authentication for student educational systems annual license subscription - approx 350,000 accounts	3	\$ 242,400.00	727,20	\$ A 00.00 be ai m to cy	dopt and use	to other district priorities.	Software as a S	ervice	04AP-11-SAAS	
	Implementation Services	1	\$ 15,000.00	15,00	0.00 co of st		This is a one time setup cost.	Consutling Serv	ices	21GN-00-CNST	
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
			\$		\$						
		4	\$ 257,400.00	742.20	\$ 00.00						
RAINING	COSTS		,	,							
				De	escribe	e how the nu	rchase(s) withi	n this element	How would your organization	sustain this	Do you plan to coordinate tl
raining	Line Item Description	Quant	ity Unit Cost	Γotal tie	e into t			he Application			training with the State Traini

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total tie	escribe how the purchase(s) within this element e into the project as described in the Application uestions 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
				0.00			

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit To	Describe how the purchase(s) within this element otal 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
0.00	
0 \$ 0.00 \$0.00	0
	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$

Document Uploads top

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

 $^{^{\}star} \textit{ZoomGrants}^{\intercal \! \! M}$ is not responsible for the content of uploaded documents.

Application ID: 484816

Become a <u>lan of ZoomGrants</u> "on Facebook Problems" Contact us at <u>Coestoned ZoomGrants com</u> 22002-2204 Grants-Nays com. All right neerved. ZoomGrants" and the ZoomGrants logo are trademarks of Grant/nalyst.com, LLC. Lo

	Auglieant Neme	Claul, Carrety Calcard District
	• •	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	
5	Operations	36 months after award
6		
7		
8		
9		
10		

^{*}Please add additional rows as necessary for your project



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

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

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 main-ractor 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.
☐ Actively engage in bidirectional sharing between Crox and SET 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-asa-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. 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. 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	Describe how the purchase(s) within this element Total tie into the project as described in the Application Questions section.	
Professional Services	Incident response plan and tabletop exercise.	1 80,000.00	\$ Enhance the preparation, response, and resilience of 80,000.00 critical systems. Ensure the continuity of operations.	Reduce funding to other district priorities.
			\$	
			\$	
			\$	
			\$	

		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
_		\$		
_		\$		
	1	\$		
	80,000.00	30,000.00		
00041117471	ON 000T0			
ORGANIZATION	ON COS18			
Organizational	Unit		ow the purchase(s) within this element tie	How would your organization sustain

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Describe how the purchase(s) within this element tie Total 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	\$ Oversight and project management to attain milestone 14,000.00 delivery associated with: the preparation, response, and resilience of critical systems. Ensure the continuity of operations.	Reduce funding to other district priorities.
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
		80	\$	\$	
			1/5.00	14,000.00	

EQUIPMENT COSTS

	000.0					
Equipmen Cost Name	^t Line Item Description ^{Quantity}	Unit T	Describe how the purchase (s) within this element tie oral into the project as described in the Application Questions section.	project if grant funding was reduced or	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	\$ \$	\$ \$			
	U	0.00 (₹			
		0.00	0.00			

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost		Describe how the purchase(s) within this all 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?
			\$	5	\$		
			\$	5	\$		
			\$	9	\$		
			\$	5	\$		

\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
0 \$	\$
0.00	0.00

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
Tatal			¢ 0 00 d	00.0			
Total		U	\$ 0.00	0.00			0

Document Uploads \underline{top}

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

 $^{^{\}star}\textit{ZoomGrants}^{\tau_{M}}$ is not responsible for the content of uploaded documents.

Application ID: 484954

Become a f<u>in of ZoomGrants</u> on Facebook
Problems* Corriact us at <u>Questions B ZoomGrants</u> com

"ZoomGrants" and the ZoomGrants of CoomGrants com

"ZoomGrants" and the ZoomGrants log or testdemaks of GrantAnalyst.com, LLC.

"ZoomGrants" and the ZoomGrants log or testdemaks of GrantAnalyst.com, LLC.

"ZoomGrants" and Toomgrants (Toomgrants) and Coomgrants (Toomgran

	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



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 OCansev

Charles OCansey cocansey@cleanwaterteam.com

Telephone 7026688066

Fax
Web www. cleanwaterteam.com
UEI MSTUUDL7AEG5
SAM Expires3/18/2025

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

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.

- 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

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, in detail, now, 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

	submit This s can re netwo and ac started Page: anony Stand admin Review Or or pr	ission ervice ecomm ork pre d-hoc d. Indi https://mous lards a histere w (NC: ur agei ur agei oject is ovide	and appraisassesses are not a specific and appraisasses are a specific and a spec	roval of a gesthe "hea as to enhan or executing oregister for the body of sa.gov/top self-asses: nology Cyl MS-ISAC, os://www.cis.ady particip to yet signed it zip code ould be different to the same of the could be different to the	grant but lith" of y continuor these your em- pics/cybe sment de bersecui during the security eating in t d up for the where the	is a poour pul rity in a ous so service ail that er-threa esignee ity Fra e first y org/ms he Cybe ne Cybe	ost-a blicly acco cans es, el you tats-a d to I mew year -isac er Hy ect w	CISA). For these required services and memberships, ple ward requirementCyber Hygiene Services Web Applic accessible web applications by checking for known vuln dance with industry and government best practices and sof public, static IPs for accessible services and vulnerability_info@cisa.dhs.gov with the subject line are requesting this service as part of the SLGCP. For more advisories/cyber-hygiene-servicesNationwide Cybereasure gaps and capabilities of a SLT's cybersecurity proof the award/subaward period of performance and annual services/ncsr (cisecurity.org). giene Services and Nationwide Cybersecurity Review (NCSR), but ill be executed. Services or Nationwide Cybersecurity Review (NCSR), but ill be executed. Services and Review (NCSR) in the address.	ation Scanning is an "internet scanning-as-a-service." erabilities and weak configurations. Additionally, CISA standards. Vulnerability Scanning evaluates external lities. This service provides weekly vulnerability reports "Requesting Cyber Hygiene Services – SLCGP" to get e information, visit CISA's Cyber Hygiene Information resecurity Review (NCSR) The NCSR is a free, orgams. It is based on the National Institute of and their subrecipients should complete the NCSR, ly. For more information, visit Nationwide Cybersecurity at understands we will be required to sign up for them if our
	canno	ot.	-					the disaster recovery network, and is the minimum requiremen	•
		t "Yes" es	•					urisdictions? s (e.g., multiple cities). Select "No" if the project primarily supp	ports a single entity.
	15. Bu projec ☑ Bu	uild or						cuses on starting a new capability, or the intent of the pro ting/current level.	eject is to close a capability gap. Select "sustain" if the
	16. If t N/A	this pr	oject is s	ustaining a	a previou	ısly aw	arde	d SLCGP project, please provide the fiscal year and proje	ct name of the original project.
ine Item	int Oi Tr Ex	formati rganiza quipme raining xercise spond	on ation - Indi ent - Equip - Content es - Hands to real ev	ividual team oment, supp and method s-on activitie	s, an ove lies, and ds of deliv	rall orga systema ery tha	aniza s tha t com	es, mutual aid agreements, strategies, and other publications; a ional structure, and leadership at each level in the structure comply with relevant standards ply with relevant training standards wledge of plans, allow members to improve their own performa	, ,
PLANN	ING C	COST	s						
Planning Name	Cost	Line I	_	Quantity	Unit Cost	Total		ribe how the purchase(s) within this element tie into the ct 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	0.00			
ORGAN Organiza			COSTS Line Item) _		Unit -		Describe how the purchase(s) within this element tie into	the How would your organization sustain this project if
Name			Descripti		antity	Cost	Γotal	project as described in the Application Questions section	
						\$	\$		
						\$	\$		
						\$ \$	\$		
						\$	\$		
						\$	\$		
						\$ \$	\$		
						\$	\$		

L

				^ ^					
				\$ \$ \$ \$					
				\$ \$					
			0 6 0	\$ \$ 00 \$					
			0 \$ 0.	0.00					
EQUIPME	ENT COSTS								
Equipment Cost Name	Description and			Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	project if gran funding was reduced or discontinued?)	.gov/grants/tools/authorized-	equipment-iist	na.gov/grants/tools/authorized-
Firewall	Security Appliance Cluster	16,494.2	18 32,988.5	6 Prevents 6 intrusions and allows monitoring of a critical infrastructur network.	added to budget at the end of the product's useful life.	Firewall, Network		05NP-00-FWAL	
Transceiver Module	Transceiver Module			The above item would not work without this module.	expense; n products equipment replacement would be added to budget at the	Components, Netwo	orking	04HW-03-NETD	
				5					
				5					
		(\$	5					
				5					
				5					
				5					
				5					
				5					
				§ §					
		6	\$	5					
		16,569.5	1 33,289.4	8					
									
TRAINING				Describe how	v the purchase(s	s) within this	How would your organizati	on sustain this	Do you plan to coordinate this
Training Cost Name	Line Item Description	Quantity C	Total	element tie in	the purchase(s to the project as Questions sectio	s described in the	project if grant funding was discontinued?	reduced or	training with the State Training Officer?
			\$ \$						
			\$ \$ \$ \$						
			\$ \$						
			\$ \$						
			Ψ						
			\$ \$						
			\$ \$ \$ \$						
			\$ \$						
			\$ \$ \$ \$ \$ \$ \$ \$ \$ \$						
			\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$						
			\$ \$ \$ \$ \$ \$ \$ \$ \$ \$						

EXERCISE COSTS

Exercise Line Item
Cost Name Description Quantity Unit Cost Total element tie into the project as described in the Application Questions section. How would your organ project if grant funding discontinued?

0 \$ 0.00

0.00

0

	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	0 \$ 0.00	0
		00
Total	0 \$ 0.00 \$0	00

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * 2023 CAFR (2024 Not Available Until After Deadline) DRAFT 2024 ACFR
Travel Policy	✓	<u>Travel Policy</u>
Payroll Policy	✓	Time and Attendance
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	Milestone Schedule

 $^{^*\}mbox{\it ZoomGrants}^{\mbox{\tiny TM}}$ is not responsible for the content of uploaded documents.

Application ID: 484971

Become a fan of ZoomGrants** on Facebook
Problems* Confact us at Questions* ZoomGrants.com
(2002-2024 Grantshyst.com. All rights reserved.
"ZoomGrants* and the ZoomGrants top are trademarks of Grant-Analyst.com, LLC.
LCC

_			
	Applicant Name	CLARK COUNTY WATER RECLAMATION D	ISTRICT
	Project Name:	Firewall Improvement for Clark Cour	ty 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



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 FFY	24
Jump to: Pre	-Application Application Questions Line Item Detail Budg	<u>det Document Uploads</u>
\$ 148,000.00 Requested Submitted: 10/28/2024 2:18:39 PM (Pacific) Project Contact Diana Clarkson d14977c@lympd.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 i13700p@lvmpd.com	Telephone 702-828-2831 Fax Web UEI SAM Expires
district, council of government, regional governm public entity, tribe, or authorized tribal organizati	nent entity, agency or instrumentality of a local governon.	p, local public authority, school district, special district, intrastate iment, rural community, unincorporated town or village, or other urisdictions. A template for obtaining this consent will be provided.
achieving this goal? (If not, the project is not eligi ✓ Yes □ No	ible for SLCGP funding).	and reducing systemic cyber risk. Does your project proposal aid in Begin to the contract of
Meeting dates are to be determined and will be comm I understand and agree. 4. All procurement is required to be compliant wi **Per FEMA legal opinion, locals may NOT use NI section for further justification).** All procurement and minority businesses, women's business enter practicable under a federal award, provide a prefer art 200.322. Any sole source procurement must You may view FEMA's written legal opinion on NRS I understand and agree. 5. Supplanting is prohibited under this grant. I understand and agree. 7. Each jurisdiction must complete its own application agrant. Subgrantees may not pass through or supplied in the prohibited understand and agree. 8. Subrecipients (i.e., agencies receiving this funsubawards. I understand and agree Application Questions top	RS 332.115 because it has been determined that NRS it must be free and open competition. Applicants are a gerprises, and labor surplus area firms per 2 C.F.R. Par erence for the purchase, acquisition, or use of goods, be pre-approved in writing by the Division of Emerge 332.115, along with DEM's procurement policy and FEM/opplanting occurs when a subapplicant reduces their out same activity. Interpretation of the grant application will be the action. The submitter of the grant application will be the abgrant funds to other agencies/organizations. Interpretation of the grant application will be the adding through the Nevada Division of Emergency Management of the grant application of Emergency Management of the Service of the Service of Emergency Management of the Service of Emergency Management of the Service of Emergency Management of the Service of the Service of Emergency Management of the Service of Emergency Management of the Service of the Service of Emergency Management of the Service of the Service of Emergency Management of the Service of the Service of Service of the Service of Serv	STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources also required to follow the socioeconomic steps in soliciting small to 20.321. All non-federal entities should also, to the greatest extent products, or materials produced in the United States, per 2 C.F.R. nory Management (DEM) in advance of the procurement. As contract provisions guide, in the "Resource Document" tab. Inward agency's funds for an activity because federal funds are asse acknowledge your understanding and agreement of this are recipient of funds. Without an application, DEM is unable to issue agement) may not use this funding to administer their own
	encompassing a population of less than 50,000 peop or project will support rural communities, select "No" and in	le)? dicate in your narrative what percentage of your project will directly
		most closely aligns. or revising cybersecurity plans, to improve capabilities to respond to

☐ 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 with	in the state, and the
information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported 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 state or local governments within the state.	by, or on behalf of, the
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state 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 threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the	
 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 	a gov internet demain
7. Ensure continuity of operations of the state or local governments within the state, including through the use of the a cybersecurity incident, including by conducting exercises the acybersecurity incident.	•
8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.	, and abilities of personnel
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 evinvolving those communications or data networks.	ent of an incident
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the may impact the performance of information systems within the jurisdiction of the state.	degradation of which
■ 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 wit consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.	hin the state should be
□ 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 proirity of enhancing cybersecurity. The threat of a cyber-at government agencies has increased dramatically. The purpose of this proposed project is to better target harden the largest law enforcement agency in the state our security posture to counter terrorism threats by utilizing established industry best practices. This will involve cybersecurity training, ransomware protection with 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 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 part 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 cybersecurity protecting our systems, law enforcement would be severely disrupted.	of Nevada by increasing KnownBe4 or something agency, it would impact artner agencies as well as
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 interproblems of social engineering, spear-phishing, and ransomware attacks and at the same time stay compliant with industry regulations like PCI, HIPAA, SOX, FFI KnowBe4 platform allows the LVMPD to provide mandatory cyber security awareness training on a continued basis to employees, which dramatically increases the LVMPD. Thycotic Behavioral Analytics provides a cloud-based solution that utilizes advanced machine learning technology to analyze privileged account activity w 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 invo privileged account credentials. These attacks are hard to discover and can go undetected for months. Examples of capabilities include two factor authentication, roweb password filler, password hiding, IP restrictions, and various service management capabilities.	ge the urgent IT security EC and GLBA.The e security posture of the rithin Thycotic Secret live compromised
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. encompasses all of Clark County, Nevada. Within Clark County, there are multiple law enforcement agencies and government partners who utilize and rely upon Linformation technology (IT) resources. These IT resources play an integral level in sharing public safety information among partner agencies as well as protecting the appropriate cybersecurity protecting our systems, law enforcement would be severely disrupted. The project's goal is to ensure that Law Enforcement is able to addeter and respond to acts of terrorism. Without appropriate cybersecurity protecting our systems, law enforcement would be severely disrupted.	VMPD managed e community. Without
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.	
 ■ Actively engage in bidirectional sharing between CISA and SET 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-servicesNationwide 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 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
PLAN	NING COSTS ng Cost Line Item Description Description Description Description Unit Total project as described in the Application Questions section. Which is element tie into the project if project as described in the Application Questions section. Grant funding was reduced or discontinued?
	\$ \$ \$
	\$ \$ \$
	\$ \$ \$
	\$
	\$ \$
	0 0.00 \$ 0.00
	NIZATION COSTS zational Cost Line Item Oversity. Unit Total Describe how the purchase(s) within this element tie into the How would your organization sustain this project if
Name	Description Cost project as described in the Application Questions section. grant funding was reduced or discontinued?
	\$
	\$ \$
	\$ \$ \$ \$
	\$ \$
	\$ \$ \$ \$
	\$ \$ \$ \$
	\$ \$
	\$ \$ \$ \$ \$ \$

Equipment Line Item Cost Name Description KnownBe4 KnownBe4 Security Training KnownBe4 KnownBe4 Rule K					0.00			
Line Item Cost Name Cost					0.00			
Security			Unit Cost	Total	the purchase (s) within this element tie into the project as described in the Application	How would your organization sustain this project if grant funding was reduced or	https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info	- https://www.fema.gov/grants/tools/authorized-
KnownBe4 KnownBe4 1 \$ The KnowBe4 We would lose Software, Network 04SW-04-NETW PhishER PhishER 28,000.00 28,000.00 platform or something similar allows the LVMPD to provide	Security Awareness	Security Awareness			section. 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, spearphishing, and ransomware attacks and at the same time stay compliant with industry regulations like PCI, HIPAA, SOX, FFIEC	this capability	Software, Malware/Anti-Vi	05HS-00-MALW
mandatory cyber security awareness training on a continued basis to employees, which dramatically increases the security posture of the LVMPD.	PhishER	PhishER			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		Software, Network	04SW-04-NETW
Thycotic Thycotic Privilege Privilege Privilege Access Access Access Management Management Management Management Management Management Service Access	Privilege Access	Privilege Access	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	this capability	Software, Malware/Anti-Vi	05HS-00-MALW

\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
3 \$	\$
148,000.00 148,00	0.00

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total ti	Describe how the purchase(s) within this element is into the project as described in the Application Duestions 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
				0.00			

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
				0.00			
Total		0	\$ 0.00	\$0.00			0

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * Single Audit
Travel Policy	✓	Travel policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	LVMPD Cyber FFY24 SLCGP Milestones

 $^{^{\}star}\textit{ZoomGrants}^{\intercal \! \! M}$ is not responsible for the content of uploaded documents.

Application ID: 485102

Become a fan of ZoomGrants¹¹¹ 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 Loout I Browset.

	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



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

Web

UEI TUFEHHFJ2P79 SAM Expires2/26/2025

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

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,

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.

✓ 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-as-ervice." 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-

(cisecu												
		ady participat	ting in the C	whor Hygiana Sa	niooo ond	Nationwide Cybe	roogurity Povi	iou (NCS	'D)			
						•	•	•	•	ands we will b	oe reau	ired to sign up for the
	ur project is aw		., ,	, , , ,			,	()	,			3 17 1 1
12. Pro	vide the 5-digi	it zip code w	here the pr	oject will be ex	ecuted.							
	oject location co	ould be differe	ent than the	sub-recipient ad	ldress.							
89431												
			any part o	of it be reduced	or expand	led? Describe t	he ways in wl	hich the	project can	be reduced	or exp	anded, or the
	s why it canno s proiect is scal		for expans	ion or reduction	as needed.							
	. ,						ications movin		l a unifical ata	ata idantitu av	atam w	bara a ainala lagin
						ould also be add						here a single login
				high-priority ND active accounts la		ons can be integr	ated initially, w	vith other	applications	added in pha	ases. Si	imilarly, user migratio
This flex	xibility ensures t	the project alig	gns with ND	A's resources w	nile laying g	groundwork for a	comprehensiv	e state-w	vide identity r	management s	system.	
	• •			other jurisdic		es). Select "No" i	if the project p	rimarily s	supporte a ci	nalo ontitu		
☐ Yes	s	ect supports i	тишре јин	saictions (e.g., i	пишрів спі	es). Select 100 l	i trie project p	riiriariiy s	виррона а зн	rigie erilly.		
▼ NO												
	in" if the proje					a new capabilit ng/current level		nt of the	project is to	o close a cap	ability	gap. Select
☐ Sus	stain											
16. If th	nis project is s	ustaining a p	oreviously a	awarded SLCG	P project,	please provide	the fiscal yea	r and pr	oject name	of the origin	al proj	ect.
N/A		J.,	,		1 - 2		, , , , , , , , , , , , , , , , , , , ,					
17. Plea	ase select all a	applicable pl	anning, or	ganization, equ	ipment, tra	aining, and exe	cise (POETE) elemen	ts for which	n fundina is l	beina s	sought for this
project	: .					-	•	•		•		•
			ies, plans, p	procedures, mutu	al aid agre	ements, strategie	es, and other p	ublication	ns; also invol	ves the collec	ction an	d analysis of
	elligence and inf		an overall o	organizational etr	icture and	leadership at eac	h level in the s	structure				
	uipment - Equip			•				Structure				
			is. and syste		with relevar	nt standards						
☐ Tra	ining - Content											
	•	and methods	of delivery t	that comply with	elevant tra		nprove their ov	wn perfori	mance, and	identify oppor	tunities	s to improve
☐ Exe	•	and methods -on activities	of delivery t which enhar	that comply with	elevant tra	ining standards	nprove their ov	wn perfor	mance, and	identify oppor	tunities	s to improve
☐ Exe	ercises - Hands	and methods -on activities	of delivery t which enhar	that comply with	elevant tra	ining standards	nprove their ov	wn perfori	mance, and	identify oppor	tunities	s to improve
☐ Exe	ercises - Hands pabilities to resp	and methods -on activities	of delivery t which enhar	that comply with	elevant tra	ining standards	nprove their ov	wn perfor	mance, and	identify oppor	tunities	s to improve
☐ Exe cap	ercises - Hands pabilities to resp	and methods -on activities	of delivery t which enhar	that comply with	elevant tra	ining standards	nprove their ov	wn perfor	mance, and	identify oppor	tunities	s to improve
□ Exe cap e Item Detail	ercises - Hands pabilities to resp Budget <u>top</u>	and methods -on activities	of delivery t which enhar	that comply with	elevant tra	ining standards	nprove their ov	wn perfori	mance, and	identify oppor	tunities	s to improve
☐ Exe cap	ercises - Hands pabilities to resp Budget <u>top</u>	and methods -on activities	of delivery t which enhar	that comply with nce knowledge o	elevant tra f plans, allo	ining standards ow members to ir			mance, and	identify oppor	tunities	s to improve
Exector Executor Exector Exector Exector Exector Executor	ercises - Hands pabilities to resp Budget <u>top</u>	and methods -on activities	of delivery t which enhar vents	that comply with nce knowledge of Describe how	the purch	ining standards	his element ti	e into	How would	l your organi	ization	s to improve sustain this projec or discontinued?
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery to which enhance vents Unit Cost	chat comply with nce knowledge of Describe how al the project as	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exected Execution Executio	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery to which enhance vents Unit Cost	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery to which enhance vents Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery to which enhance vents Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exector Executor Exector Exector Exector Exector Executor	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery to which enhance vents Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery t which enhant vents Unit Cost October 100	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery to which enhance wents Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exector Executor Exector Exector Exector Exector Executor	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	of delivery to which enhance wents Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	Unit Cost	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exector Executor Exector Exector Exector Exector Executor	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	Unit Cost	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exector Executor Exector Exector Exector Exector Executor	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	Unit Cost	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exector Executor Exector Exector Exector Exector Executor	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	Unit Cost	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Exectant Execution	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real evanuation	Unit Cost Unit Cost	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Execution Eltem Detail ANNING C Inning L	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real ev	Unit Cost Unit Cost	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exectant Exectant Execution Eltem Detail ANNING C Inning L	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real evanuation	Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization	sustain this projec
Exercise Item Detail ANNING C Inning L Ist Name I	ercises - Hands pabilities to resp Budget top COSTS Line Item	and methods s-on activities cond to real evanuation	Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti	e into	How would	l your organi	ization duced (sustain this projec or discontinued?
Exercise Item Detail ANNING Conning Let Name I	ercises - Hands pabilities to resp Budget top COSTS Line Item Description	and methods s-on activities cond to real evanuation	Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to in hase(s) within the din the Applica	his element ti	e into	How would if grant fun	l your organi ding was rec	ization duced (sustain this projector discontinued?
Exercise Item Detail ANNING Conning Let Name I	ercises - Hands pabilities to resp Budget top COSTS Line Item Description	and methods s-on activities cond to real evanuation. Quantity	Unit Cost Total	Describe hoval the project as section.	the purch	ining standards ow members to ir	his element ti tion Question	e into	How would if grant fun	your organi	ization duced d	sustain this projector discontinued? How would your organization sustaithis project if grant funding was reduced.
Exercise Item Detail ANNING Conning Let Name Conning Let	Budget top OSTS Line Item Description	Quantity O	Unit Cost Total	Describe how at the project as section.	the purch	ining standards by members to in hase(s) within the Applica	his element ti tion Question	e into ns	How would if grant fun this eleme on Question	l your organi ding was rec nt tie into the ns section.	ization duced d	sustain this projector discontinued? How would your organization sustain this project if grant

	security features, testir support for transitioning single sign-on system	g NDA's to Azure		reconfiguring NDA multi-factor auther	stem (NVDIS). This includes migrating us a applications, and ensuring robust secur atication and user access tracking. By ha	ity through ndling the
	Entra ID and Azure AD under the NVDIS frame	B2C		project's complex goals of reducing	technical requirements, the vendor supp cybersecurity risks, improving user accord providing secure, streamlined access to	orts NDA's unt
				\$		
				\$		
				\$		
			·	\$		
				\$		
			·	\$		
				\$		
				\$		
			·	\$		
				\$		
			1 \$ 39,600.00 39,600.0	\$ 0		
EQUIPME	NT COSTS					
		Describe how the				
		purchase (s) within	How would your			
Equipment,	Day Barre	this element tie	organization	Name - Search	AEL Numbe	r - Search
Cost	Line Item Quantity Cost Description	Total into the	project if grant https	s://www.fema.gov/ pment-list to find /	grants/tools/authorized- https://www	.fema.gov/grants/tools/authorized- ist to find AEL info
Name		project as described	funding was Equi	pment-list to find A	AEL IIIIO equipment-i	IST TO TING ALL INIO
		in the Application	diagontinuo d?			
		Questions				
	\$	section.				
	\$	\$				
	\$	\$				
	\$ \$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$ \$	\$				
	\$	\$				
	\$	\$				
	\$ \$	\$				
	0 \$	\$ \$				
	0.00	0.00				
TRAINING	COSTS	Des	cribe how the purchas	eo(e) within this	How would your organization such	ain Do you plan to coordinate
Training Cost Name	Line Item Description Quantity	Cook Total elem	ent tie into the projec	t as described in	How would your organization susta this project if grant funding was	this training with the State
		tile r	Application Questions	s section.	reduced or discontinued?	Training Officer?
		\$ \$ \$ \$				
		\$ \$				
		\$ \$				
		\$ \$ \$ \$				
		\$ \$				
		\$ \$				
		\$ \$				
		\$ \$ \$ \$				
		\$ \$				
		\$ \$				
	0	\$ \$ \$ \$				0
	o d	0.00 0.00				U

EXERCISE	COSTS					
Exercise Cost Name	Line Item Description	Quantity	Unit T	Describe how the purchase(s) w otal element tie into the project as de the Application Questions sectio	scribed in this project if grant funding was	n Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		0	\$ 0.00	\$		0
				0.00		
Total		0	\$ 0.00 \$	0.00		0

Document Uploads \underline{top}

Documents Requested * A-133 Audit (Most Current)	Required?	Attached Documents * 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 <u>lan of ZoomGrants</u> on Facebook
Problems? Confact us at <u>Questions B ZoomGrants.com</u>
Problems? Confact us at <u>Questions B ZoomGrants.com</u>
ZoomGrants on the ZoomGrants logs are trademarks of GrantAnalyst.com, LLC.

<u>Location</u> <u>Browners</u>

	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



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

Powered by ZoomGrants Mand		
Nevada Office of the Military, Division of Emergency Management		
FFY 2024 State and Local Cybersecurity Grant Program (SLCGP) Deadline: 11/1/2024		
Nevad	a Department of Transportation - Cybersecurity FY 2024 SLCGP NDOT	
Jump to: Pre-Application	Application Questions Line Item Detail Budget Doc	sument Uploads
\$ 2,253,244.00 Requested	Nevada Department of Transportation - Cybersecurity	
Submitted: 10/18/2024 4:09:52 PM (Pacific) Project Contact	1263 S Stewart St Carson City, NV 89712	——— Telephone 7757724297 Fax Web UEI
Rick Hays thays@dot.nv.gov Tel: 7757724297	United States Chief Accountant Tiffany Smorra	SAM Expires
Additional Contacts christopherjohnson@dot.nv.gov	TSmorra@dot.nv.gov	
Pre-Application too	_	
 Is your organization one of the following types of entities?: Co council of government, regional government entity, agency or in or authorized tribal organization. Be advised that state agencies receiving SLCGP funds will have to over the council or the state agencies receiving states. 	strumentality of a local government, rural commu	nity, unincorporated town or village, or other public entity, tribe,
□ No		
2. All funds granted under the State and Local Cybersecurity Grachieving this goal? (If not, the project is not eligible for SLCGP ✓ Yes □ No		ng systemic cyber risk. Does your project proposal aid in
3. In order for your application to be considered, you must atten you do not send representation to the required meetings, your a Meeting dates are to be determined and will be communicated to SL I understand and agree.	pplication will not be considered.	r's Cybersecurity Task Force. This is a requirement of the grant. If
4. All procurement is required to be compliant with Nevada Revi FEMA legal opinion, locals may NOT use NRS 332.115 because i further justification).** All procurement must be free and open of businesses, women's business enterprises, and labor surplus a federal award, provide a preference for the purchase, acquisition procurement must be pre-approved in writing by the Division of You may view FEMA's written legal opinion on NRS 332.115, along to I understand and agree.	it has been determined that NRS 332.115 is less re ompetition. Applicants are also required to follow rea firms per 2 C.F.R. Part 200.321. All non-federa n, or use of goods, products, or materials product Emergency Management (DEM) in advance of the	estrictive than 2 C.F.R. Part 200 (see Resources section for the socioeconomic steps in soliciting small and minority I entities should also, to the greatest extent practicable under a ad in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement.
 5. Supplanting is prohibited under this grant. Supplanting occur expected to be available) to fund that same activity. I attest that funding for this project does not currently exist within or 		's funds for an activity because federal funds are available (or
 6. Entities applying as a subgrantee must meet a 30% cost share I understand and agree. 	e requirement for FY 2024 SLCGP. Please acknow	ledge your understanding and agreement of this requirement.
 7. Each jurisdiction must complete its own application. The subs Subgrantees may not pass through or subgrant funds to other a I understand and agree. 		of funds. Without an application, DEM is unable to issue a grant.
 8. Subrecipients (i.e., agencies receiving this funding through the I understand and agree 	ne Nevada Division of Emergency Management) m	ay not use this funding to administer their own subawards.
Application Questions top		
1. Is this agency considered a rural area (an area encompassing If your agency is not considered a rural area, but your project will sup Nevadans. Yes		ur narrative what percentage of your project will directly benefit rural
✓ No		
incidents and ensure continuity of operations. Objective 2: Understand their current cybersecurity posture and ar	ures, including developing, implementing, or revising of eas for improvement based on continuous testing, eva	ybersecurity plans, to improve capabilities to respond to cybersecurity
 Objective 3: Implement security protections commensurate with ris Objective 4: Ensure organization personnel are appropriately train 		

- 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 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

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
 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
 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 Esplanation: 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 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. Decay years and decay any of the fallowing Very Cybersequeity Post Decations 2	
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 tic 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 ite	
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 author	orized 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	ces 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 Si	atellite 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.	atomic internet dystem will help
The purchase and installation of the security cameras will be used to continuously monitor the critical infrastructure and cybersecurity equipment across NDOT and en	sures 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 facilitie include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure 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 SLCGP NOFO.	re, layout, systems, or critical
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 service Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and post-award requirement. —Cyber Hygiene Services—Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "here accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance see industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulne 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 more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services Review (NCSR)—The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity progra. National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipient NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nati 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) but understands we will be required to sign up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR) but understands we will be required to sign up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR) but	d approval of a grant but is a alth" of your publicly curity in accordance with of public, static IPs for lerability_info@cisa.dhs.gov vice as part of the SLGCP. sNationwide Cybersecurity ams. It is based on the is should complete the ionwide Cybersecurity
☑ 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	or 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 responsible to the project is scalable at the organization's desire once built and will be expanded.	easons why it cannot.
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 "su maintains a core capability at its existing/current level.	ustain" if the project strictly
□ 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 Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of inte 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	

								y with relevant tra edge of plans, al		mprove their own performance, and	l identify opportu	nities to improve capabilities to respond to real
Line Item Det	ail Budget <u>t</u>	<u>op</u>										
PLANNING Planning Cos Name			Quan		Unit Cost	Total			rchase(s) within opplication Ques	n this element tie into the project stions section.		rour organization sustain this project if grant reduced or discontinued?
						\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$						
				0	0.00	0.00						
ORGANIZA Organization Name	al Cost Lin		n '	Quanti		Unit Cost \$	Total \$	Describe how tl project as desc	ne purchase(s) v	within this element tie into the lication Questions section.		d your organization sustain this project if grant as reduced or discontinued?
						\$ \$ \$ \$	\$ \$ \$					
						\$ \$ \$	\$ \$ \$					
						\$	\$					
				(0 \$ (\$ 0.00					
EQUIPMEN	IT COSTS											
Equipment		Oua	ntity	Unit C	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?	equipment-list to find AEL info	ools/authorized	AEL Number - Search - https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Switches with Network Access Control (NAC) Policies	Control solutions	ed th	1 \$	23,30	4.00 \$	23,	304.00	Support network security activity for NAC		Switch, Network		04HW-03-SWCH
Routers	A router is a device that connects tw or more packet- switched networks or subnetworks	0	1 \$	66,39	3.00 \$	66,	393.00	Support network security activity for NAC, Provide Stealth Networking and Resiliency	security operations at a reduced	Router		04HW-03-ROUT

	convoc hus							
	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 firewall 12345. NGFWs are deep-packet inspection firewall sthat 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	security	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	secure remote locations for	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	security	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	operations at a reduced	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, Vulner	ability Scan	05NP-00-SCAN	
Authentication Devices	•	150	\$ 115.00	\$ 17,250.00	Authentication	Will maintain security operations at a reduced effectiveness	Device, Biom	etric User Au	05AU-00-BIOM	
Forensics Lab	Forensic Laptops, Imagers, and Media	1	\$ 192,083.00		Will allow for	Will maintain security f operations at a reduced effectiveness	Forensics, So	oftware	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		Equipment, S	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			continuous monitoring via video surveillance, which creates vulnerabilities of critical		mation Techn	05SM-00-ITAM	
			\$	\$						
			\$ \$	\$						
		165	\$	\$ 253 244 00						
			2,146,109.00	2,253,244.00						
TRAINING	COSTS									
Training Cost Name	Line Item	Quantit	Unit y Cost Tota	l into the pr	oject as describ	se(s) within this sed in the Applic	ation	How would your organiz project if grant funding v	ation sustain this vas reduced or	Do you plan to coordinate this training with the State Training
JJSE HAIRE	Description		\$ \$	Questions	section.			discontinued?		Officer?

\$ \$ \$ \$

\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
0 \$ 0.00		0
	0.00	

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total in	escribe how the purchase(s) within this element tie to the project as described in the Application uestions 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

Document Uploads \underline{top}

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	<u>Travel Policy</u>
		<u>Audit</u>
		Nevada Single Audit Report
		Milestones NDOT Cybersecurity Equipment Needs
Travel Policy	✓	Travel Policy
Payroll Policy	✓	<u>Payroll</u>
Procurement Policy	✓	Procurement Policy
Milestones	✓	Milestones FY 2024 NDOT
download template		Milestones NDOT Cybersecurity Equipment Needs
		Milestones NDOT Cybersecurity Equipment Needs

 $^{^*\}ensuremath{\textit{ZoomGrants}}^{\ensuremath{\textit{TM}}}$ is not responsible for the content of uploaded documents.

Application ID: 484405

Become a fan of ZoomGrants™ on Facebook
Probleme? Cortiact us at <u>Cuestors ® ZoomGrants com</u>
©ZoomGrants com
Grants° and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Loow I 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
	Willestone Description	Bute 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
2	Next-Generation Firewalls (NGFWs); purchase equipment; train personnel and	
3	deploy equipment; and maintain equipment	Friday, November 28, 2025
	Cellular Routers; purchase equipment; train personnel and deploy equipment;	
4	and maintain equipment	Friday, November 28, 2025
5	Wireless Access Points (APs); purchase equipment; train personnel and deploy	
5	equipment; and maintain equipment	Friday, November 28, 2025
6	WAN-in-a-Box; purchase equipment; train personnel and deploy equipment;	
О	and maintain equipment	Friday, November 28, 2025
_	Network Testing Tools; purchase equipment; train personnel and deploy	
/	equipment; and maintain equipment	Friday, November 28, 2025
	Authentication Devices; purchase equipment; train personnel and deploy	
9	equipment; and maintain equipment	Friday, November 28, 2025
10	Forensics Lab; purchase equipment; train personnel and deploy equipment; and	
10	maintain equipment	Friday, November 28, 2025
11	Satellite Internet System; purchase equipment; train personnel and deploy	
11	equipment; and maintain equipment	Friday, November 28, 2025
12	Security Cameras with Installation; purchase equipment; train personnel and	
_12	deploy equipment; and maintain equipment	Friday, November 28, 2025
13		

^{*}Please add additional rows as necessary for your project



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 Reques	ested
-----------------------------	-------

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

Project Contact

Tiffany Morelli <u>tiffanymorelli@it.nv.gov</u> 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.
 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; Ijean@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

and a asse ways exec regis body https annu Tech MS-I: https	approval of a grant but is a post- sses the "health" of your public s to enhance security in accorda cuting continuous scans of public ster for these services, email vult y of your email that you are reque s://www.cisa.gov/topics/cyber-th ual self-assessment designed to mology Cybersecurity Framewo SAC, during the first year of the s://www.cisecurity.org/ms-isac/s	-award requirementCyber Hygier ly accessible web applications by connect with industry and government c, static IPs for accessible services nerability info@cisa.dhs.gov with cesting this service as part of the SL areats-and-advisories/cyber-hygien measure gaps and capabilities of the award/subaward period of perform ervices/ncsr (cisecurity.org).	ne Services Web Application Scanning thecking for known vulnerabilities and value and the practices and standards. Vulnerabilities and vulnerabilities. This service provict the subject line "Requesting Cyber Hyg GCP. For more information, visit CISA's e-services Nationwide Cybersecurity a SLT's cybersecurity programs. It is base MS-ISAC. Entities and their subreciping the subreciping such services and subreciping such services.	e note that participation is not required for submission g is an "internet scanning-as-a-service." This service weak configurations. Additionally, CISA can recommend oility Scanning evaluates external network presence by des weekly vulnerability reports and ad-hoc alerts. To iene Services – SLCGP" to get started. Indicate in the s Cyber Hygiene Information Page: Review (NCSR) The NCSR is a free, anonymous, sed on the National Institute of Standards and ients should complete the NCSR, administered by the on, visit Nationwide Cybersecurity Review (NCSR)
□ (i	Our agency has not yet signed up fois awarded	or the Cyber Hygiene Services or Natio		nderstands we will be required to sign up for them if our project
	Provide the 5-digit zip code where project location could be different to 11			
13. Is cann		y part of it be reduced or expanded	? Describe the ways in which the project	ct can be reduced or expanded, or the reasons why it
This		he license funding. It would be possible	e to reduce the costs by reducing the number	er of political subdivisions to be licenses. Initially, we've scoped
Sele∈ ✓ \	Yes		. Select "No" if the project primarily suppor	ts a single entity.
1				
proje	<mark>ect strictly maintains a core capa</mark> Build	this project focuses on starting a ribility at its existing/current level.	new capability, or the intent of the projec	ct is to close a capability gap. Select "sustain" if the
₹ (Sustain			
	f this project is sustaining a prev 2021 Homeland Security Grant Pro		ease provide the fiscal year and project	name of the original project.
F i (v T E	Planning - Development of policies, information Organization - Individual teams, an o Equipment - Equipment, supplies, a Training - Content and methods of d	plans, procedures, mutual aid agreem overall organizational structure, and lea nd systems that comply with relevant s lelivery that comply with relevant trainir	ents, strategies, and other publications; also idership at each level in the structure itandards ig standards	which funding is being sought for this project. o involves the collection and analysis of intelligence and e, and identify opportunities to improve capabilities to respond
Line Item Deta	ail Budget <u>top</u>			
Line Item Deta PLANNING Planning Cos Name	COSTS		se(s) within this element tie into the ne Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
PLANNING Planning Cos	COSTS	ost project as described in the		
PLANNING Planning Cos	COSTS	ost project as described in the		
PLANNING Planning Cos	COSTS	ost Total project as described in the		
PLANNING Planning Cos	COSTS	ost Project as described in the same state of th		
PLANNING Planning Cos	COSTS	ost Total project as described in the		
PLANNING Planning Cos	COSTS	ost Project as described in the second secon		
PLANNING Planning Cos	COSTS	ost Project as described in the second secon		
PLANNING Planning Cos	COSTS	ost Project as described in the second secon		
PLANNING Planning Cos	COSTS	ost Project as described in the second secon		
PLANNING Planning Cos	COSTS	ost Project as described in the second secon		
PLANNING Planning Cos	COSTS It Line Item Quantity C Description Quantity C	ost Project as described in the state of the		
PLANNING Planning Cos	COSTS It Line Item Quantity C Description Quantity C	ost Project as described in the state of the		
PLANNING Planning Cos	COSTS It Line Item Quantity C Description Quantity C	ost Project as described in the state of the		
PLANNING Planning Cos Name	COSTS It Line Item Quantity C Description Quantity C	ost Project as described in the state of the		
PLANNING Planning Cos Name	COSTS at Line Item Quantity Company Cost Line Item 0 0	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name	COSTS It Line Item Quantity C Description 0 0	ost Total project as described in the state of the state	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name ORGANIZA Organizationa	COSTS It Line Item Quantity C Description 0 0 TION COSTS al Cost Line Item Quantity	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name ORGANIZA Organizationa	COSTS It Line Item Quantity C Description 0 0 TION COSTS al Cost Line Item Quantity	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name ORGANIZA Organizationa	COSTS It Line Item Quantity C Description 0 0 TION COSTS al Cost Line Item Quantity	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name ORGANIZA Organizationa	COSTS It Line Item Quantity C Description 0 0 TION COSTS al Cost Line Item Quantity	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name ORGANIZA Organizationa	COSTS It Line Item Quantity C Description 0 0 TION COSTS al Cost Line Item Quantity	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name ORGANIZA Organizationa	COSTS It Line Item Quantity C Description 0 0 TION COSTS al Cost Line Item Quantity	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?
PLANNING Planning Cos Name ORGANIZA Organizationa	COSTS It Line Item Quantity C Description 0 0 TION COSTS al Cost Line Item Quantity	ost Project as described in the state of the	ne Application Questions section.	grant funding was reduced or discontinued?

		\$ \$ \$ \$		
		\$ \$		
	0 \$	0.00 \$		
		0.00		
EQUIPMENT COSTS				
EQUIFWENT COSTS		Describe how		
Equipment Line Item Cost Name Description Quantity	Unit T	into the otal project as described in	oroject if grant equipunding was	Name - Search AEL Number - Search s://www.fema.gov/grants/tools/authorized- https://www.fema.gov/grants/tools/authorized- pment-list to find AEL info equipment-list to find AEL info
		Application	educed or discontinued?	
Public 35 Sector Digital Services Professional - Fulfiller	\$ 6,370.92 222,982	access to the tool which will allow agencies	equest will cover OCIO costs through	AEL information to be completed if project is awarded (further information required) - AJ 11/06/24
User v2 (2 years)		experiences in using cybersecurity tools and maintain a centralized asset repository to		
Business 8 Stakeholder User V4 (2 years)	\$ 5,317 664.65	7.20 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	request will cover OCIO costs through he new biennium. OCIO	NEL information to be completed if project is awarded (further information required) - AJ 11/06/24
	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
	\$ \$	\$		
	\$	\$		
43	\$ 7.035.57.229.200	\$		
TRAINING COSTS	7,035.57 228,299	7. ⇔U		

TRAINING COSTS

	Line Item Description	Quantity	Unit Cost	Total		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		Training is a one-time cost that would not be required to fund after the successful completion of the project.	No
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			

	\$	\$	
	\$	\$	
	¢ c	\$	
	Φ	Φ	
201	\$	\$	
	21,408.63 69,62	28.32	

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total el	escribe how the purchase(s) within this ement tie into the project as described in the oplication Questions section.	How would your organization sustain project if grant funding was reduced o discontinued?	
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		0	\$ 0.00	\$			0
				0.00			
Total		0	\$ 0.00	\$0.00			0

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * 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

 $^{^{\}star}\textit{ZoomGrants}^{\tau_{\textit{M}}}$ is not responsible for the content of uploaded documents.

Application ID: 485403

Become a fan of ZoomGansts 110 on Facebook
Problema? Contact us at Question of ZoomGrants com
62002-2004 Granthvalys.com. All rights reserved.
ZoomGrants' and the ZoomGrants or Endemarks of Granthvalyst.com, LLC.
LOOAL | Browser.

		Office of the Chief Information Officer Cyber Tool Tracking System 2.0 – (CTTS) 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



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

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

MAXGJADTHWV7 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
ı	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

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. Image: Provided the state of the state of the state of the state of the state in the event of an incident involving those communications or data networks.
Involving those communications of data fetworks. Involving those communicati
■ 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, 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:

httns:/	//www.cisa.gov/tonia	cs/cvhar-th	reate-and-ar	dvienriae/cv	ber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous, annual
					of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology
					MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during
					and annually. For more information, visit Nationwide Cybersecurity Review (NCSR)
https:/	//www.cisecurity.org	g/ms-isac/se	ervices/ncsr	r (cisecurity.	.org).
□ Oι	ur agency is already p	articipating i	n the Cyber F	Hygiene Serv	rices and Nationwide Cybersecurity Review (NCSR)
✓ Ou	ur agency has not vet	sianed up fo	r the Cyber H	Ivaiene Servi	ices or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project
	awarded	3		,5	
12 Pro	ovide the 5-digit zip	code where	the project	will be exe	cuted
	oject location could b				
89711		e umerem u	iaii iiie sub-i	ecipierit add	1633.
09/11					
12 lc 4	this project scaleab	lo2 Can any	, part of it be	o roducod o	r expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it
		ier Can any	part or it be	e reduced o	r expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it
canno			(b. a		depend the manifestation and additional and the manifestation and the second state of
vve car	n scale by expanding (or reducing t	ine number of	r starring nire	d and the positions needed based on the needs of our partner entities.
	this project shareab				
Select	"Yes" if the project su	upports multi	iple jurisdictio	ons (e.g., mι	ultiple cities). Select "No" if the project primarily supports a single entity.
✓ Ye	es				
□ No	n				
_ 110					
15 Du	ild or Suctain: Salar	ot "build" if	this project	focusos on	starting a new capability, or the intent of the project is to close a capability gap. Scloot "sustain" if the
					starting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if the
	t strictly maintains a	a core capai	Dility at its e	xisting/curr	ent level.
☐ Bu	uild				
✓ Su	ustain				
16. lf tl	his project is sustain	ning a previ	iously award	ded SLCGP	project, please provide the fiscal year and project name of the original project.
	Support Staff Kickstart		, arruit		
1 123 0	- apport oran Monoran	•			
17 DIA	asse select all annie	ahle nlanni	ina orazniza	ation equin	ment, training, and exercise (POETE) elements for which funding is being sought for this project.
	• • • • • • • • • • • • • • • • • • • •	•	U, U		
		of policies, p	pians, proced	dures, mutual	l aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and
int	formation				
✓ Or	rganization - Individual	l teams, an o	overall organiz	zational struc	ture, and leadership at each level in the structure
✓ Eo	quipment - Equipment,	. supplies, ar	nd systems th	nat comply wi	ith relevant standards
			•		levant training standards
	•		,		ů
		ctivities whic	ch enhance kr	nowledge of p	plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond
to	real events				
Line Item Detail	Rudget fon				
Line item Detail	budget <u>top</u>				
DI ANNING C	'ASTS				
PLANNING C	.0313				
	l ine Item	U	Init 🚅 De	escribe how	the purchase(s) within this element tie into the How would your organization sustain this project if
Planning Cost	Line Item				the purchase(s) within this element tie into the scribed in the Application Questions section. How would your organization sustain this project if grant funding was reduced or discontinued?
Planning Cost	l ine Item		ost Total pr		the purchase(s) within this element tie into the scribed in the Application Questions section. How would your organization sustain this project if grant funding was reduced or discontinued?
Planning Cost	Line Item		ost star pr		
Planning Cost	Line Item		ost Total pr		
Planning Cost	Line Item		ost s		
Planning Cost	Line Item		s s		
Planning Cost	Line Item		\$ \$ \$ \$ \$ \$		
Planning Cost	Line Item		s s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		s		
Planning Cost	Line Item		ost pri pri		
Planning Cost	Line Item		ost pri pri		
Planning Cost	Line Item		ost pri pri		
Planning Cost	Line Item	Co	ost		
Planning Cost	Line Item	Co	ost pri pri		
Planning Cost	Line Item	Co	ost		
Planning Cost	Line Item	Co	ost pri pri		
Planning Cost Name	Line Item Qu Description Qu	Co	ost pri pri		
Planning Cost	Line Item Qu Description Qu	Co	ost pri pri		
Planning Cost Name	Line Item Description Qu	Co	ost pri pri	oject as des	grant funding was reduced or discontinued? How would your organization sustain this
Planning Cost Name ORGANIZATI Organizational	Line Item Description Quality ION COSTS Line Item	0 0	s pri pri	Total	Describe how the purchase(s) within this element tie into the Power funding was reduced or discontinued?
Planning Cost Name	Line Item Description Qu	0 0	ost pri pri	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 as described in the Application Questions section.
Planning Cost Name ORGANIZATI Organizational Cost Name	Line Item Description Quality ION COSTS Line Item Description	0 0	ost pro	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 as described in the Application Questions section. How would your organization sustain this project if grant funding was reduced or discontinued?
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ION COSTS Line Item Description Staffing to support	0 0	ost production production	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 as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT We may look to subsidize the IRP efforts from other
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description Quality ION COSTS Line Item Description	0 0	ost production production	Total \$ 1 553,998.00	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT We may look to subsidize the IRP efforts from other partners within the State of Nevada, to include the rural entities. We sources within the State government. The most
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ION COSTS Line Item Description Staffing to support	0 0	ost production production	Total \$ 1 553,998.00	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT By creating an Incident Response Team we can support our SLTT By creating an Incident Response Team we can support our SLTT Can provide immediate assistance when any entity is experiencing likely approach if grant funding is reduced or likely approach if grant fun
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description Quality ION COSTS Line Item Description Staffing to support SLTT entities and	0 0	ost production production	Total 553,998.00	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT We may look to subsidize the IRP efforts from other partners within the State of Nevada, to include the rural entities. We sources within the State government. The most
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost production production	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We sources within the State of Nevada, to include the rural entities. We sources within the State of Nevada, to include the rural entities. We sources within the State government. The most can provide immediate assistance when any entity is experiencing a cyber threat or attack. Additionally, an IRT can advise and assist
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost production production	Total \$ 1 553,998.00	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total \$ 1553,998.00	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We sources within the State of Nevada, to include the rural entities. We sources within the State of Nevada, to include the rural entities. We sources within the State government. The most can provide immediate assistance when any entity is experiencing a cyber threat or attack. Additionally, an IRT can advise and assist
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total 553,998.00 6 6 6 6 6 6 6 6 6	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total \$ 1553,998.00	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total 553,998.00 6 6 6 6 6 6 6 6 6	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost production production	Total 553,998.00 \$	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost production production	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost production production	Total \$ 1 553,998.00 \$ \$ \$ \$ \$ \$ \$ \$ \$	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost production production	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total 553,998.00 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total 553,998.00 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total 553,998.00 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.
Planning Cost Name ORGANIZATI Organizational Cost Name Sustain	Line Item Description ON COSTS Line Item Description Staffing to support SLTT entities and create an incident	0 0	ost pri pri	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By creating an Incident Response Team we can support our SLTT partners within the State of Nevada, to include the rural entities. We accomprovide 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 sources of funding or wait until the next legislative.

				9						
			3 18	4,666.0	\$ 0 553,998.00					
EQUIPMENT	COSTS				Describe					
Equipment Cos [,] Name	: Line Item Description	n Quantity	Unit Cost	Tota	how the purchase (s) within this element tie into the project as described in the Application Questions section.	project if grant funding was reduced or	equipment-iist t	na.gov/grants/tools/authoriz	AEL Number - ed- https://www.fe equipment-list	Search ema.gov/grants/tools/authorized- to find AEL info
Staff Support Hardware/Softwa	Hardware re and Software that the IRT staff will need to assist with their work for the state		\$ 2,000.00		This line item will support both the hardware and software needs of the IRT as they	If grant funding was reduced or a discontinued, OCDC would not be able to sustain the project in its e current form. We would look to maximize the impact of the IRT while on contract before the contract ultimately expired.		uter	04HW-01-INHW	V
			\$	\$		охриоц.				
			\$	\$						
			\$ \$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$ \$	\$						
		3	\$	\$						
			2,000.00)					
TRAINING CO	STS									
	e Item	Quantity	Unit Cost Tota	al tie int	ribe how the to the projections section	t as described i	ithin this elemen in the Application	t How would your organizat n project if grant funding wa discontinued?	ion sustain this s reduced or	Do you plan to coordinate thi training with the State Trainin Officer
			\$	\$						Silicon
				\$						
			\$	\$						
				\$						
				\$						
				\$ \$						
				\$ \$						
				\$						
				\$						
				\$						
				\$						
			\$	\$						

EX	_	\sim 1	CE	\sim		-
	EK.	u	36	UU	0	

\$ \$ 0 \$ 0.00 \$ 0.00

Exercise Cost Name	Line Item Description	Quantity	Unit T	Describe how the purchase(s) within this otal 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 \$ 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)	✓	<u>A-133 FY22</u>
Travel Policy	✓	DPS Travel Policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	IRT Grant Milestones

 $^{^{\}star}$ ZoomGrants $^{\text{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 485178

Bacome a <u>lan of ZoomGrants!**</u> on Facebook
Problema® Confact us at <u>Question all ZoomGrants com</u>
Problema® Confact us at <u>Question all ZoomGrants com</u>
"ZoomGrants" and the <u>ZoomGrants com</u>
"ZoomGrants" and the <u>ZoomGrants logs</u> are tackemarks of GrantAnalyst.com, LLC.
<u>Logorial Biomerar</u>

	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
	Policy/Planning: Incident response plans	
1	(IRPs) created for majority of counties	
	(10/17)	11/30/2027
	Operation: IRT able to assist in remediation	
2	and recovery after attack in majority of	
	incidents	11/30/2027
	Equipment: Provide state-approved	
3	equipment to contracted employees to	
3	ensure they are able to work on state	1-month after receiving grant
	systems and with SLTT partners	funding.
4		
5		
6		
7		
8		
9		
10		

^{*}Please add additional rows as necessary for your project



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

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.
✓ 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.
- Sijective 4. Ensure organization personner are appropriately statiled in dyboroccounty, 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.

Th ab to	ne desired outcome i	s a large perd abilities and in ading the netv	entage of public e dicators of compr ork. Finally, the gr	omise and alert the effe	n, and SLTT partners t ected entity. This ensu	ires a more robi	ust cybersecurity posture a	OC. The SOC would then be and a whole-of-state approach are they are able to adequately
(T a fu P	his prohibition doe building's structure	es not includ e, layout, sys le costs, plea understandin	e minor building stems, or critical ase refer to Secti	modifications neces	ssary to install and c g's safety, or otherwi	onnect grant-p	ourchased equipment th	other physical facilities. at do not substantially affect eful life of a building). For a
th fo a- A Si FF N. Cy IS po (c	e Cybersecurity ar or submission and a service." This serve diditionally, CISA co- canning evaluates ovides weekly vult Requesting Cyber lor more information ationwide Cyberse ybersecurity progra AC. Entities and the erformance and an isecurity.org).	Ind Infrastruction of a cice assesse an recomme external netheral netheral properties of the control of the con	ture Security Age grant but is a pe s the "health" of nd ways to enha work presence b ports and ad-hoc rices – SLCGP" s Cyber Hygiene w (NCSR) The N ed on the Nation ients should con tore information	ency (CISA). For these ost-award requiremency our publicly accessince security in accordance y executing continuous alerts. To register for get started. Indicate Information Page: half in a free, anony all Institute of Standaplete the NCSR, adr	se required services ntCyber Hygiene sible web application dance with industry bus scans of public, or these services, em te in the body of you ttps://www.cisa.govymous, annual self-fards and Technolog ninistered by the MS bersecurity Review of the sible services.	and members Services Wel is by checking and governme static IPs for a ail vulnerability email that you topics/cyber-tassessment de y Cybersecurity ISAC, during (NCSR) https://	hips, please note that pa b Application Scanning of for known vulnerabilities ent best practices and s ccessible services and s cy_info@cisa.dhs.gov w ou are requesting this se threats-and-advisories/o signed to measure gap; ty Framework and is spot the first year of the awa/www.cisecurity.org/ms	vulnerabilities. This service ith the subject line rvice as part of the SLGCP. cyber-hygiene-services. — s and capabilities of a SLT's onsored by DHS and the MS-rd/subaward period of
[Our agency has n if our project is aw		up for the Cyber H	ygiene Services or Nat	tionwide Cybersecurity	Review (NCSF	R), but understands we will	be required to sign up for them
T	2. Provide the 5-dig the project location of 19711							
re De th	asons why it canne epending on grant re	ot. sourcing, the re data for ma	project will be sca llicious cyber incic	lable. If the grant fundidents or indicators of co	ng is fully appropriated	d, OCDC will be		d or expanded, or the uses to more entities, allowing C, the less licenses OCDC will
S	I. Is this project shadelect "Yes" if the project Yes No			•	s). Select "No" if the p	roject primarily	supports a single entity.	
"s				focuses on starting a apability at its existin	• • • • • • • • • • • • • • • • • • • •	he intent of the	e project is to close a ca	pability gap. Select
	6. If this project is s Y23 OCDC Statewid	•	•	led SLCGP project, p	please provide the fis	scal year and p	project name of the origin	nal project.
pi [[[oject. Planning - Develo intelligence and in Organization - Ind Equipment - Equip Training - Content Exercises - Hands	pment of polic formation ividual teams oment, supplic and methods s-on activities	es, plans, proced an overall organizes, and systems the of delivery that co which enhance kr	ures, mutual aid agree ational structure, and l at comply with relevant mply with relevant train	ments, strategies, and eadership at each leve t standards ning standards	d other publication	ents for which funding is ons; also involves the colle	ection and analysis of
I ine Item I	capabilities to res	pond to real e	vents					
PLANNIN	IG COSTS		Dos	cribe how the purch	aco(c) within this old	mont tip into		
Planning Cost Nam	Line Item e Description	Quantity	Cost Total the	cribe how the purch project as described tion.				nization sustain this project educed or discontinued?
			\$					
			\$					
			\$					
			\$					
			\$					
			\$					

\$

		\$		
		\$		
		\$		
	0 0.00	\$		
		0.00		
ORGANIZATION (COSTS			
Organizational Coat			Describe how the purchase(s) within this H	low would your organization sustain this
Organizational Cost Name	Line Item Description Quant	tity Unit Cost	· · ·	roject if grant funding was reduced or iscontinued?
Direct Partner Outreach	Working with all state entities, including rural, to ensure smoother deployments of support projects.	1 \$ 20,000.00	20,000.00 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.	In y reduction or discontinuation of grant funding or partner outreach runs the risk of SLTT partners of having the information and hands on setup ecessary to join in on SOC services. Reducing he number of entities that opt-in to SOC services oses 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 create a conference or symposium to bring we together entities across the state to show them the value of opting-in to a managed SOC that is the contracted with the State. By bringing them we will be stated to show the state of t	
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	30,200.00 towards funding a third-party SOC and the licenses necessary for entities to have to provide the information needed to the SOC for	any reduction or discontinuation in grant funding or contracted SOC services or license will irectly impact the amount of support that the OC can provide and the amount of licenses that an be provided to entities that need them.
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$ \$	\$ \$	

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description Quantity		Total	this element tie into the project as	reduced or	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	\$)			

\$ \$ 365,200.00 365,200.00

TRAINING C	OSTS					
Training Cost Name	Line Item Description	Quantity	Unit Cost		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?	
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 a providing to the SOC and how they are handling the outcomes of the reports the SOC provides.	re
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		4	\$ 8,700.00	\$ 34,800.00		0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit T	otal	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

Document Uploads \underline{top}

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * A-133 FY22
Travel Policy	✓	DPS Travel Policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	Milestones Document

 $^{^{\}star}\textit{ZoomGrants}^{\text{\tiny{TM}}}$ is not responsible for the content of uploaded documents.

Application ID: 485184

	Applicant Name	Office of Cyber Defense Coordination
	Project Name:	Statewide SOC/ISAC
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
4	Increase enrolled entities to the SOC by	
1	50% from previous year.	30-Nov-26
	Purchase training vouchers in DEC or JUL,	
2	whichever comes first after appropriation	
	of award.	7/30/2025, 12/30/25
	Dissemination of 50% of training vouchers	
3	to rural entities to increase awareness and	
3	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



Nevada Office of the Military, Division of Emergency Management

Deadline: 11/1/2024	Washoe County	
	Vulnerability Management To	pol
Jump to: Pre-Application	Application Questions Line Item Detail I	Budget Document Uploads
\$ 275,000.00 Requested	Washoe County	
Submitted: 10/28/2024 10:27:49 AM (Pacific)	1001 E. 9th St.	Telephone (775) 328-2200
Project Contact	Reno, NV 89512 United States	Fax Web www.washoecounty.gov
Christopher Bower cbower@washoecounty.gov	IT Manager	UEI GPR1NY74XPQ5 SAM Expires
Tel: 7758585935	James Wood	·
Additional Contacts	jawood@washoecounty.gov	
none entered		
Pre-Application top		
Is your organization one of the following types of entitie	s?: County, municipality, city, town, tow	vnship, local public authority, school district, special district, intrastat
district, council of government, regional government entity public entity, tribe, or authorized tribal organization.	y, agency or instrumentality of a local g	overnment, rural community, unincorporated town or village, or other
Be advised that state agencies receiving SLCGP funds will ha	ve to obtain consent for their project from l	ocal jurisdictions. A template for obtaining this consent will be provided.
✓ Yes □ No		
All funds granted under the State and Local Cybersecul in achieving this goal? (If not, the project is not eligible for	, ,	ging and reducing systemic cyber risk. Does your project proposal a
✓ Yes	3,	
□ No		
		t of the Governor's Cybersecurity Task Force. This is a requirement o
the grant. If you do not send representation to the required Meeting dates are to be determined and will be communicated I understand and agree.		
Per FEMA legal opinion, locals may NOT use NRS 332.11 section for further justification). All procurement must be and minority businesses, women's business enterprises, extent practicable under a federal award, provide a prefer C.F.R. Part 200.322. Any sole source procurement must be	I5 because it has been determined that e free and open competition. Applicants and labor surplus area firms per 2 C.F.R ence for the purchase, acquisition, or us e pre-approved in writing by the Division	SING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENT NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources are also required to follow the socioeconomic steps in soliciting smat. Part 200.321. All non-federal entities should also, to the greatest see of goods, products, or materials produced in the United States, pen of Emergency Management (DEM) in advance of the procurement. FEMA's contract provisions guide, in the "Resource Document" tab.
5. Supplanting is prohibited under this grant. Supplanting available (or expected to be available) to fund that same at I attest that funding for this project does not currently exist w	ctivity.	heir own agency's funds for an activity because federal funds are
 6. Entities applying as a subgrantee must meet a 30% cos requirement. I understand and agree. 	t share requirement for FY 2024 SLCGP	P. Please acknowledge your understanding and agreement of this
7 Each jurisdiction must complete its own application. Th	a submitter of the grant application will	he the recipient of funds. Without an application, DEM is unable to
issue a grant. Subgrantees may not pass through or subg		be the recipient of funds. Without an application, DEM is unable to ons.
, ,	ugh the Nevada Division of Emergency	Management) may not use this funding to administer their own
subawards. ✓ I understand and agree		
Application Questions top		
 Is this agency considered a rural area (an area encompa If your agency is not considered a rural area, but your project water benefit rural Nevadans. Yes 		people)? and indicate in your narrative what percentage of your project will directly
☑ No		
2. There are four (4) objectives for FY 2024 SLCGP. Please Objective 1: Develop and establish appropriate governance		oject most closely aligns. nting, 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.
Objective 4. Ensure organization personner 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 December of the details
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

	•			•	of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) (ncsr (cisecurity.org).
	Our age	ncy is alread	y participatir	ng in the Cy	ber Hygiene Services and Nationwide Cybersecurity Review (NCSR)
	Our age is award		et signed up	for the Cyl	ber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project
	12 Provido	the E digit =	in codo wh	oro tho pr	oject will be executed.
					sub-recipient address.
	13. Is this p	roject scale	able? Can a	any part of	f it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it
					vendor that implements a vulnerability management tool. This project can be scaled to the extent that the cost of available solutions varies quirements stipulated by the referenced CIS controls.
					other jurisdictions? sdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
	✓ No				
	project stric ✓ Build				eject focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if the its existing/current level.
	☐ Sustain				
	16. If this pr n/a	oject is sus	taining a pr	eviously a	twarded SLCGP project, please provide the fiscal year and project name of the original project.
	☐ Planning informat	- Developm on ation - Individ	ent of policie	es, plans, po n overall or	anization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. rocedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and reganizational structure, and leadership at each level in the structure ms that comply with relevant standards
	☐ Exercise	s - Hands-or			nat comply with relevant training standards ace knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond
	to real e	ents/			
	D-1-II D-1-I				
ine Item	n Detail Budg	jet <u>top</u>			
	ING COST			Unit	Describe how the numbers (a) within this element tie into the How would your experiention quetain this project if
Name	g Cost Line I Desc	ription	Quantity	Unit Cost	al 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		\$ \$
				0.0	
	IIZATION (Heid	Describe how the number of a visiting this planeaut tie into the Herry would very experientian contain this project if
organiza Name	ational Cost	Line item Description	Quan	tity Unit Cost	Total ' '
				\$	\$
				\$ \$	\$ \$
				\$	\$
				\$	\$
				\$ \$	\$ \$
				\$	\$
				\$	\$ \$
				\$ \$	\$ \$
				\$	\$
				\$ \$	\$
				0 \$ 0.00	\$) \$
					0.00
EQUIP	MENT COS	STS			Describe

	Description '		Unit Cost		how the purchase (s) within this element tie into the project as described in the Application Questions section.	project if grant funding was reduced or discontinued?	equipment-list to linu AEL I	iiio	AEL Number - Search https://www.fema.gov/grants/tools/authori equipment-list to find AEL info	zed-
Vulnerability Managemen Tool		1 :	\$ 275,000.00 2		purchase	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 2	\$ 75,000.00)					

TRAINING COSTS

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

EXERCISE COSTS

Line Item Description	Quantity	Unit Cost	Total element tie into the project as described in the	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
	0.00	
Total	0 \$ 0.00 \$0.00	0
Document Uploads <u>top</u>		

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

 $^{^*\}mbox{\it ZoomGrants}^{\mbox{\tiny TM}}$ is not responsible for the content of uploaded documents.

Application ID: 484898

Become a fan of ZoomGrants*** on Facebook Problems* Confact us af <u>Desistored ZoomGrants com</u> 02002-0204 Gartal-Nayls com. Air right reserved. ZoomGrants* and the ZoomGrants logs are transmissed of GrantAnalyst.com, LLC.

	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



Nevada Office of the Military, Division of Emergency Management

FFY 2024 State and Local Cybersecurity Grant Program (SLCGP)

	Emergency Management & Homeland Security Progracial District Court: Cyber Security and Net	
•	Application Questions Line Item Detail Budget Document	
\$ 566,251.40 Requested	Washoe County Emergency Management & Homeland Security Program	
Submitted: 10/31/2024 10:45:48 AM (Pacific)		Telephone 7753994811
Broingt Contact	5195 Spectrum Blvd Reno, NV 89512	Fax Web www.readywashoe.com
Project Contact Francisco Ceballos	United States	UEI
FCeballos@washoecounty.gov		SAM Expires11/10/2021
Tel: 7752244109	Emergency Manager Kelly Echeverria	
Additional Contacts	KEcheverria@washoecounty.gov	
Valerie.Moser@washoecourts.us,chris.long@washoecourts.us		
Pre-Application <u>top</u>		
1. Is your organization one of the following types of entities?: Co council of government, regional government entity, agency or in tribe, or authorized tribal organization. Be advised that state agencies receiving SLCGP funds will have to cover yes No No 2. All funds granted under the State and Local Cybersecurity Grachieving this goal? (If not, the project is not eligible for SLCGP ✓ Yes No 3. In order for your application to be considered, you must attengrant. If you do not send representation to the required meeting Meeting dates are to be determined and will be communicated to SL ✓ I understand and agree. 4. All procurement is required to be compliant with Nevada Rev FEMA legal opinion, locals may NOT use NRS 332.115 because further justification).** All procurement must be free and open cousinesses, women's business enterprises, and labor surplus a federal award, provide a preference for the purchase, acquisitio source procurement must be pre-approved in writing by the Div You may view FEMA's written legal opinion on NRS 332.115, along I understand and agree. 5. Supplanting is prohibited under this grant. Supplanting occur	nstrumentality of a local government, rural community, obtain consent for their project from local jurisdictions. A ten and Program must focus on managing and reducing sy funding). Indicate the second sec	unincorporated town or village, or other public entity, inplate for obtaining this consent will be provided. Stemic cyber risk. Does your project proposal aid in other security Task Force. This is a requirement of the like 332, PURCHASING: LOCAL GOVERNMENTS. **Per tive than 2 C.F.R. Part 200 (see Resources section for poice conomic steps in soliciting small and minority itses should also, to the greatest extent practicable under the United States, per 2 C.F.R. Part 200.322. Any sole the procurement. Sions guide, in the "Resource Document" tab.
expected to be available) to fund that same activity. I attest that funding for this project does not currently exist within or		,
6. Entities applying as a subgrantee must meet a 30% cost share ✓ I understand and agree.	e requirement for FY 2024 SLCGP. Please acknowledge	your understanding and agreement of this requirement
 Each jurisdiction must complete its own application. The subigrant. Subgrantees may not pass through or subgrant funds to I understand and agree. 		nds. Without an application, DEM is unable to issue a
8. Subrecipients (i.e., agencies receiving this funding through th ✓ I understand and agree	ne Nevada Division of Emergency Management) may no	ot use this funding to administer their own subawards.
Application Questions <u>top</u>		
1. Is this agency considered a rural area (an area encompassing If your agency is not considered a rural area, but your project will sup Nevadans. ☐ Yes ☑ No		rative what percentage of your project will directly benefit run
2. There are four (4) objectives for FY 2024 SLCGP. Please selec Objective 1: Develop and establish appropriate governance struct cybersecurity incidents and ensure continuity of operations. Objective 2: Understand their current cybersecurity posture and ar	tures, including developing, implementing, or revising cybers reas for improvement based on continuous testing, evaluation	ecurity plans, to improve capabilities to respond to

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

 ${\bf 3.\ Please\ select\ which\ of\ the\ SLCGP\ program\ elements\ your\ project\ addresses.}$

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 st local governments within the state.	ate o
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 with state, against cybersecurity risks and cybersecurity threats.	in the
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecur threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.	ity
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.	3
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 workfor 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 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.	ı
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.	al
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 with 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 wirely 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 accepoints, 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 will atest cyber security recommendations. SJDC would like to enhance password security by purchasing a system that allows sharing to applicable Tech Services Administrative personnel with 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 issue 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 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, unincorpor Washoe County which enco	ess ess ith thout es end- rity
5. How does your project align with the objective selected in Question 22	

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)

	agency has not yet signed u rded	p for the Cyber Hygic	ene Services or	Nationwide Cyb	persecurity Review (NCSR), but unders	stands we will be re-	quired to sign up for them if our project is		
	ride the 5-digit zip code wh ect location could be differe								
If necess	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.								
strictly r ☑ Build	maintains a core capability d			ng a new capal	oility, or the intent of the project is t	o close a capabili	ty gap. Select "sustain" if the project		
		reviously awarded	SLCGP projec	ct, please provi	ide the fiscal year and project name	of the original pr	oject.		
☐ Plan ☑ Orga ☑ Equ ☐ Trair	ning - Development of polici anization - Individual teams, a ipment - Equipment, supplies ning - Content and methods or rcises - Hands-on activities v tts	es, plans, procedure an overall organizations, and systems that co of delivery that compl	s, mutual aid ag nal structure, a omply with rele y with relevant	greements, strate nd leadership at vant standards training standard	each level in the structure	olves the collection a	g sought for this project. and analysis of intelligence and information les to improve capabilities to respond to real		
Line item Detail B	uuget <u>top</u>							-	
PLANNING CO Planning Cost L Name D					hin this element tie into the project uestions section.		r organization sustain this project if grant duced or discontinued?		
	·	\$		••		, and the second			
		\$							
		\$							
		\$							
		\$ \$							
		\$							
		\$							
		\$ \$							
	0	0.00 \$							
		0.00							
ORGANIZATIO	N COSTS								
Organizational Cost Name	Line Item Description	Quantity Unit (project as de	v the purchase(s) within this element scribed in the Application Question	ns section.	How would your organization sustain this project if grant funding was reduced or discontinued?		
Consultant Service	s consult to assist with alway on VPN activation and monitoring			0 on VPN config	uration development. Consultant will vere with current security standards.		Above base funding would be requested.		
			\$ 9						
			\$	3					
			\$ 9						
			\$ \$ \$						
			\$	3					
			\$ 9						
			\$ 9 \$						
			\$ 3						
		1 30,00	\$ 30,000.0						
EQUIDMENT O									
EQUIPMENT C	.0818		Describe						
				How would					
Emulare and Occident	l in a law		within this element tie	your organization	AEL Name - Search	AE	L Number - Search		
Equipment Cost Name	Line Item Quantity L Description	Jnit Cost Tota	project as	sustain this project if gran funding was	https://www.fema.gov/grants/tool	Is/authorized- http	os://www.fema.gov/grants/tools/authorized ipment-list to find AEL info	-	

					Questions	discontinued?			
Password protection/manager	Secure Passwords	1	\$ 14,000.00		passwords and allows system	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	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	continue to request budget authority from Washoe County	Cyber Security En Host	05HS-00-MALW	
Software - proactive alerting, trending and planning	Software	1	\$ 20,000.00		Preempt infrastructure		Cyber Security En Ntwk	05NP-00-IDPS	
Network Switches	network switches	1	\$ 410,000.00		Enable the creation of virtualized networks that automate	funding would be requested	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	provides additional insight into cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.	submit a request to the County for additional budget authority to carry out this project. If denied, SJDC	Information Tech Hardware	04HW-01-INHW	
			\$	\$		avalidDIE.			
			\$ \$	\$ \$					
			\$	\$					
			\$ \$	\$					
			\$	\$					
		50	\$ \$	\$ \$					
				ى 36,251.40					

TRAINING COSTS

Training Cost Name	Line Item	Quantity	Unit To	Describe how the purchase(s) within this element tie otal 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	
	0.00		

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total t	Describe how the purchase(s) within this element ie 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 00				
Total		U	\$ 0.00	\$0.00			0

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * A-133 Audit 2023
Travel Policy	✓	WC Travel Policy
Payroll Policy	✓	SJDC Personnel Manual
Procurement Policy	✓	Washoe County Purchasing Manual
Milestones download template	•	Milestones

 $^{^{\}star}ZoomGrants^{\tau\!\!M}$ is not responsible for the content of uploaded documents.

Application ID: 485279

Become a fan of ZoomGrants¹¹ on Facebook
Problems* Conlact us at Questions 2 CoomGrants.com
©2002-2024 Grant/Analyst.com. All rights reserved.
"ZoomGrants' and the ZoomGrants logo are trademarks of Grant/Analyst.com, LLC
Logout | Browser

	Applicant Namo	Second Judicial District Court
	•	SJDC's Cyber - Security
	Project Funding Stream:	FY 2024 SLCGP
	Milestone Description*	Date of Expected Completion
	Acceptance of Funding by Washoe County	Assume award notification by
1	Board of County Commissioners (BCC),	10/1/2025. Within 90 days of
	Setting up of separate grant tracking of	receipt of Award notification. By
	fiscal expenses within financial system	end of December 2025
		within 90 days of receipt of Award
2	Obtain necessary updated quotes from	notification. By end of December
	vendors for all equipment	2025
		within 45 days of acceptance of
3		funds by BCC. By February 15,
	Issue of Purchase Orders for equipment	2025
		within 90 days of receipt of
		equipment. May vary depending
4		on product backlog/shipment
	Install of equipment	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



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 of	OI
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

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.

✓ Lunderstand 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 state in the event of an incident state.
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.

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

Please indicate your understanding of this policy.

✓ I understand and agree

1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	es the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can mend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network ce by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and adrits. To register for these services, email vulnerability info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. e 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: www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. –Nationwide Cybersecurity Review (NCSR)—The NCSR is a free, anonymous, self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and blogy Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the Cr. during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org). In agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR) In agency is already participating in the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our ject is awarded Wide the 5-digit zip code where the project will be executed. Signature of the 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 is project shareable or deployable to other jurisdictions? Yes" if the project supports multiple	
ŗ	ld 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 strictly maintains a core capability at its existing/current level. Id stain	
	is project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project. ject was not a previously awarded SLCGP project.	
	ase select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project. nning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and ormation ganization - Individual teams, an overall organizational structure, and leadership at each level in the structure uipment - Equipment, supplies, and systems that comply with relevant standards ining - Content and methods of delivery that comply with relevant training standards ercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to pond to real events	
Line Item	Budget <u>for</u>	
Line Item	Budget <u>fop</u>	_
PLANNII	OSTS	
	OSTS Line Item Quantity Unit Total Describe how the purchase(s) within this element tie into the Boundary Cost Total Project as described in the Application Questions section. Grant funding was reduced or discontinued?	
PLANNII Planning	OSTS Line Item Quantity Unit Total Describe how the purchase(s) within this element tie into the How would your organization sustain this project if	
PLANNII Planning	OSTS Line Item Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project if grant funding was reduced or discontinued? \$ \$ \$ \$ \$	
PLANNII Planning	OSTS Line Item Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project if grant funding was reduced or discontinued? \$ \$ \$ \$ \$ \$ \$ \$	
PLANNII Planning	OSTS Line Item Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project if grant funding was reduced or discontinued? \$ \$ \$ \$ \$	
PLANNII Planning	OSTS Line Item Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project if project as described in the Application Questions section. How would your organization sustain this project if grant funding was reduced or discontinued?	
PLANNII Planning	OSTS Line Item Description Quantity 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? \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
PLANNII Planning	OSTS Line Item Description Quantity 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? \$	
PLANNII Planning	OSTS Line Item Description Quantity Unit Cost Total project as described in the Application Questions section. S S	
PLANNII Planning	Description Quantity Unit Cost Total Cost 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? S S S S S S S S S S S S S	
PLANNII Planning	Description Quantity Cost Total Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. S	
PLANNII Planning	DOSTS Jene Item Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project if project as described in the Application Questions section. S S S S S S S S S S S S S	
PLANNII Planning	Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. S	
PLANNII Planning Name	OSTS Line Item Description Quantity Cost Total Cost Total Describe how the purchase(s) within this element tie into the project if grant funding was reduced or discontinued?	
PLANNIII Planning Name ORGANI	Description Quantity Cost Total Describe how the purchase(s) within this element tie into the project if project as described in the Application Questions section. How would your organization sustain this project if grant funding was reduced or discontinued? \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
PLANNIII Planning Name	Description Quantity Description Quantity Describe how the purchase(s) within this element tie into the project if project as described in the Application Questions section. S	
PLANNIII Planning Name ORGANI	Description Quantity Cost Total Describe how the purchase(s) within this element tie into the project if project as described in the Application Questions section. How would your organization sustain this project if grant funding was reduced or discontinued? \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
PLANNIII Planning Name ORGANI	DOSTS Line Item Description Quantity Unit Total Project as described in the Application Questions section. S S S S S S S S S S S S S	
PLANNIII Planning Name ORGANI	DOSTS Jane Item Description Quantity Unit Cost Total Project as described in the Application Questions section. Describe how the purchase(s) within this element tie into the grant funding was reduced or discontinued? S S S S S S S S S S S S S S S S S S	
PLANNIII Planning Name ORGANI	DOSTS Line Item Description Quantity Unit Total Project as described in the Application Questions section. S S S S S S S S S S S S S	
PLANNIII Planning Name ORGANI	DOSTS Line Item Description Quantity Cost Total Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By S S S S S S S S S S S S S	
PLANNIII Planning Name ORGANI Organizat	Description Quantity Cost Total project as described in the Application Questions section. S S S S S S S S S S S S S	
PLANNIII Planning Name ORGANI Organizat	DOSTS Line Item Description Quantity Cost Total Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. By S S S S S S S S S S S S S	
PLANNIII Planning Name ORGANI Organizat	DSTS Line Item Description Quantity Unit Cost Total Describe how the purchase(s) within this element tie into the project if grant funding was reduced or discontinued?	

\$

			0	\$ 0.00						
					0.00					
EQUIPME	NT COSTS									
Equipment Cost Name	Line Item Description G	Quantity Unit	: Cost	Tota	Describe how the purchase (s) within this element tiel into the project as described in the Application Questions section.	project if gran funding was reduced or	equipment-natio	a.gov/grants/tools/authorized	AEL Number - - https://www.fe equipment-list	Search ma.gov/grants/tools/authorized- to find AEL info
Cyber Forensic Infrastructure	Infrastructure required for cyber forensic investigations includes software, hardware, and licensing	1 60,0	\$ 00.00 6		In order to onvestigate systems in the event of a cyber attack, this system would be used to perform indepth analysis of an intrusion.	ŕ	Software, Forension		05HS-00-FRNS	
			\$	9						
			\$ \$	9						
			\$	9						
			\$	9						
			\$	9						
			\$ \$	9						
			\$	9						
			\$ \$	9						
			\$	4						
		1 60,0	\$ 00.00 6	\$ 0,000.0						
TRAINING				De	scribe how	the purchase(s) within this	How would your organization	on sustain this	Do you plan to coordinate this
Training Cost Name	Line Item Description	Quantity	Cost	Total ele	ement tie into	the project as estions section	described in the	project if grant funding was discontinued?		training with the State Training Officer?
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
		0 \$	0.00	\$ 0.00						0
				5.50						
EXERCISE	COSTS						A 101 1 11 1			
Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total e	lement tie in	the purchase(to the project a uestions section	s described in the	How would your organizati project if grant funding was discontinued?		Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$			•			2.0.000 0111001 1
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			\$	\$						
			Ψ	Ψ						

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

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * FY 22 Audit
Travel Policy	✓	<u>Travel Policy</u>
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy Procurement Procedure
Milestones download template	✓	Forensic System Milestones

 $^{^*\}mbox{\it ZoomGrants}^{\mbox{\tiny TM}}$ is not responsible for the content of uploaded documents.

Application ID: 485352

Become a fan of ZoomGrants 1^{to} on Facebook
Problema? Confact us at <u>Question is ZoomGrants com</u>
Economistro on Confact on at <u>Confact in the Confact on </u>

	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



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

Iohlin@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.washoeso

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.
 It is not the during it each, 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-servicesNationwide 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 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
	n Detail Budget top
	IING COSTS g Cost Line Item Description Quantity Unit Total Describe how the purchase(s) within this element tie into the project if grant funding was reduced or discontinued? How would your organization sustain this project if grant funding was reduced or discontinued?
	\$ \$
	\$ \$
	<u> </u>
	\$ \$ \$
	\$ \$ \$
	\$ \$
	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
ORGA	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
Organiz	S S S S O 0.00 \$ O.00 NIZATION COSTS rational Cost Line Item Ouantity Unit Total Describe how the purchase(s) within this element tie into the How would your organization sustain this project if
Organiz	S S S S S S S S S S S S S S S S S S S
Organiz	NIZATION COSTS ational Cost 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. But the project as described in the Application Questions section. S S S S S S S S S S S S S
Organiz	NIZATION COSTS ational Cost Line Item Description Quantity Quantity Quantity Cost Total Describe how the purchase(s) within this element tie into the project if grant funding was reduced or discontinued?
Organiz	NIZATION COSTS ational Cost Line Item Description Quantity Cost S S S S S S S S S S S S S S S S S S
	NIZATION COSTS ational Cost Line Item Description Quantity Victor 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? \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
Organiz	NIZATION COSTS ational Cost Line Item Description Quantity Unit Total Project as described in the Application Questions section. Unit Project as described in the Application Questions section. S S S S S S S S S S S S S S S S S S
Organiz	NIZATION COSTS ational Cost Line Item Description Quantity Victor 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? \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
Organiz	NIZATION COSTS ational Cost Line Item Description Quantity S S S S S S S S S S S S S S S S S S S

			0	\$ 0.0	0.00				
CUDME									
Equipment	NT COSTS Line Item Description Quant	tity Unit	Cost	То	Describe how the purchase (s) within this element tital into the project as described in the Application Questions section.	your organization sustain this project if gran funding was reduced or discontinued?	AEL Name - Search thttps://www.fema.gov/grants/tools/authorize equipment-list to find AEL info	AEL Number - S ed- https://www.fen equipment-list t	na.gov/grants/tools/authorized
Disaster Recovery nfrastructure	All infrastructure required for data backups, storage, security, and recovery.	1 250,00	\$ 00.00 2	250,000	\$ In order to 00 restore systems in the event c a cyber attack, this system would be used to securely backup, store, and restore data.	of expenditure to acquire the	Hardware, Computer, Integ	04HW-01-INHW	
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
			\$		\$				
		1	\$	250.000	\$				
		250,00	JU.UU ∠		UU				

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total e	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
				0.00			

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit . Cost	Describe how the purchase(s) within this Total 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 * A-133 Audit (Most Current)	Required? ✓	Attached Documents * Audit FY22
Travel Policy	✓	Travel Policy
Payroll Policy	✓	<u>Payroll</u>
		Payroll
Procurement Policy	✓	Procurement Policy
Milestones download template	~	Implementation Plan

 $^{^{\}star}\textit{ZoomGrants}^{\intercal \! \! M}$ is not responsible for the content of uploaded documents.

Application ID: 484936

Become a <u>fan of ZoomGrantal**</u> on Facebook Problema* Contact us at <u>Questions if ZoomGrants.com</u> 2002.02.2024 Grantshopts.com. Air grists reserved. "ZoomGrants" and the ZoomGrants logs are trademarks of Grant-Analyst.com, LLC. <u>Local Ellipsystem</u>

	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



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

vashoeschools.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 or 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.
To Distribute tribes, notice, expansionally of administration to rocal governments.
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,

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.

	Cybers and ap assess ways to execu- register body of	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, annu										
	self-as Cyber the firs https://	ssessment designsecurity Framer st year of the awalloww.cisecurity ur agency is alrea	gned to mea work and is ward/subawa y.org/ms-isa ady participati	sure gap sponsor ard perion ac/service ing in the	ed by d of p es/nc: Cybei	I capabilities of a SLT's cybersecurity programs. It is based on the DHS and the MS-ISAC. Entities and their subrecipients should concerformance and annually. For more information, visit Nationwide or (cisecurity.org). Hygiene Services and Nationwide Cybersecurity Review (NCSR) Hygiene Services or Nationwide Cybersecurity Review (NCSR), but under	ne National Institute of Standards and Technology complete the NCSR, administered by the MS-ISAC, during Cybersecurity Review (NCSR)					
		roject location co				ct will be executed. recipient address.						
	13. Is	this project scal	leable? Can	any part	of it	pe reduced or expanded? Describe the ways in which the project	can be reduced or expanded, or the reasons why it					
	such a	roject will support as business email	compromise	, come fro	om ins	tra-organization email security. This is critical because most email threatide the organization (intra-org). This project will cover all staff and stude ally degrade WCSD's capabilities in the event of a compromise of students.	nt accounts. Limiting implementation to just staff members,					
		t "Yes" if the proje es				ner jurisdictions? tions (e.g., multiple cities). Select "No" if the project primarily supports	a single entity.					
	15. Bu projec □ Bu	uild or Sustain: S				t focuses on starting a new capability, or the intent of the project existing/current level.	is to close a capability gap. Select "sustain" if the					
		t his project is su 22 - "Email Securi		reviousl	y awa	rded SLCGP project, please provide the fiscal year and project na	ame of the original project.					
	☐ Plainf ☐ Or ☑ Ed	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										
LANN	n Detail	I Budget top COSTS Line Item		Unit _		escribe how the purchase(s) within this element tie into the	How would your organization sustain this project if					
ame		Description	Quantity	Cost	F	roject as described in the Application Questions section.	grant funding was reduced or discontinued?					
					\$							
					\$							
					\$							
					\$							
					\$							
					\$							
					\$							
					\$							
					\$							
					\$							
	0 0.00 \$											
DOAL		ION COSTS			0.00							
		ION COSTS Cost Line Item	0	U	nit _	Describe how the purchase(s) within this element tie into the	How would your organization sustain this project if					
ame		Description	on Quar		ost	project as described in the Application Questions section.	grant funding was reduced or discontinued?					
					\$	\$ \$						
					\$	\$						
					\$	\$						
					\$	\$						
					\$	\$						

✓ I understand and agree

			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$ \$	\$					
			0 \$ 0.00	\$					
				0.00					
EQUIPME	ENT COSTS								
				Describe					
Equipment Cost Name	i Line Item Description	ity Unit Co	st Tota	element tie into the project as	your organization sustain this project if grant	AEL Name - Seal		AEL Number - d- https://www.fe	Search ma.gov/grants/tools/authorized- to find AEL info
				the Application	funding was reduced or discontinued?			о ч а.ро	
				Questions section.					
Email Security Software License	Software licensing for email security product, including cloud portal and vendor support	1 275,000.0		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	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.		ware AS	04AP-11-SAAS	
			\$ \$						
			\$ \$						
			\$ \$						
			\$ \$ \$ \$						
			\$ \$						
			\$ \$						
			\$ \$						
			\$ \$						
			\$ \$						
			\$ \$						
			\$ \$ \$ \$						
			\$ \$						
			0 275,000.00						
TRAINING	G COSTS								
Training	I ine Item	116					How would your organization		Do you plan to coordinate this
	e Description	Quantity Co	et lotal tie	into the projec estions sectio		in the Application	project if grant funding was discontinued?	reduced or	training with the State Training Officer?
			\$ \$						

\$ \$

\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
\$ \$	
0 \$ 0.00 \$	0
0.00	

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total e	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your org project if grant fund discontinued?	ganization sustain this ling was reduced or	Do you plan to coordinate the exercise with the State Exercion Office of the coordinate of the coordin	ise
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
		0	\$ 0.00	\$					0
				0.00					
Total		0	\$ 0.00	\$0.00					0

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * FY22 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	✓	<u>Payroll</u>
Procurement Policy	✓	Procurement Policy Procurement Procedure
Milestones download template	✓	Email Security milestones

 $^{^*\}mbox{\it ZoomGrants}^{\mbox{\tiny TM}}$ is not responsible for the content of uploaded documents.

Application ID: 485374

Become a fan of ZoomGrants ¹⁴ on Facebook
Problems? Contact us at <u>Countions</u> 8 ZoomGrants com
6/2002-2024 Grant/Analyst.com. All rights reserved.
ZoomGrants* and the ZoomGrants log are tandemaks of GrantAnalyst.com, LLC.
Locout | Browser

	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



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 D	Occument Uploads
\$ 309,495.81 Requested	Washoe County Sheriff's Office	
Submitted: 10/31/2024 3:16:47 PM (Pacific) Project Contact Rebecca DiMaggio SOGrants@washoecounty.us Tel: 7753283013 Additional Contacts	911 Parr Blvd Reno, NV 89512 United States Sheriff Darin Balaam sogrants@washoecounty.us	Telephone 7753283013 Fax Web UEI LJCKY7DLT898 SAM Expires10/19/2024
svanderwall@washoecounty.gov		
Pre-Application top		
authorized tribal organization. Be advised that state agencies receiving SLCGP funds will have to observed. Yes No 2. All funds granted under the State and Local Cybersecurity Granthis 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 you do not send representation to the required meetings, your ap Meeting dates are to be determined and will be communicated to SLCGV I understand and agree.	tain consent for their project from local jurisdictions. Interpretation on managing and reducing the program must focus on managing and reducing the program must focus on managing and reducing the program of the Governor plication will not be considered. In applicants as soon as the dates are known. In applicants are also required to follow the social c.F.R. Part 200.321. All non-federal entities shown a subapplicant are also required to follow the social c.F.R. Part 200.321. All non-federal entities shown a products, or materials produced in the United	ing systemic cyber risk. Does your project proposal aid in achieving or's Cybersecurity Task Force. This is a requirement of the grant. If d/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA we than 2 C.F.R. Part 200 (see Resources section for further cioeconomic steps in soliciting small and minority businesses, build also, to the greatest extent practicable under a federal award, d States, per 2 C.F.R. Part 200.322. Any sole source procurement it. provisions guide, in the "Resource Document" tab. It's funds for an activity because federal funds are available (or wledge your understanding and agreement of this requirement.
I. Is this agency considered a rural area (an area encompassing a lf your agency is not considered a rural area, but your project will support Nevadans. ☐ Yes ☑ No		our narrative what percentage of your project will directly benefit rural
2. There are four (4) objectives for FY 2024 SLCGP. Please select t ☐ Objective 1: Develop and establish appropriate governance structur incidents and ensure continuity of operations. ☐ Objective 2: Understand their current cybersecurity posture and area ☐ Objective 3: Implement security protections commensurate with risk ☑ Objective 4: Ensure organization personnel are appropriately trained. 3. Please select which of the SLCGP program elements your projects may align with more than one element.	res, including developing, implementing, or revising or as for improvement based on continuous testing, eva. d in cybersecurity, commensurate with responsibility.	cybersecurity plans, to improve capabilities to respond to cybersecurity plants, and structured assessments.

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.

	work 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, re	sponse, 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	I cybersecurity threats. tinuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats
on information systems, applica	ations, and user accounts owned or operated by, or on behalf of, the state or local governments within the state. I governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
\square 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 operation cybersecurity incident. 	ons 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
	r Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the nin 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	o address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training. unication 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 netwo	rks.
	e greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the stems within the jurisdiction of the state.
•	are cyber threat indicators and related information between the state, local governments within the state, and CISA. rvices offered by CISA. (See Application Question 10 for further details on these services.)
• • • • •	echnology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational
14. Develop and coordinate str	rategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted.
	ittees should also consider consulting neighboring entities, including adjacent states and countries. o, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, ser	vices, capabilities, or activities to local governments.
4. Describe your project in detail	
The Northern Nevada Cyber Cente	How does this project improve cybersecurity protection for your agency? 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 threa	ats.
Training Requests:	Pids Assessment
Course – Performing a Cybersec For the manager to perform risk as:	sessments for compliance and audits.
2. Course – Foundations: Compute For two members to build fundame	rs, Technology, & Security: ntal cybersecurity knowledge, covering basic to intermediate concepts.
Course – Introduction to Cyber S For one member to cover a broad s	ecurity: spectrum of cybersecurity topics including mobile device security, IoT, AI, authentication, authorization, cryptographic processes, network attacks, and more.
4. Course – Security Essentials – N For one member to cover essential	Network, Endpoint, and Cloud: skills for defending systems and networks.
5. Course - Practical Open-Source For three expert members to cover	Intelligence (OSINT): OSINT research and investigations for law enforcement and private sector businesses.
	Malware: Malware Analysis Tools and Techniques: malware analysis tools and techniques to examine malicious programs that target and infect Windows systems.
Benefits of Training:	
Bolster knowledge and skills to add Implement continuous vulnerability Increase knowledge of adversary to Adopt best practices to enhance cy	assessments and threat mitigation. bols and tactics.
Equipment Requests:	
1. Cellebrite Software Licenses:	
Inseyets Unlocks: Allows access to	n for extracting, decoding, reviewing, managing, and triaging digital equipment. I locked digital devices. gement system for secure evidence sharing and management.
Benefits of Cellebrite Software:	
Monitor, audit, and track activity on Enhance the resilience of information	on systems against risks.
	r threat information between state and local governments.
Ensure access to services and prog	grams in rural areas.
UPS Replacement Request: Uninterruptible Power Solution (UP The current UPS is over a decade of	S) Replacement: old, failing frequently, and needs replacement to prevent unnecessary server room access and hardware degradation.
Benefits of UPS Replacement: Enhance resilience against cyberse	pourity rights
Mitigate risks to critical infrastructur Ensure system reconstitution (back	re and information systems.
This comprehensive request for tra security and resilience of critical info	ining, equipment, and UPS replacement will significantly enhance the Cyber Center's capabilities to address and mitigate cybersecurity threats and ensure the rastructure in Northern Nevada.
5. How does your project align v Primary Objective: Personnel Cybe	vith the objective selected in Question 2? rsecurity Training
Training Courses: - Cybersecurity Risk Assessment: I	Equips managers with skills to assess and mitigate risks, ensuring compliance.
- Foundations: Computers, Technol	logy & Security: Builds foundational knowledge for two members, progressing to advanced cybersecurity concepts. ers network attacks, malware, and cryptography for one member.
- Security Essentials: Teaches core	defense skills for networks, endpoints, and cloud security. erts in OSINT for law enforcement and intelligence work.
- Reverse-Engineering Malware: Pr	ovides three experts with tools to analyze malware targeting Windows systems. r personnel's skills to effectively handle cybersecurity risks.
·	rotections Commensurate with Risk
Cellebrite Software:	

Celebrite 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, Loyelock, Winnemucca, Battle Mountain, Eureka, Elko, Carlin, Wells, West Wendover, and Elv. 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:

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 Insevets 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.

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

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/msisac/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

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

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 \$		

Organizational Co Name	ost Line Item G Description	Quantity	Unit To			rchase(s) withir	this element tie into the project stions section.	our organization sustain this project if grant reduced or discontinued?
			\$ \$	\$				
			\$ \$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$ \$	\$				
			\$	\$				
			\$ \$	\$				
		0	\$ 0.00	\$.00				
FOURDMENT C	0070							
EQUIPMENT C	0515				Describe			
					how the purchase(s) within this			
Equipment Cost						organization	AEL Name - Search	AEL Number - Search
Name L	ine Item Description C	Quantity	Unit Cost	Tot	project as described in the Application Questions	project if grant	https://www.fema.gov/grants/tool equipment-list to find AEL info	https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Inseyets/Guardian (S or product with T same capabilities 1	Fotal = \$57,547.35), 150 Inseyets Unlocks -	1 1	\$ 66,478.81	166,478.8	of Cellebrite software and Cellebrite	financial obligation created by the	Software, Forensic	05HS-00-FRNS
= G (\$	\$228.38/Unlock - Total = \$34,257.00), 7 Guardian Licenses \$10,667.78/License - Fotal = \$74,674.46)				project by enabling the Cyber Center			
					to monitor, audit, and track network traffic and device	licenses, replace hardware, and to maintain proficiency		
					activities, enhancing its oversight capabilities.	training updates		
					the Center's	initial grant funding period.		
						funding solution could involve a combination of		
					enhances secure evidence management	strategies: Budget Allocation , within		
					in online services. These tools	Participating Agencies: As the project progresses and		
					the Center's ability to	agencies reap the benefits of enhanced capabilities, it may be feasible		
					information	to allocate funds from their respective		
					while targeted training and software	cover ongoing expenses associated with license		
					extend cybersecurity support to rural areas,	updates, and occasional		
					ensuring equitable access and participation.	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.

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.

Revenue

by implementing a combination of these strategies, the project can establish a sustainable funding solution to cover continuing

		inancial obligations obeyond the nitial grant unding period. This ensures he longevity and affectiveness of he project's efforts in enhancing cybersecurity capabilities and protecting against cyber hreats in Vorthern Nevada.			
Liebert EXS UPS One (1) Liebert EXS, or product with Model same capabilities 53S30HCFR0CB0SW, 30 kVA / 30 kW Capacity, 3 phase UPS with 2 String(s)	00.00 EXS UPS t	ime purchase and would not need to be	Components, Networking, D	O4HW-03-NETD	
\$ \$	\$				
\$	\$				
\$ \$	\$				
\$	\$				
\$ \$	\$				
\$ \$	\$				
\$	\$				
\$	\$				
2 \$	\$				
206,478.81 206,4					
TRAINING COCTS					
TRAINING COSTS Training Cost Name Line Item Description Quantity Unit Cost To	otal Describe how the	ne purchase(s)	within this element tie into tl plication 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 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.	project if grant funding was reduced or discontinued?	training with the State Training Officer?
1 - Training Course Intelligence (OSINT) - (Registration \$8,951, GOSI Certification \$1,028)	3 \$ 9,979.00	\$ The purchase of training courses is integral to enhancing the Cyber 29,937.00 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	project primarily revolves around the potential need to renew software licenses, replace d hardware, and to maintain proficiency through periodic training updates beyond the initial grant	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

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 hardware, and to maintain proficiency through threat mitigation, ensuring personnel stay current on threat periodic training updates beyond the initial grant 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 funding period. To address this, a proposed funding solution could involve a combination of

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 seek grain renewals of 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 grantmaking 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 \$ \$ 3,575.00 The purchase of training courses is integral to enhancing the Cyber "The continuing financial obligation created by the NO 2 - Training Performing a Cybersecurity Risk 3,575.00 Center's preparation, response, and resilience by equipping project primarily revolves around the potentia Coure need to renew software licenses, replace Registration Assessment - On personnel with skills to tackle cybersecurity threats effectively Courses like these support continuous vulnerability assessment and hardware, and to maintain proficiency through threat mitigation, ensuring personnel stay current on threat periodic training updates beyond the initial gra Demand - (Registration periodic training updates beyond the initial grant management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses funding period. To address this, a proposed funding solution could involve a combination of 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. **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. Foundations: Computers, "The continuing financial obligation created by the NO 3 - Training \$ \$ 7,140.00 The purchase of training courses is integral to enhancing the Cyber 3.570.00 Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively Technology, & Security - Web-Based project primarily revolves around the potential need to renew software licenses, replace Course Registraion (Registration \$3,171, Courses like these support continuous vulnerability assessment and hardware, and to maintain proficiency through **GFACT Certification \$399** threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program periodic training updates beyond the initial grant funding period. To address this, a proposed aligned with the NICE Framework, the initiative addresses workforce gaps in knowledge and skills. Training also supports funding solution could involve a combination of modernization efforts by aligning IT and operational technology Budget Allocation within Participating Agencies: cybersecurity, while collaborative training fosters coordinated cybersecurity strategies across local and state governments. 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 grantmaking 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

Revenue Generation Strategies: Investigating revenue generation strategies, such as providing

cybersecurity initiatives.

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 Introduction to Cyber \$ \$ 8.829.00 The purchase of training courses is integral to enhancing the Cyber "The continuing financial obligation created by the NO Security - On Demand -8,829.00 Center's preparation, response, and resilience by equipping project primarily revolves around the potentia Course personnel with skills to tackle cybersecurity threats effectively Registration (Registration \$7,801, need to renew software licenses, replace GSIF Certification \$1,028) Courses like these support continuous vulnerability assessment and hardware, and to maintain proficiency through threat mitigation, ensuring personnel stay current on threat management practices. Through a comprehensive training program aligned with the NICE Framework, the initiative addresses periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of workforce gaps in knowledge and skills. Training also supports modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated Budget Allocation within Participating Agencies: cybersecurity strategies across local and state governments. 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. 5 - Training "The continuing financial obligation created by the project primarily revolves around the potential need to renew software licenses, replace Reverse-Engineering Malware: Malware \$ The purchase of training courses is integral to enhancing the Cyber 9,979.00 29,937.00 Center's preparation, response, and resilience by equipping NO 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 periodic training updates beyond the initial grant funding period. To address this, a proposed Course Registration Analysis Tools and Techniques - (Registration 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 \$8,951, GREM Certification \$1,028) funding solution could involve a combination of strategies: modernization efforts by aligning IT and operational technology cybersecurity, while collaborative training fosters coordinated **Budget Allocation within Participating Agencies:** cybersecurity strategies across local and state governments. 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 grantmaking 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.

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

2,270.00

\$ \$ 6,810.00 The purchase of training courses is integral to enhancing the Cyber "The continuing financial obligation created by the Center's preparation, response, and resilience by equipping personnel with skills to tackle cybersecurity threats effectively Courses like these support continuous vulnerability assessment and hardware, and to maintain proficiency through 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.

project primarily revolves around the potentia need to renew software licenses, replace 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.

6 - Training Course Registration Security Essentials -Network, Endpoint, and Cloud - On Demand -(Registration \$8.951. GSEC Certification \$1.028)

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. need to renew software licenses, replace Courses like these support continuous vulnerability assessment and hardware, and to maintain proficiency through 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 periodic training updates beyond the initial grant funding period. To address this, a proposed funding solution could involve a combination of

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

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 grantmaking 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	\$	\$	0
50,	451.00 103,	017.00	

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
				0.00			
Total		0	\$ 0.00	\$0.00			0

Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * SAM.gov Reg
		Single Audit
Travel Policy	✓	Travel Policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	<u>Project Milestones</u>

 $^{^*}$ ZoomGrants $^{\text{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 485357

	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 i	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