

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

# Board of Regents of the Nevada System of Higher Education on behalf of the Desert Research Institute DRI Cybersecurity Workforce Development Program

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

\$ 472,890.00 Requested

Submitted: 8/30/2023 1:39:34 PM (Pacific)

Project Contact
Ryan Coots
ryan.coots@dri.edu

Tel: 775-673-7381

Additional Contacts

none entered

Board of Regents of the Nevada System of Higher Education on behalf of the Desert Research Institute

2215 Raggio Pkwy Reno, NV 89512 United States

Director of Administration Services and Compliance
Diane Samuel
diane.samuel@dri.edu

Telephone 775-673-7381
Fax 775-673-7363
Web https://www.dri.edu
EIN 886000024
UEI MV1JFXA4S621

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.

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. 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 20% cost share requirement for FY 2023 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.

#### Application Questions top

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

directly benefit rural Nevadans.
Yes
✓ No
2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.  Objective 3: Implement security protections commensurate with risk.
Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
3. Please select which of the SLCGP program elements your project addresses.  Projects may align with more than one element.
1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
<ul> <li>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.</li> </ul>
7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
■ 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
16. Distribute funds, items, services, capabilities, or activities to local governments.
10. Biolinate lands, territor, companies, or doubles 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 goals of the DRI Cybersecurity Workforce Development Program are to train and provide hands-on experience to community college students, high school graduates and incumbent workers so they are qualified to respond to the array of cyber-attacks facing modern organizations. This will occur through an initial, 2-day on-site capture the flag assessment for 80 people, hosted by DRI at DRI's Reno and Las Vegas locations. The top 20 performers in each location will be selected for the next phase of the workforce development program. These 40 participants will be awarded a Cybersecurity Essentials self-study course and exam voucher. Over the following 3 months participants will complete the Cybersecurity Essentials course, complete the exam using the provided voucher, and meet at DRI locations twice a month. During the on-premise meetings, participants will learn to design hardened server systems in a cloud environment, learn how to setup and configure modern, enterprise based perimeter firewalls, examine and correlate security logs, treat malware infections, be introduced to enterprise grade security solutions such as Anti-virus, patching, phishing, and penetration testing applications, as well as provide security awareness training to end-users. The meetings will consist of hands-on participation, live demos, self-study, and collaborative working groups. Finally, DRI will award the top 4 finishers of the program with a higher-level course and exam voucher of their choosing. To our knowledge, the proposed DRI program will be the only one in Nevada to combine in-person training with hands-on cybersecurity workforce development at an organization with a large and distributed IT infrastructure.

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

The proposed program meets SLCGP's objective #4 by ensuring organization personnel are appropriately trained in cybersecurity, commensurate with responsibility, and that participants who successfully complete the program are prepared for well-paid "middle-skills" cybersecurity positions with many openings in the State.

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

Participants will have the opportunity to bolster their knowledge, skills and abilities, by spinning up and hardening Windows systems in the cloud (i.e., apply configurations and policies to strengthen defenses of system in accordance with NIST guidelines), validate configuration of systems, understand how to patch, configure, and maintain an enterprise based firewall and Next Generation protections (IDS/IPS, Application Control and URL Filtering, Anti-Bot, Anti-malware, VPN), and understand the role enterprise based cybersecurity applications (A/V, Patching, MFA, Pen-Testing, Phishing, Security Awareness Training) play in a company's cybersecurity posture. The curriculum will follow the US National Institute of Standards and Technology's Cybersecurity Framework. This aligns with identifying and mitigating gaps in the cybersecurity workforce by training individuals for middle-skills jobs in NICE Framework categories such as Investigate, Operate and Maintain, Protect and Defend, and Securely Provision.

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

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

Training Program Details - Participants will be given the opportunity to "play" a 2-day Capture the Flag event, an online program that evaluates the players aptitude for cybersecurity-related problem solving. The top 20 High-scorers from each location (40 total) will be admitted to the DRI Workforce Development Program. Curriculum in the program will be a combination of participant self-study in an organized and timely course and required exam, instruction using already developed content, and in-house curriculum focusing on securing the modern enterprise at the Desert Research Institute. On-site hosted events including capture the flags, hands-on training sessions, and study sessions will be with DRI's Information Security Officer Ryan Coots. The tuition for the self-study course and exam, hosting, and locations costs for this program will be provided at no cost to participants through this grant. SLCGP funding from this proposal will be used to develop content and structure for the workforce development program. The program will host alternating on-premises meetings in each of DRI's main campus locations in Reno and Las Vegas.

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

The primary desired outcomes of this project are to educate and train participants to be able to;

1. Respond to an array of cyber-attacks.

	I how to provide security awareness t	aining to end-users.		
<ol><li>Treat and</li></ol>	emediate malware infections.			
<ol><li>Understand</li></ol>	I the function of and be able to config	re and secure enterpris	e grade firewalls.	
	systems from scratch with a security			
· ·	,			
Participants v	the complete the DRI program will be	qualified for positions in	cluding enterprise defender information sec	curity analyst, cyber-awareness trainer, and security
·		qualifica for positions in	oldaring enterprise deterrider, information see	diffy dilaryst, cyber awareness trainer, and security
operations ar	aiysi.			
	•	* '	` .	inkedin.com/pulse/shortage-cyber-security-professionals
david-rotenbe	g/). In Nevada, throughout 2022 there	were 6,907 people emp	ployed in the cybersecurity workforce and 6,9	902 cybersecurity job openings, a workforce
supply/demai	d ratio of 1.0 (https://www.cyberseek	org/heatmap.html ). Ma	ny of these jobs do not require 4-year degre	ees, but technical skills that can be acquired through on
the-iob trainir	<ul> <li>a. industry certifications, community of</li> </ul>	ollege courses, and mo	dern vocational and skills education program	ms. Nevada salaries for information security analysts,
				nent of Employment, Training, and Rehabilitation).
positions requ	ming child industry certificates of an	issociate degree, nave	Thedian wage of \$65,250 (Nevada Departir	ion of Employment, Training, and Renabilitation).
0 Managam	ont & Administration (M&A) may b	rotained at up to E9/	of the total east of the project. Will you b	he retaining funds for MOA2 If VEC enter the
-	, , ,	retained at up to 5%	of the total cost of the project. Will you t	be retaining funds for M&A? If YES, enter the
•	are retaining. If NO, enter "N/A"			
M&A costs a	e not operational costs but are neces	sary costs incurred in d	rect support of the grant, or as a consequer	nce of the grant (i.e., financial management, reporting,
oversight of t	nose involved in the operational aspe	ts of the grant)		
N/A				
10. Does this	project require new construction	renovation, retrofitting	g. or modifications of an existing structu	ure which would necessitate an Environmental
	Historic Preservation (EHP) revie		g, og og og og	
-	, ,		a atmost up in alcoling amount things like northin	na naile in walls. Places are the EUD Cuidense
		ipts trie environment or	a structure, including small things like puttin	ng nails in walls. Please see the EHP Guidance
	r more information on EHP reviews.			
Yes				
✓ No				
140				
		•		cipate in a limited number of free services by the
Cybersecuri	y and Infrastructure Security Ager	cy (CISA). For these r	equired services and memberships, plea	ase note that participation is not required for
submission	and approval of a grant but is a po	t-award requirement	Cyber Hygiene Services Web Applica	ation Scanning is an "internet scanning-as-a-
		•		own vulnerabilities and weak configurations.
				pest practices and standards. Vulnerability Scannin
		-	•	ces and vulnerabilities. This service provides
weekly vuln	erability reports and ad-hoc alerts	To register for these	services, email vulnerability_info@cisa.c	dhs.gov with the subject line "Requesting Cyber
Hygiene Ser	vices – SLCGP" to get started. Ind	cate in the body of yo	our email that you are requesting this ser	rvice as part of the SLGCP. For more information,
visit CISA's	Cyber Hygiene Information Page: h	ttps://www.cisa.gov/to	pics/cyber-threats-and-advisories/cyber-	-hygiene-servicesNationwide Cybersecurity
		•		pabilities of a SLT's cybersecurity programs. It is
				DHS and the MS-ISAC. Entities and their
				ubaward period of performance and annually. For
			os://www.cisecurity.org/ms-isac/services/	· · · · · · · · · · · · · · · · · · ·
☐ Our age	ncy is already participating in the Cyb	er Hygiene Services and	Nationwide Cybersecurity Review (NCSR),	either on our own or as a condition of FY 2022 SLCGP
Our age	ncy has not yet signed up for the Cyb	er Hygiene Services or I	Nationwide Cybersecurity Review (NCSR) bu	ut understands we will be required to sign up for them if
3	ect is awarded	, 9	,,	
ou. p.o,	or is arrai asa			
40.1.41				
•		be reduced or expan	ded? Describe the ways in which the pro	oject can be reduced or expanded, or the reasons
why it canno				
This project is	scalable, however we would need to	find additional sources	of match/in-kind funding as the project scale:	S.
13. Provide	he 5-digit zip code where the pro	ect will be executed.		
The project le	cation could be different than the sul	-recipient address.		
89512		•		
14 Build or	Sustain: Salact "huild" if this proje	et focuses on starting	a new canability or the intent of the pro	oject is to close a capability gap. Select "sustain" if
				pect is to close a capability gap. Select Sustain in
	trictly maintains a core capability	at its existing/current	level.	
Build				
Sustain				
AF to date on				
	oject shareable or deployable to o			
Select "Yes"	f the project supports multiple jurisdi	tions (e.g., multiple citi	es). Select "No" if the project primarily suppo	orts a single entity.
✓ Yes				
□ No				
140				
				for which funding is being sought for this project.
Each selection	n should have an accompanying item	in the line item detail b	udget table on the next tab	
✓ Planning	- Development of policies, plans, pro	cedures, mutual aid agr	eements, strategies, and other publications:	; also involves the collection and analysis of intelligence
and info			,g, p,	
Organiz	ation - Individual teams, an overall orç	anizational structure, an	d leadership at each level in the structure	
Equipm	ent - Equipment, supplies, and system	s that comply with relev	ant standards	
	<ul> <li>Content and methods of delivery that</li> </ul>		_	
		e knowledge of plans, al	low members to improve their own performa	ance, and identify opportunities to improve capabilities to
respond	to real events			
= -				
Line Item Detail Bu	dget <u>top</u>			
DI ANNINIO CO	ete			
PLANNING CO	313			
			Describe how the purchase(s) within	this How would your organization sustain
<b>Planning Cost Name</b>	Line Item Description Qua	ntity Unit Cost To	otal element tie into the project as descri	
J		•	the Application Questions section.	or discontinued?
0	DDI 0 1		•••	
	DRI Salary + fringe - Cyber	1	\$ half of a month of time for 1 DRI cyber e	
and Program planning	Expert content planning and	23,443.20 11,721	.60 develop cloud range and curriculum.	curriculum for future use.
	development			
			¢	
			\$	

\$	
\$	
\$	
\$	
\$	
\$	
\$	
\$	
\$	
\$	
\$	
\$	
1 \$	
23,443.20 11,721.60	

# **ORGANIZATION COSTS**

Organizational 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?
In-person Instruction and Hosting	DRI Salary + fringe - Cyber Expert hands-on instruction and initial assessment hosting	1	\$ 23,443.20	\$ Half of a month of time for in-person hands on to host 11,721.60 instruction, training, and initial assessments	We would seek alternate funding, primarily through grants or gifts to continue funding of this project.
Initial Participant Assessment	Initial Capture the Flag Assessment licensing and customization	80	\$ 825.00	\$ 2-day Initial CTF assessment in each location to 66,000.00 select program finalists, 40 participants in each location will participate and 2 from each location will be selected	We would seek alternate funding, primarily through grants or gifts to continue funding of this project.
Participant Course and Exam Vouchers	Cybersecurity Essentials Course and Exam Vouchers	40	\$ 7,609.80	\$ Course and Exam Vouchers for program finalists (20 304,392.00 in Reno, 20 in LV)	We would seek alternate funding, primarily through grants or gifts to continue funding of this project.
Finalist Course and Exam Vouchers	Course and Exam Vouchers	4	\$ 7,609.80	\$ Course and Exam Vouchers for top performers in 30,439.20 program. Finalists will get to choose their preferred higher level course.	We would seek alternate funding, primarily through grants or gifts to continue funding of this project.
Travel	Travel between Reno and Las Vegas, NV	2	\$ 6,613.20	\$ 2 Instructors travelling from Reno to LV and back 13,226.40 every other week for alternating sessions.	We would seek alternate funding, primarily through grants or gifts to continue funding of this project.
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
		127	\$	\$	
			46,101.00	425,779.20	

# **EQUIPMENT COSTS**

	ILITI OCCIO						
Equipment Cost Name	Line Item Quantit Description	Unit Y Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	organization sustain this project if grant funding was reduced	https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Cloud Based Lab	Azure Cloud 1 Based Lab	Ψ.		the hands- on demo lab where	primarily through grants or gifts to		
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				

\$	\$
\$	\$
\$	\$
\$	\$
\$	
\$	\$
\$	\$
1 \$ 4,950.00 4,95	\$ .00
	\$ \$ \$ \$ \$ \$ \$ \$ 4,950.00 4,950

# **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit Cost	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?	Do you plan to coordinate this training with the State Training Officer?
Cloud Course and Exam Voucher	Cloud Academy Course and Exam Voucher for Instructors	2	\$ 15,219.60		Cloud Academy Training for instructors on securing the cloud.	We would seek alternate funding, primarily through grants or gifts to continue funding of this project.	No
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		2	\$ 15,219.60	30.439.20	)		0

# **EXERCISE COSTS**

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

# Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	~	NSHE 2022 Audit
Travel Policy	~	DRI Travel Policy
Payroll Policy	~	DRI Payroll Policy
Procurement Policy	✓	DRI Procurement Policy
Milestones download template	~	DRI Milestones
Capabilities Assessment download template	~	DRI Capabilities Assessment

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

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

	Applicant Name	Ryan Coots	
	Project Name:	DRI Cybersecurity Workforce Development Program	
	Project Funding Stream:	FY 2023 SLCGP	
	Milestone Description*	Date of Expected Completion	
1	Schedule Initial skills assessment event	January, 2024	
2	Curriculum setup	January, 2024	
3	Cloud Lab setup	January, 2024	
4	Host Initial Skills Assessment, identification of participants	January-February, 2024	
5	Participants take Cybersecurity Essentials self-study course	February-May, 2024	
6	On-premises, firsthand instruction begins	February-May, 2024	
7	Students submit Exam scores, Select 4 top performers	May, 2024	

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

D

✓ No

	arson City Fire/Emergency Management EM / Physical Security Proximity/	Camera Camera
Jump to: Pre-Application	Application Questions Line Item Detail Budget Doce	ument Uploads
\$ 191,039.10 Requested	Carson City Fire/Emergency Management	
Submitted: 8/30/2023 5:22:51 PM (Pacific)	777 S. Stewart Street Carson City, NV 89701	Telephone 7752837820 Fax
Project Contact	United States	Web
Carson City Fire	Pusinasa Manana	EIN 88600189
carsonfiregrants@carson.org	Business Manager Dave Aurand	UEI SAM Expires
Tel: 7752837820	Daurand@carson.org	SAM Expires
Additional Contacts sduarte@carson.org, fabella@carson.org		
1. Is your organization one of the following types of entities? district, council of government, regional government entity, public entity, tribe, or authorized tribal organization.		
✓ Yes		
□ No		
2. All funds granted under the State and Local Cybersecurity achieving this goal? (If not, the project is not eligible for SLOW) Yes No  3. In order for your application to be considered, you must a grant. If you do not send representation to the required mee Meeting dates are to be determined and will be communicated to I understand and agree.	CGP funding). ttend open meetings to testify in front of the Govern tings, your application will not be considered.	
4. All procurement is required to be compliant with Nevada R FEMA legal opinion, locals may not use NRS 332.115 becaus free and open competition. Applicants are also required to felabor surplus area firms per 2 C.F.R. Part 200.321. All non-fethe purchase, acquisition, or use of goods, products, or mat approved in writing by the Division of Emergency Managem You may view FEMA's written legal opinion on NRS 332.115, along I understand and agree.	e it has been determined that NRS 332.115 is less r ollow the socioeconomic steps in soliciting small a deral entities should also, to the greatest extent pr erials produced in the United States, per 2 C.F.R. Pa ent (DEM) in advance of the procurement.	restrictive than 2 C.F.R. Part 200. All procurement must be nd minority businesses, women's business enterprises, and acticable under a federal award, provide a preference for art 200.322. Any sole source procurement must be pre-
<ul> <li>5. Supplanting is prohibited under this grant. Supplanting of (or expected to be available) to fund that same activity.</li> <li>I attest that funding for this project does not currently exist w</li> </ul>		cy's funds for an activity because federal funds are availabl
<ul> <li>6. Entities applying as a subgrantee must meet a 20% cost s requirement.</li> <li>I understand and agree.</li> </ul>	hare requirement for FY 2023 SLCGP. Please ackno	owledge your understanding and agreement of this
7. Each jurisdiction must complete its own application. The a grant. Subgrantees may not pass through or subgrant fund	•	ent of funds. Without an application, DEM is unable to issue
Application Questions <u>top</u>		
1. Is this agency considered a rural area (an area encompas If your agency is not considered a rural area, but your project will rural Nevadans.  Yes Per Dave Fogerson, through Zach Edler, the task for	support rural communities, select "No" and indicate in yo	, , , , , ,

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

Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to

cybersecurity incidents and ensure continuity of operations.	
Objective 2: Understand their current cybersecurity posture and a	areas for improvement based on continuous testing, evaluation, and structured assessments.
Objective 3: Implement security protections commensurate with	
Objective 4: Ensure organization personnel are appropriately train	ned in cybersecurity, commensurate with responsibility.
<ol><li>Please select which of the SLCGP program elements your pro Projects may align with more than one element.</li></ol>	ject addresses.
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 noluding legacy information systems and information technology that are no longer supported by the manufacturer of
	or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the
<ul> <li>3. Enhance the preparation, response, and resilience of informativithin the state, against cybersecurity risks and cybersecurity th</li> </ul>	on systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments reats.
cybersecurity threats on information systems, applications, and u	assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and ser accounts owned or operated by, or on behalf of, the state or local governments within the state.
	lopt and use best practices and methodologies to enhance cybersecurity.
	ine services by the state or local governments within the state, including through the use of the .gov internet domain.  In the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding
<ul> <li>8. Use the National Initiative for Cybersecurity Education (NICE) workforces of the state or local governments within the state, enh</li> </ul>	Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity nance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of ddress cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
involving those communications or data networks.	the jurisdiction of the state between the state and local governments within the state in the event of an incident
may impact the performance of information systems within the ju	
	ited information between the state, local governments within the state, and CISA.
12. Leverage cybersecurity services offered by CISA. (See Quest     13. Implement an information technology and operational technology.)	ion 12 for further details on these services.)  ogy modernization cybersecurity review process that ensures alignment between information technology and
operational technology cybersecurity objectives.	isks and cybersecurity threats. Local governments and associations of local governments within the state should be
consulted. Cybersecurity Planning Committees should also consi	ider consulting neighboring entities, including adjacent states and countries.
<ul> <li>15. Ensure adequate access to, and participation in, cybersecurit</li> <li>16. Distribute funds, items, services, capabilities, or activities to leading to the companion of the</li></ul>	
to information and hardware restricted to support the city and all of its of activities. We are looking to invest into a new state-of-art proximity car badge/card access for the doors and implementing this project will help to physical security relative to IT/cyber and the EOC.	ergency Operations Center (EOC). The new EM and IT-Cyber facility will require the highest security to keep access operations. Not having this support would jeopardize our ability to detect, prevent, and respond to EM and IT-Cyber d, cypher locks, and video camera system to enhance access and security to the centers. We currently do not have p us to eliminate the use of keys in our environment. This will serve to significantly increase our capacity as it pertains ensing) and adding proximity readers for doors/gates and video security inside and outside the building. This project am by being able to tell who is access which doors and when.
	nent and the Fire/Emergency Managment Department is essential to buying down risk to the city preparedness, ig the risk of cyber events in the community. The physical security measures will assist in preventing unwanted
and the information technology deployed on those information systems	stems, applications, and user accounts owned or operated by, or on behalf of, the local government within the state, is imperative to Carson City and the State of Nevada. Ensuring that the local governments within the state, adopt y adding physical security to the IT/Cyber Department and the Fire/Emergency Managment will promote continuity of
	ify who (i.e., staff, contractor) will perform the work.  ks, communication boards, and electrical wiring) will be implemented by a vendor. As doors readers are installed by rove the installation. IT/Cyber will also monitor, track, investigate, and report any unauthorized attempts to access the
cards, cypher locks, and video camera systems will ensure a more respecific badges/doors are used, increasing our ability to track those at Ensures continuity of IT communication and data networks within the juthose communications or data networks.  This project will prevent, assess and mitigate, to the greatest degree p may impact the performance of information systems within Carson City	prefercy Managment centers and increase our ability to monitor and track door access. The combination of proximity stricted access and monitoring of permitted physical access. These systems allow us the ability to set alerts when ttempting access to secure rooms. urisdiction of the state between the state and local governments within the state in the event of an incident involving possible, cybersecurity risks and threats relating to critical infrastructure and key resources, the degradation of which
Leverage cybersecurity services offered by the Department (See Apper Implement an IT and physical technology modernization review proces	ndix G for additional information on CISA resources and required services and membership).  s that ensures alignment between information technology and operational technology cybersecurity objectives.

9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"

M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant) 9097.10

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

EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for more information on EHP reviews.

and I grant your acco publi vulne reque advis capa the N	Infrastructure It but is a post publicly accordance with it ic, static IPs if erability_info esting this se sories/cyber-It bilities of a S MS-ISAC. Enti	e Security Agence t-award requirer essible web app industry and gov for accessible se @cisa.dhs.gov v ervice as part of nygiene-services SLT's cybersecu ities and their su	y (CISA) nentC lications vernmen ervices a vith the the SLG cNatio rity prog	). For these required cyber Hygiene Servic s by checking for known the best practices and and vulnerabilities. T subject line "Reques CP. For more inform mwide Cybersecurity grams. It is based on ents should complete	services and men ces Web Applicat own vulnerabilities standards. Vulner his service provid- sting Cyber Hygien ation, visit CISA's r Review (NCSR) the National Instities the NCSR, admin	berships, please no ion Scanning is an "s and weak configura ability Scanning evalues weekly vulnerabile Services – SLCGP Cyber Hygiene Infor The NCSR is a free, ute of Standards and istered by the MS-IS	te that participation is no internet scanning-as-a-s ations. Additionally, CIS. Ituates external network ity reports and ad-hoc al " to get started. Indicate mation Page: https://www.anonymous, annual self Technology Cybersecu AC, during the first year	od number of free services be of required for submission a service." This service assess A can recommend ways to e presence by executing contects. To register for these se in the body of your email tw.cisa.gov/topics/cyber-thre-assessment designed to me rity Framework and is spons of the award/subaward per	nnd approval of a es the "health" of enhance security in inuous scans of ervices, email hat you are eats-and- easure gaps and cored by DHS and
<b>✓</b>	Our agency is	already participat	ing in the	e Cyber Hygiene Servi	ces and Nationwide	Cybersecurity Review	* **	es/ncsr (cisecurity.org).  n or as a condition of FY 2022 e will be required to sign up fo	
12. Is cann		scaleable? Can	any par	t of it be reduced or	expanded? Descr	ibe the ways in whic	h the project can be red	uced or expanded, or the re	easons why it
Yes.	Should there r			m the state, Carson Cit curity and the three ph				rant cycles to procure, install,	and make operational.
	oroject location			e project will be exec ne sub-recipient addres					
strict ✓				project focuses on s existing/current level		ability, or the intent o	of the project is to close	a capability gap. Select "su	stain" if the project
15. Is	s this project ct "Yes" if the p			e to other jurisdiction urisdictions (e.g., mult		No" if the project prima	rily supports a single entit	у.	
Each	selection sho Planning - De information Organization - Equipment - E Training - Con Exercises - H real events	uld have an accorvelopment of polici velopment of polici Individual teams, Equipment, supplicatent and methods ands-on activities	mpanying cies, plan an overa es, and s of delive	g item in the line item on the line item	detail budget table of aid agreements, str ture, and leadership ith relevant standard levant training stand	on the next tab ategies, and other pub at each level in the str ds ards	olications; also involves the	ng is being sought for this percollection and analysis of interest of the collection and analysis of interest opportunities to improve capat	illigence and
DI ANNING	COSTS								
PLANNING Planning Cost		Quantity	Unit <sub>T</sub>			hin this element tie i		ld your organization sustair	
Name	Description	Quantity	Cost	project as desc	ribed in the Applic	ation Questions sect	ion. funding v	vas reduced or discontinued	1?
				\$					
				\$					
				\$					
				\$					
				\$					
				\$					
				\$					
				\$					
				\$					
				\$					
				\$					
		0	0.00	\$ 0.00					
				0.00					
ORGANIZA	ATION CO	DSTS			_		3 M. C.		
Organizational Name	l Cost Li	ne Item Descript	ion	Quantity Unit Cost	Total into the Question	how the purchase(s project as described as section.	s) within this element tie in the Application	How would your organizate project if grant funding was discontinued?	
Carson City Fire/Emergency Management		lowable 5% M& A ant management				ing will be the allowab nent of the grants Staff		We would lose the allowable application.	costs from the grant

\$ \$

\$

\$

\$

✓ No

\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$	\$
\$ 10 9,097	\$ 97.10
	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$

<b>EQUIPMEN</b>	T COSTS	3						
Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	•	How would your organization sustain this project if grant funding was reduced or discontinued?	equipment-list to find AEL info	AEL Number - Search - https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Intrusion Security System, Infrastructure Only	System wiring project for the entire system by square feet	18,024	\$ 1.75		Hardware required to support the product/service.	After initial install, the maintenance would be general fund	System, Intrusion Detecti	05NP-00-IDPS
Access Control System, Keypad/Controller	6 panels, one in each external access of the building	6	\$ 5,000.00		Hardware required to support the product/service.	After initial install, the maintenance would be general fund	System, Intrusion Detecti	05NP-00-IDPS
Cypher locks	15 high security point cyphers	15	\$ 2,000.00		Hardware required to support the product/service.	from budget if not funded.	System, Intrusion Detecti	05NP-00-IDPS
Multi-Directional Sensor Camera	10 Multi- Directional Sensor Cameras for intrusion tracking	10	\$ 1,900.00		Hardware required to support the product/service.	from budget if not funded.	Systems, Video Assessment	14SW-01-VIDA
Fish Eye Camera	10 Fish Eye Cameras	10	\$ 900.00		Hardware required to support the product/service.	from budget if not funded.	Systems, Video Assessment	14SW-01-VIDA
Standard Camera	6 Standard Surveillance Cameras	6	\$ 400.00		Hardware required to support the product/service.	from budget if not funded.	Systems, Video Assessment	14SW-01-VIDA
Access Control Proximity Strike pad	20 Proximity Strike pads	20	\$ 1,000.00		Hardware required to support the product/service.	from budget if not funded.	System, Credentialing	4AP-05- CRED
Vendor installation	Contractor will install the hardware and software for physical security.	1	\$ 40,000.00	40,000.00	The Vendor will install the proximity access, Cyphei locks, and video camera security systems.	The program would have to be reduced for		
			\$ \$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
		18,092	\$ <b>\$</b>	\$ <b>\$</b>				
			51,201.75					

TRAININ	TRAINING COSTS								
Training Cost Name	Line Item Description	Quantity	Unit . Cost	Total ti	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 training with the State Training Officer?		
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
		0	\$ 0.00	\$ 0.00			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.	Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		0 \$	0.00	\$		0
				0.00		
Total		0 \$	0.00 \$0	0.00		0

### Document Uploads top

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

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

Application ID: 449130

Become a fan of ZoomGrants\*\*\* on Facebook
Problems\*\* Contact us at Questions\*\* ZoomGrants com
@2002-2003 Grantshugst.com. At pitts reserved.

\*ZoomGrants\* and the ZoomGrants logs are trademarks of GrantAnalyst.com, LLC.
\*Zoom I Errowse\*\*

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

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

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

#### **Carson City School District** State and Local Cyber Security Grants Program

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

\$ 24,401	.60	Reaue	ested

Submitted: 8/29/2023 11:19:53 AM (Pacific)

Jessica Greener

greener@carson.k12.nv.us

Tel: 7752832064

#### Additional Contacts

cperkins@carson.k12.nv.us,rmedeiros@carson.k12.nv.us

#### **Carson City School District**

1402 W King St Carson City, NV 89703 United States

**Director of Fiscal Services** Spencer Winward

swinward@carson.k12.nv.us

775-283-2100 Telephone 775-283-2093 Fax

https://www.carsoncityschools.com/ Web

EIN 886000130 UEI EFKAWSDPMLJ4

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.

✓ 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. 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 preapproved 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 20% cost share requirement for FY 2023 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.

#### 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 Per Dave Fogerson, through Zach Edler, the task force is to consider Carson City a rural area. - AJ 09/11/2023

✓ No

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

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

[	Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
	✓ Objective 3: Implement security protections commensurate with risk.
I	Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	Please select which of the SLCGP program elements your project addresses.  rojects 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.
[	<ul> <li>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.</li> <li>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.</li> </ul>
1	<ul> <li>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.</li> <li>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</li> </ul>
	involving those communications or data networks.  10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which
[	may impact the performance of information systems within the jurisdiction of the state.  11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
	12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
	13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
[	14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
[	15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
l	16. Distribute funds, items, services, capabilities, or activities to local governments.
0	How does your project align with the objective selected in Question 2? ur risk assessments indicate a need for improvements around physical security. The objective of this project is to mitigate the risks associated with unauthorized access.
Α	How does your project align with the program element(s) selected in Question 3? ddressing gaps in our physical security posture would better align us with CISA and NIST best practices. In addition, it would allow us to better protect critical infrastructure and key sources from unauthorized access.
D U	Describe, in detail, how, and by whom, the proposed project will be implemented.  escribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  pon being awarded the grant, the district will purchase the equipment needed to replace our existing unsecured equipment racks with new secured equipment racks. This work will be onducted by district employees and will be scheduled to take place over school breaks to avoid negative impacts to operations.
	Describe, in a few sentences, the desired outcome(s) of your project.  ur desired outcome is to secure access to ICT equipment for the purpose of mitigating cyber risk associated with unauthorized access.
	Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are
th:	staining. If NO, enter "N/A"  &A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of lose involved in the operational aspects of the grant)  A
H E in	D. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and istoric Preservation (EHP) review?  HP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for more formation on EHP reviews.  Yes
	☑ Tes No
11 an graph you are are are the are	I. 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 reart 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 our publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in coordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of ublic, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email ulnerability 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-dvisories/cyber-hygiene-services. "Nationwide Cybersecurity Review (NCSR)" The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and apabilities 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 lee 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), either on our own or as a condition of FY 2022 SLCGP
	<ul> <li>Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP</li> <li>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 proje awarded</li> </ul>

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it

cannot.

This project can be reduced by reducing the number of secure equipment racks that are purchased. However, doing this would have a negative impact on the intended outcome of the project.

	cessary.	anded, we r	need a sp	ecilic r	number of secure equipment rack	s to replace our existing unsecure equi	ornent racks. Purchasing more than what is being requested is					
The p		uld be differe			ct will be executed. recipient address.							
strictl	y maintains a co	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 ntains a core capability at its existing/current level.										
	t "Yes" if the proje				ner jurisdictions? ions (e.g., multiple cities). Select	"No" if the project primarily supports a	single entity.					
<b>✓</b> N												
Each :	selection should he Planning - Develop Information Organization - Indi Equipment - Equip Training - Content	nave an acco oment of policy vidual teams oment, suppliand methods	ompanying cies, plans s, an overa ies, and sy s of delive	item its, process, pr	in the line item detail budget table redures, mutual aid agreements, s nizational structure, and leadersh is that comply with relevant standa comply with relevant training star	e on the next tab strategies, and other publications; also it ip at each level in the structure ards idards	nich funding is being sought for this project.  Involves the collection and analysis of intelligence and analysis of intelligence and and identify opportunities to improve capabilities to respond to					
	ail Budget <u>top</u>											
PLANNING												
Planning Cost Name	Line Item Description	Quantity	Unit T		escribe how the purchase(s) w roject as described in the Appl		How would your organization sustain this project if grant funding was reduced or discontinued?					
				\$								
				\$								
				\$								
				\$								
				\$								
				\$ \$								
				\$								
		0	0.00	\$								
				0.00								
ORGANIZA	ATION COS	TS										
Organizational Name	Cost Line Item Description			Init To		e(s) within this element tie into the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?					
				\$ \$	\$							
				\$	\$							
				\$ \$	\$							
				\$	\$							
				\$	\$							
				\$	\$							
				\$ \$	\$							
				\$	\$							
			0 \$ 0	.00	\$							
EOUIDMEN	UT COSTS			(	0.00							
EQUIPMEN	41 00313				Describe how How would the purchase(s) your within this organization							
Equipment Lin- Cost Name Des		Quantity	Unit Cost	Total	element tie sustain this into the project project if	AEL Name - Search https://www.fema.gov/grants/tools equipment-list to find AEL info	AEL Number - Search /authorized- https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info					

				Questions section.	or discontinued	2	
Storage Cabinet	The Cabinet System is a series of wall-mounted and floor-supported telecommunications enclosures and accessories designed to secure communications equipment for a cross connect.	27	\$ \$ \$ \$ <b>748.00</b> 20,196.00	Our objective is to physically	If funding was reduced or discontinued we would not be able to secure all sites.	Hardware, Computer, Integ	04HW-01-INHW
Storage Cabinet	This compact-sized cabinet helps maximize interior and floor space and is a fitting choice for small data centers. The wall-mount cabinet features a rail mounting system that allows system administrators to install hardware components to suit server room needs.	7	<b>600.80</b> 4,205.60	Our objective is to physically secure access to our Information and Communications Technology (ICT) by replacing unsecured ICT equipment racks with secured racks capable of locking. Doing so will prevent unauthorized access by contractors, vendors, employees, etc. In addition, it will prevent unauthorized configuration changes, additional equipment being added to the network without IT Dept. knowledge, and similar.	reduced or discontinued we would not be able to secure all sites.	Hardware, Computer, Integ	04HW-01-INHW
			\$ \$				
			\$ \$ \$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$ \$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
		34 1	\$ \$ ,348.80 24,401.60				

# **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit Cost		Do you plan to coordinate this training with the State Training Officer?
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	

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

# **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total ti	Describe how the purchase(s) within this element in into the project as described in the Application Duestions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		0 \$	0.00	\$		0
Total		0.4	0.00	00.0		0
TOTAL		0 3	0.00	pu.uu		U

#### Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required?	Attached Documents * 2022 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	✓	Payroll Policies Payroll Policies
Procurement Policy	✓	Purchasing Policies Purchasing Policies
Milestones download template	✓	Milestones
Capabilities Assessment download template	✓	Capabilities Assessment Template

 $<sup>^*</sup>$  ZoomGrants  $^{\text{\tiny TM}}$  is not responsible for the content of uploaded documents.

Application ID: 449453

Become a <u>fan of ZoomGranis</u> on Facebook
Problems? Contact us a <u>Questions BizoomGrants com</u>
©2002-2023 GrantAnalyst.com. All pitts reserved.

"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
LCOOL | Browser.

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

	Applicant Name	Carson City School District	
	Project Name:	State and Local Cyber Security Grants	Progran
	Project Funding Stream:	FY 2023 SLCGP	
	Milestone Description*	Date of Expected Completion	
1	From date of award - Planning	2 months	
2	From date of award - Ordering	3 months	
3	From date of award - 60 % Installation	12 months	
4	From date of award - 100 % Installation	18 months	
5			
6			
7			
8			
9			
10			

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

# City of Reno **CONTINGENT** Core Router Replacement

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

¢	1.	11	25	1 1	24	Requested	
D	- 14	44	OJ.	4.,	24	Requested	

Submitted: 8/31/2023 3:10:29 PM (Pacific)

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

**Additional Contacts** 

none entered

City of Reno

PO Box 1900 Reno. NV 89505 **United States** 

**Director of Finance** Vicki Van Buren vanburenv@reno.gov

Telephone 775-334-3105

Fax

Web reno.gov EIN 88 6000201 UFI TH74SE96JVC7

SAM Expires

#### Pre-A

۱	pplication <u>top</u>
	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.  Yes
	$\square$ 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. 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 20% cost share requirement for FY 2023 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.

#### 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

	nere are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
	Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to
	cybersecurity incidents and ensure continuity of operations.  Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
	Objective 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.
	Coposito 1. Enous organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	ease select which of the SLCGP program elements your project addresses. ects 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.
<b>✓</b>	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.
<b>~</b>	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.
<b>√</b>	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
<b>√</b>	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
<b>√</b>	involving those communications or data networks.  10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
	11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
	12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
1	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.
7	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.
isse	The City has underfunded our network infrastructure replacement plan that has not allowed for these critical central devices to be replaced. Leveraging the network design ssment along with this device replacement will enable the new router to be set up with segmentation best practices to improve cyber resilience. This grant will allow the City to II new redundant core routers with security best practices along with moving off old hardware well beyond its useful life that could start to experience hardware failures in the near e.
Leve This	ow does your project align with the objective selected in Question 2?  raging the network design assessment along with this device replacement will enable the new router to be set up with segmentation best practices to improve cyber resilience.  grant will allow the City to install new redundant core routers with security best practices along with moving off old hardware well beyond its useful life that could start to rience hardware failures in the near future.
	ow does your project align with the program element(s) selected in Question 3? new routers follow the NIST framework - Identify, Protect, Detect, Respond and Recover:
PR.A	AC-5: Network integrity is protected (e.g., network segregation, network segmentation) NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
	DS-2: Data-in-transit is protected -NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
	DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity NIST SP 800-53 Rev. 4 SC-16, SI-7
	YT-4: Communications and control networks are protected - NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, I2, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
DE.C	CM-1: The network is monitored to detect potential cybersecurity events - NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
Des	escribe, in detail, how, and by whom, the proposed project will be implemented.  cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  Senior Network Analyst will rack, install and configure the new core routers.
The	escribe, in a few sentences, the desired outcome(s) of your project.  City of Reno core routers would be upgraded to the latest hardware versions, most recent patches and with the most up to date security features enabled. Redundant power and ears provide for resilience in an attack, equipment failure, or disaster.
are i	anagement & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you retaining. If NO, enter "N/A"
M&A	costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight ose involved in the operational aspects of the grant)
10. [ and <i>EHP</i>	Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning Historic Preservation (EHP) review?  The reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for a information on EHP reviews.
1	Yes No
	TWI I

; ; ;	and ap assess ways t execut registe body o	oproval of a gra ses the "health" to enhance secting continuous or for these serv of your email th	nt but is a p of your pul urity in acco scans of pu vices, email at you are re	oost-aware blicly acc ordance w ublic, stat vulnerab equesting	d requir essible rith indu ic IPs fo ility_info ı this se	ement. —Cyber Hygiene Services—Web Application Scanning is web applications by checking for known vulnerabilities and we stry and government best practices and standards. Vulnerabili r accessible services and vulnerabilities. This service provides @cisa.dhs.gov with the subject line "Requesting Cyber Hygier vice as part of the SLGCP. For more information, visit CISA's ( sories/cyber-hygiene-services. —Nationwide Cybersecurity Revi	s an "internet scanning-as-a-service." This service ak configurations. Additionally, CISA can recommend ty Scanning evaluates external network presence by weekly vulnerability reports and ad-hoc alerts. To be Services – SLCGP" to get started. Indicate in the Cyber Hygiene Information Page:
9 (	self-as Cybers the firs https://	sessment design security Framewat st year of the aw www.cisecurity	gned to mea work and is a ward/subaw y.org/ms-isa	sure gaps sponsore ard perio c/services	s and ca d by DH d of per s/ncsr (c	pabilities of a SLT's cybersecurity programs. It is based on the S and the MS-ISAC. Entities and their subrecipients should con ormance and annually. For more information, visit Nationwide	National Institute of Standards and Technology nplete the NCSR, administered by the MS-ISAC, during Cybersecurity Review (NCSR)
		our agency has no roject is awarded		up for the	Cyber F	giene Services or Nationwide Cybersecurity Review (NCSR), but un	derstands we will be required to sign up for them if our
-	cannot The pro	t.	te replaceme	ent of our o		reduced or expanded? Describe the ways in which the project rs. It would not be best practice to do a partial replacement, nor wou	•
	13. Pro	·	t zip code w	vhere the		will be executed. ipient address.	
	project ☑ B	t strictly mainta				cuses on starting a new capability, or the intent of the project isting/current level.	is to close a capability gap. Select "sustain" if the
		es				jurisdictions? s (e.g., multiple cities). Select "No" if the project primarily supports a	single entity.
	<b>16. Ple</b> Each s □ Pl	ease select all a selection should l	have an acco	ompanying	item in	ion, equipment, training, and exercise (POETE) elements for water line item detail budget table on the next tabures, mutual aid agreements, strategies, and other publications; also	
	☐ O ☑ E:	organization - Ind quipment - Equip raining - Content	oment, suppli and methods	ies, and sy s of delive	stems the	ational structure, and leadership at each level in the structure at comply with relevant standards mply with relevant training standards owledge of plans, allow members to improve their own performance,	and identify opportunities to improve capabilities to respond
Line Iten		ail Budget <u>top</u>					
DI ANN	IINIC	COSTS					
	Cost	Line Item Description	Quantity	Unit Cost	pro	• • • • • • • • • • • • • • • • • • • •	How would your organization sustain this project if grant funding was reduced or discontinued?
					\$		
					\$		
					\$		
					\$		
					\$		
					\$ \$		
					\$		
					\$		
					\$		
			0	0.00	\$		
OBCAL	\   <b>7</b>	TION COS	Te				
		Cost Line Item Description	Qua	ntity Co	nit 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?
					\$ \$		
					\$ \$		
					\$ \$ \$ \$ \$		
					\$ \$ \$ \$ \$ \$		
					\$ \$ \$ \$		

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

EQUIPM	ENT COS	TS					
Equipment Cost Name		Quantity Unit Cost	ho pur wit ele Total pro de: the Ap Qu	escribe ow the urchase(s) thin this ement tie to the oject as siscribed in e oplication uestions ction.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info	AEL Number - Search - https://www.fema.gov/grants/tools/authorized equipment-list to find AEL info
Router - managed - rack- mountable	Router	2 \$ 9,617.09	19,234.18 equare for red and cor sol cor sol wh	dundancy d a mplete lution. The mplete lution is nat follows	This is a complete replacement of the core router, if the funds are not available we would have to re-prioritize what we will accomplish this year with regards to infrastructure and security.	Hardware, Computer, Integ	04HW-01-INHW
Foundation Care Next Business Day Exchange Service - extended service a	Maintenance	2 \$ 2,557.04	5,114.08 equare for red and cor sol cor sol wh	dundancy d a mplete lution. The mplete lution is nat follows	This is a complete replacement of the core router, if the funds are not available we would have to re-prioritize what we will accomplish this year with regards to infrastructure and security.	Hardware, Computer, Integ	04HW-01-INHW
Power supply - hot- plug - 1800 Wa	Internal Parts/Modules	8 \$ 1,781.92	14,255.36 equare for red and cor sol cor sol wh	dundancy d a mplete lution. The mplete lution is nat follows	This is a complete replacement of the core router, if the funds are not available we would have to re-prioritize what we will accomplish this year with regards to infrastructure and security.	Hardware, Computer, Integ	04HW-01-INHW
Management Module - network management device	Parts/Modules	2 \$ 6,407.51	12,815.02 equare for red and cor sol cor sol wh	dundancy d a mplete lution. The mplete lution is nat follows ST	This is a complete replacement of the core router, if the funds are not available we would have to re-prioritize what we will accomplish this year with regards to infrastructure and security.	Hardware, Computer, Integ	04HW-01-INHW
48 Port 1G 10G 25GbE SFP28 v2 Extended Tables Module	Internal Parts/Modules	2 \$ 35,610.30	71,220.60 equare for red and cor sol cor sol	dundancy d a mplete lution. The mplete lution is	This is a complete replacement of the core router, if the funds are not available we would have to re-prioritize what we will accomplish this year with	Hardware, Computer, Integ	04HW-01-INHW

			NIST framework.	regards to infrastructure and security.		
48-port 1GbE Class 4 PoE and 4-port SFP56 v2 Module - switch	Internal Parts/Modules	2 \$ 7,123.84	14,247.68 equipment are needed for redundancy and a complete solution. The complete solution is	This is a complete replacement of the core router, if the funds are not available we would have to re-prioritize what we will accomplish this year with regards to infrastructure and security.	Hardware, Computer, Integ	04HW-01-INHW
	Internal Parts/Modules	2 \$ 349.28	and a complete solution. The complete solution is	This is a complete replacement of the core router, if the funds are not available we would have to re-prioritize what we will accomplish this year with regards to infrastructure and security.	Hardware, Computer, Integ	04HW-01-INHW
FDN SUB 7Y	License and Subscription	2 \$ 3,634.38	\$ The City has 7,268.76 adopted a seven year replacement strategy for IT infrastructure. The City is clearly behind and is trying to catch equipment up to align with that strategy.	Subscription for seven years.	Applications, Software as	04AP-11-SAAS
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		22 \$ 67,081.36	\$ 144,854.24			

# **TRAINING COSTS**

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

# **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	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
	0.00	
Total	0 \$ 0.00 \$0.00	0

# Document Uploads $\underline{top}$

Documents Requested * A-133 Audit (Most Current)	Required?	Attached Documents * A-133 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	~	Payroll Policy
Procurement Policy	✓	Procurement Policy
		Purchasing Policy
Milestones download template	✓	2023 Grant Milestone
Capabilities Assessment download template	✓	Capabilities Assessment

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

Application ID: 449760

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems? Contact us at Questions 8 ZoomGrants.com
©2002-2023 GrantAnalyst.com. All rights reserved.
"ZoomGrants' and the ZoomGrants to go are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	City of Reno
	Project Name:	Core Router Replacement
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Order Approved	October 2023
2	Equipment Ordered	1 Week
3	Equipment Received	Six Weeks
4	Equipment Installed	Two Weeks
5	Equipment Configured	Two Weeks
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

# City of Reno CONTINGENT Network and Security Assessment

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

\$ 52,237.00 Requested

Submitted: 8/31/2023 2:22:45 PM (Pacific)

Project Contact Mark Stone

stonema@reno.gov Tel: 7753343105

Additional Contacts none entered

City of Reno

PO Box 1900 Reno, NV 89505 United States

Director of Finance Vicki Van Buren vanburenv@reno.gov Telephone 775-334-3105

Fax

 Web
 reno.gov

 EIN
 88 6000201

 UEI
 TH74SE96JVC7

SAM Expires

#### Pre-Application top

1. Is your organization one of the following types of entities?: County, municipality, city, town, township, local public authority, school district, special
district, intrastate district, council of government, regional government entity, agency or instrumentality of a local government, rural community,
unincorporated town or village, or other public entity, tribe, or authorized tribal organization.

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. 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 20% cost share requirement for FY 2023 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.

li c	Is this agency considered a rural area (an area encompassing a population of less than 50,000 people)?  i 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 rectly benefit rural Nevadans.  Yes
	☑ Tes ☑ No
2	. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
	Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
	Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
	Objective 3: Implement security protections commensurate with risk.
	Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	. 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.
	<ul> <li>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.</li> </ul>
	3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
	4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
	▼ 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
	6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
	7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
	8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
	9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
	■ 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
	11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
	12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
	13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
	14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
	15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
	☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.

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

The City of Reno would like to engage a consultant to assess the network for network segmentation and security best practice recommendations and changes. The network and security assessment is the first step in identifying vulnerabilities and the best practice steps to remedy those vulnerabilities. Currently the network is very flat with a wide "blast radius" should malware get through. It is also lacking a detailed network diagram of how traffic is flowing and where the critical choke points are if containment is needed. By adopting cybersecurity best practices for a network design it can limit the damage of an intrusion and the ability of an attacker to move laterally. The deliverables for this project include:

Executive Summary

Application Questions top

- Recommendations in a series of deliverable documents
- Logical Network Map
- Layer 2 Topology and Layer 3 Topology for 5 sites/buildings
- · Layer 2 assessment information
- Layer 3 assessment Information, including routing design

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

This assessment is the first step in identifying and prioritizing the gaps we have in our network architecture and lack of segmentation. By using this analysis we can then begin to redesign it so that it's a more defensible network and all flows are documented so that in the event of an attack it can be easier contained.

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

The assessments/scope of work in this project that relate to the elements in question 3:

- · Network discovery with toolset
- •The assessment will discover approximately 175 network devices
- Review of up to 16 Wireless SSID's for security best practices
- $\bullet$  Review firewall connectivity and provide recommendations to best utilize firewalls in network
- Review network to identify opportunities for segmentation to enhance security
- Review L2/L3 connectivity and provide recommendations for a reliable and fault tolerant network
- Layer 2 and Layer 3 connectivity diagrams
- Device configurations (depending on the capabilities of the device)

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

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

	City of Reno IT Manager, Senior Network Engineer and Senior Cybersecurity Analyst will work in conjunction with the consultant engineers to run a toolset and a second to be completed.
The Crequir	scribe, in a few sentences, the desired outcome(s) of your project.  City will receive a deliverable report with prioritized action items. Action items will be assessed and planned based on funding needed, if hardware replacement ed, staff time balance with day to day operations and when changes can be implemented while minimizing down time/user impact. Recommendations with no cial impact will be assessed and scheduled. Recommendations with a financial impact will be assessed and prioritized for budgeting.
	nagement & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter
M&A	costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, ting, oversight of those involved in the operational aspects of the grant)
Envir	oes this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an conmental Planning and Historic Preservation (EHP) review?  The reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidan
attacl	nment for more information on EHP reviews.
<b>✓</b>	
the C for su as-a-s confi Vulne vulne with as pa hygie capal spon- aware	EQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by bersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not requirement approval of a grant but is a post-award requirementCyber Hygiene Services Web Application Scanning is an "internet scanniservice." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak gurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standard erability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and erabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs the subject line "Requesting Cyber Hygiene Services - SLCGP" to get started. Indicate in the body of your email that you are requesting this set into the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/contens-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and bilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of d/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR)
4	://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org). Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 20 SLCGP
	Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up them if our project is awarded
12. Is	this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the
	ons why it cannot.
This p	ons why it cannot.  broject cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.
This p	ons why it cannot.  broject cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  rovide the 5-digit zip code where the project will be executed.  broject location could be different than the sub-recipient address.
13. P The p 89501 14. B "sust	ons why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  provide the 5-digit zip code where the project will be executed.  project location could be different than the sub-recipient address.    uild 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 rain" if the project strictly maintains a core capability at its existing/current level.  Build
13. P The p 89501 14. B "sust	ons why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  project location could be different than the sub-recipient address.  uild 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 reain" if the project strictly maintains a core capability at its existing/current level.
13. P The p 89501 14. B "sust	or why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  provide the 5-digit zip code where the project will be executed.  project location could be different than the sub-recipient address.    uilld 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 rain" if the project strictly maintains a core capability at its existing/current level.    Build   Sustain     this project shareable or deployable to other jurisdictions?     this project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.     Yes   Sustain     The project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
13. P The µ 89501  14. B "sust  ✓  15. Is Select	or why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  provide the 5-digit zip code where the project will be executed.  project location could be different than the sub-recipient address.  uild 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 ain" if the project strictly maintains a core capability at its existing/current level.  Build  Sustain  It this project shareable or deployable to other jurisdictions?  It "Ves" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.  Yes  No  lease select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for the
This p  13. P  The p  89501  14. B  "sust  If the selection of the selecti	or why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  provide the 5-digit zip code where the project will be executed.  project location could be different than the sub-recipient address.  uild 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 ain" if the project strictly maintains a core capability at its existing/current level.  Build  Sustain  It this project shareable or deployable to other jurisdictions?  It "Ves" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.  Yes  No  lease select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this
13. P The p 89501  14. B "sust    15. Is Select    16. P proje Each    17. Is Select    18. Is Select    19. Is Select    19. Is Select    19. Is Select    10. Is Select    11. Is Select    11. Is Select    12. Is Select    13. Is Select    14. Is Select    15. Is Select    16. Is Select    17. Is Select    18. Is Select    19.	ons why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  provide the 5-digit zip code where the project will be executed.  project location could be different than the sub-recipient address.  uild 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 cain" if the project strictly maintains a core capability at its existing/current level.  Build  Sustain  this project shareable or deployable to other jurisdictions?  It "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.  Yes  No  lease select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for thic ct.  selection should have an accompanying item in the line item detail budget table on the next tab  Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information  Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
13. P The p	ons why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  project location could be different than the sub-recipient address.  uild 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 cain" if the project strictly maintains a core capability at its existing/current level.  Build  Sustain  this project shareable or deployable to other jurisdictions?  It "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.  Yes  No  lease select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this calculations in the line item detail budget table on the next tab  Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
13. P The p 14. B 89501  14. B "sust	ons why it cannot.  project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  provide the 5-digit zip code where the project will be executed.  project location could be different than the sub-recipient address.  It will dor 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 rain" if the project strictly maintains a core capability at its existing/current level.  Build  Sustain  It is project shareable or deployable to other jurisdictions?  It "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.  Yes  No  lease select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for thic ct.  selection should have an accompanying item in the line item detail budget table on the next tab  Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information  Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure  Equipment - Equipment, supplies, and systems that comply with relevant standards
13. P The p 89501  14. B "sust V	one why it cannot.  Project cannot be scaled due to the need for a complete assessment. There really is no way to break up the professional services or the deliverables.  Provide the 5-digit zip code where the project will be executed.  Project location could be different than the sub-recipient address.  I will 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 ain" if the project strictly maintains a core capability at its existing/current level.  Build Sustain  It his project shareable or deployable to other jurisdictions?  It "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.  Yes  No  Rease select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for thict.  Selection should have an accompanying item in the line item detail budget table on the next tab  Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information  Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure  Equipment - Equipment, supplies, and systems that comply with relevant training 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

# **PLANNING COSTS**

Planning 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.
Fixed Fee Cost	Total cost for complete assessment.	1	52,237.00	\$ This is a fixed price for the complete network 52,237.00 and security assessment.

in How would your organization sustain this project if grant funding was reduced or discontinued?

This is a one time assessment, if the funds are not available we would have to re-prioritize what we will accomplish this year with regards to infrastructure and security.

\$
 \$
 \$
\$
\$
\$
\$
\$
\$
\$
\$
\$
1 \$
<b>52,237.00</b> 52,237.00

# **ORGANIZATION COSTS**

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Describe how the purchase(s) within this eletal into the project as described in the Application Questions section.	nent tie How would your organization sustain this project if grant funding was reduced or discontinued?
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
		0	\$	\$	
			0.00	.00	

# **EQUIPMENT COSTS**

Eddii iliEiti od							
Equipment Line Item Cost Name Description	Quantity (	Unit . Cost	Total	element tie	organization sustain this project if grant funding was reduced	equipment-list to find AEL info	AEL Number - Search  https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
	0	, \$ 0,00	0.00				
		0.00	0.00				

# **TRAINING COSTS**

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

# Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	_	A-133 Audit
Travel Policy	~	<u>Travel</u>
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement
		<u>Purchasing</u>
Milestones download template	✓	2023 Grant Milestone
Capabilities Assessment download template	✓	<u>Capabilities Assessment</u>

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

Application ID: 449751

Become a fan of ZoomGrants<sup>19</sup> on Facebook
Problems? Contact us at Questions@ZoomGrants.com
@Z002-2023 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Loout | Browser

	Applicant Name	City of Reno
	Project Name:	Network Assessment
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Scope of Work Approval	Sept. 2023
2	Project Initiation	October 2023
3	Planning and Design	2 Weeks
4	Customer UAT Handoff	2 Weeks
5	Final Customer Report and Acceptance	2 Weeks
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

#### City of Reno **CONTINGENT/SUSTAIN** Switch Replacement

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

\$	205,	023.39	Reques	ted
----	------	--------	--------	-----

Submitted: 8/31/2023 3:11:22 PM (Pacific)

Mark Stone

tonema@reno.gov Tel: 7753343105

Additional Contacts

none entered

#### City of Reno

PO Box 1900 Reno, NV 89505 United States

**Director of Finance** Vicki Van Buren vanburenv@reno.gov

Telephone 775-334-3105

Web reno.gov EIN 886000201 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.

Yes

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. 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 preapproved 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 20% cost share requirement for FY 2023 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.

#### 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 2023 SLCGP. Please select the objective with which your project most closely aligns.

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

	Objective O. Hadevetand their aureant subsequently poeture and group for improvement based on continuous testing availation, and structured accompanies
	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.
	lease select which of the SLCGP program elements your project addresses.
Proj	ects 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.
<b>✓</b>	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.
<b>✓</b>	
	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.
4	5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
<b>✓</b>	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.
<b>✓</b>	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.
~	<ul><li>11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.</li><li>12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)</li></ul>
	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.
What The inter targe pane	escribe your project in detail.  at would you like to do? Why? How does this project improve cybersecurity protection for your agency?  City of Reno has 64 network switches that went end of sale starting in 2009 with no new software releases since 2014. These devices are left with CLI management only as the web face requires Java 6 and IE 8 to configure through a GUI limiting the ability of other staff to assist with troubleshooting during an outage. Network infrastructure is becoming a prime et for attackers to hide in as they lack the ability to run monitoring tools leaving a security blind spot that is made worse by no patches. They also prevent the ability to create a single e of glass for all logging to speed up investigation and remediation in the event of an attack. The City has underfunded our network infrastructure replacement plan for many years. This ect would assist the City in getting back inline with consistent replacement.
This easi segr	ow does your project align with the objective selected in Question 2? grant will allow the City to replace unsupported network switches and consolidate around one standardized switch vendor, get ongoing software and security patches again, and allow er standardization of log collection and sharing with any potential State SOC or other syslog system of our own that current devices lack. The switches would be implemented using the mentation best practices outlined in the network assessment. Finally these switches are also part of the network fabric that critical infrastructure like the Stead Wastewater Treatment and the regional 911 CAD public safety and dispatching software traverses that supports the citizens of Reno, Washoe, Sparks, UNR PD, RSIC PD, Pyramid PD, and Reno Airport.
The	ow does your project align with the program element(s) selected in Question 3? new switches follow the NIST framework - Identify, Protect, Detect, Respond and Recover: AC-5: Network integrity is protected (e.g., network segregation, network segmentation) NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
PR.I	DS-2: Data-in-transit is protected NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
PR.I	DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity NIST SP 800-53 Rev. 4 SC-16, SI-7
	PT-4: Communications and control networks are protected NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
DE.	CM-1: The network is monitored to detect potential cybersecurity events NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
Des	escribe, in detail, how, and by whom, the proposed project will be implemented.  cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  Senior Network Analyst will replace unsupported switches with the new hardware and configure each device.
	escribe, in a few sentences, the desired outcome(s) of your project.  oldest City of Reno switches would be upgraded to the latest hardware versions, most recent patches and with the security segmentation best practices configured.
9. M	lanagement & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are
M&A	ining. If NO, enter "N/A"  A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of e involved in the operational aspects of the grant)
	Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and
EHF infor	oric Preservation (EHP) review?  Previews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for more mation on EHP reviews.  Yes

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-

ca the an	pabilities of a SLT's MS-ISAC. Entities d annually. For mor	cybersecu and their su e information	irity progra ubrecipient on, visit Na	ns. It is base s should con tionwide Cyb	ed on the National In aplete the NCSR, addersecurity Review (	nstitute of Standard Iministered by the (NCSR) https://ww	ds and Technology MS-ISAC, during tl w.cisecurity.org/ms	annual self-assessment desigr Cybersecurity Framework and he first year of the award/subar s-isac/services/ncsr (cisecurity. er on our own or as a condition of	is sponsored by DHS and ward period of performance org).
			-					nderstands we will be required to s	
	. Is this project scal nnot.	eable? Can	any part o	f it be reduce	ed or expanded? De	escribe the ways in	n which the project	t can be reduced or expanded,	or the reasons why it
am	ount of switches that	need to be r	replaced. Th	e total of each		is \$6,454.51 and thu		ved for even one switch helps us e scaled up or down. We would be	
Th	. Provide the 5-digit e project location cou 501								
sti	. Build or Sustain: Sictly maintains a co Build Sustain					capability, or the ii	ntent of the project	is to close a capability gap. So	elect "sustain" if the project
Se	. Is this project shar elect "Yes" if the proje Yes				ictions? , multiple cities). Sele	ect "No" if the projec	t primarily supports a	a single entity.	
	ch selection should h	ave an acco	mpanying it	em in the line	item detail budget tab	ble on the next tab	•	which funding is being sought	
	Organization - Indiv Equipment - Equip Training - Content a Exercises - Hands	ment, suppli and methods	ies, and sys s of delivery	ems that com that comply w	structure, and leaders ply with relevant stan ith relevant training st e of plans, allow mem	ndards tandards		and identify opportunities to impro	ove capabilities to respond to
	real events								
	NG COSTS								
Planning Co Name	ost Line Item Description	Quantity	Unit Cost		now the purchase(s) described in the Ap			How would your organizatio funding was reduced or disc	n sustain this project if grant continued?
				\$					
				\$					
				\$					
				\$					
				\$ \$					
				\$					
				\$ \$					
				\$					
		0		\$ \$					
			0.						
	ZATION COST nal Cost Line Item		Uni	t Desc	ribe how the purcha	ase(s) within this e	element tie into the	How would your organiza	tion sustain this project if
Name	Descriptio	n Qua	ntity Cos	t Total proje	ct as described in th			grant funding was reduce	
			\$						
			\$						
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			9	\$					

				0 \$ 0.0	0.00			
EQUIPN	IENT COS	STS						
Equipment Cost Name	Line Item Description Q	uantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	project if	AEL Name - Search https://www.fema.gov/grants/tools/authorized equipment-list to find AEL info	AEL Number - Search - https://www.fema.gov/grants/tools/authorize equipment-list to find AEL info
48FP L2 Stck Cld- Mngd 48x GigE 740W PoE Switch	Switch	27	\$ 5,433.70		The switch and maintenance/warranty follows NIST framework.	These are smaller replacement purchases, we could modify the project as needed.	Hardware, Computer, Integ	04HW-01-INHW
	License and Subscription	27	\$ 1,666.26		The switch and maintenance/warranty follows NIST framework.	These are smaller replacement purchases, we could modify the project as needed.	Applications, Software as	04AP-11-SAAS
24P L2 Stck Cld- Mngd 24x GigE 370W PoE Switch	Switch	3	\$ 3,403.87		The switch and maintenance/warranty follows NIST framework.	These are smaller replacement purchases, we could modify the project as needed.	Hardware, Computer, Integ	04HW-01-INHW
	License and Subscription	3	\$ 1,037.62		The switch and maintenance/warranty follows NIST framework	These are smaller replacement	Applications, Software as	04AP-11-SAAS

purchases, we could modify

the project as needed.

framework.

\$

\$

\$

\$

\$

\$

\$ \$ \$

\$

\$ \$ \$ \$ 11,541.45 205,023.39

# TRAINING COSTS

License and Support, 7YR

INAIMIN	0 00313						
Training Cost Name	Line Item Description	Quantity	Unit . Cost	Total <b>t</b>	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 training with the State Training Officer?
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		0	\$	\$			0
			0.00	0.00			

		STS

Exercise 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.	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 * A-133 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
		Purchasing Policy
Milestones	✓	2023 Grant Milestone
download template		
Capabilities Assessment download template	✓	Capabilities Assessment

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

Application ID: 449761

Become a fan of ZoomGrants\*\*\* on Facebook
Problems\*\* Contact us at Questions 8 ZoomGrants com
@2002-2003 GrantAnalyst.com. At pilips reserved.
\*ZoomGrants\* and the ZoomGrants logs are trademarks of GrantAnalyst.com, LLC.

	Applicant Name	City of Reno
	Project Name:	Unsupported Switch Replacement
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Order Approved	October 2023
2	Equipment Ordered	1 Week
3	Equipment Received	6 Weeks
4	Equipment Configured and Deployed	Three Months
5		
6		
7		
8		
9		
10		

Will request grant year be corrected if contingent project is funded - AJ 09/11/23

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

### **Clark County School District**

# **CONTINGENT** - Incident Response Planning and Tabletop Exercise

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

¢	68	750	ΛΛ	Requested

Submitted: 8/30/2023 2:49:48 PM (Pacific)

### Project Contact

Dirk Florence floreda@nv.ccsd.net

Tel: 702-799-5272

### **Additional Contacts**

abajiv@nv.ccsd.net,delmom@nv.ccsd.net,jonescv1@nv.ccsd.net,sharon.reynolds@kudelskisecurity.com

### **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 EIN

88 6000030 SRBYQ7XFBYA6

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.

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. 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 20% cost share requirement for FY 2023 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.

ation	Questions top
If yo	this agency considered a rural area (an area encompassing a population of less than 50,000 people)?  ur 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 votly benefit rural Nevadans.  Yes
4	No
_	here are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.  Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities 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.
	lease select which of the SLCGP program elements your project addresses. ects 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.
<b>4</b>	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.
<b>√</b>	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 ever of an incident involving those communications or data networks.
	10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
	11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
	12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
	13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
	14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
	15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
	16. Distribute funds, items, services, capabilities, or activities to local governments.
Wha Sec table	escribe your project in detail.  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  Urity Vendor will work with Clark County School District staff to update incident response plans, create additional departmental work aids, and create a tailored stop focused on transportation and food services disruptions due to cyberattack. CCSD is focused on these critical services to ensure continuity of operations.   Effits the 7.24% of rural communities that Clark County School District provides critical services to.
In re	sponse to question 1: There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.
	ow does your project align with the objective selected in Question 2? project ensures that the proper protocols are in place to respond effectively to cybersecurity incidents and ensure continuity of operations.
The	ow does your project align with the program element(s) selected in Question 3? project ensures that there has been proper preparation by examining the response and resilience of the information systems in place. Further, the project will ensuthere will be continuity of service in the event of a cybersecurity incident.

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

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

Security vendor will conduct interviews to collect critical processes, information systems and single points of failure information from CCSD staff. Vendor will update incident response plans, playbooks and create specific departmental work aids to be used in the event of a cybersecurity event. Vendor will facilitate a tabletop exercise with stakeholders. Vendor will update playbooks and provide a after action report.

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

Robust and practical incident response plan that has been tested to ensure resilience of information systems and applications associated with CCSD.

# 9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"

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

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an

	eviews are required for AN ment for more information		the environn	ment or a structure, including small things like putting	nails in walls. Please see the EHP Guidance								
<b>✓</b> 1	No												
the Cy for su as-a-s config Vulne vith t as pa hygie capak spons awarc https:	/bersecurity and Infrastr bmission and approval of tervice." This service ass jurations. Additionally, C rability Scanning evaluate rabilities. This service pithe subject line "Request tt of the SLGCP. For more-servicesNationwide billities of a SLT's cybersectored by DHS and the MS I/subaward period of per //www.cisecurity.org/ms-	ucture Security Agen of a grant but is a pos esses the "health" of CISA can recommend tes external network rovides weekly vulne ting Cyber Hygiene S re information, visit C e Cybersecurity Revie ecurity programs. It i ti-ISAC. Entities and to formance and annua isac/services/ncsr (ci	cy (CISA). It-award req f your publication ways to en ways to en rability reporter ervices – SI SISA's Cybe sew (NCSR)s s based on heir subrecilly. For more security.org	cipients and subrecipients are required to participate these required services and memberships, plantermentCyber Hygiene Services Web Applicity accessible web applications by checking for hance security in accordance with industry and by executing continuous scans of public, static IP ports and ad-hoc alerts. To register for these servity to get started. Indicate in the body of your Hygiene Information Page: https://www.cisa.go The NCSR is a free, anonymous, annual self-assible the National Institute of Standards and Technologients should complete the NCSR, administered re information, visit Nationwide Cybersecurity Regions and Nationwide Cybersecurity Review (NCSR), eignet and Nationwide Cybersecurit	ease note that participation is not required cation Scanning is an "internet scanning-known vulnerabilities and weak government best practices and standards. s for accessible services and ces, email vulnerability_info@cisa.dhs.gov r email that you are requesting this service v/topics/cyber-threats-and-advisories/cyber-tessment designed to measure gaps and gy Cybersecurity Framework and is by the MS-ISAC, during the first year of the eview (NCSR)								
✔ (		LCGP ur 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											
12. Is	this project scaleable? ( ns why it cannot.		reduced or	expanded? Describe the ways in which the proj	ect can be reduced or expanded, or the								
Can n	ot be scaled due to the ver	ndor package of an inci	dent respons	se plan and single tabletop exercise.									
	roject location could be dif	ovide the 5-digit zip code where the project will be executed.  Oject location could be different than the sub-recipient address.											
"susta ✓ E	tild 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 ain" if the project strictly maintains a core capability at its existing/current level.  Build  Bustain												
	′es	• •	•	s? iple cities). Select "No" if the project primarily support	s a single entity.								
projec Each : □ F	ct. selection should have an a	accompanying item in the policies, plans, procedu	he line item d	nent, training, and exercise (POETE) elements for detail budget table on the next tab aid agreements, strategies, and other publications; a									
_				ture, and leadership at each level in the structure									
	Equipment - Equipment, su Training - Content and meth												
	Exercises - Hands-on activi capabilities to respond to re		owledge of p	lans, allow members to improve their own performance	e, and identify opportunities to improve								
- K D-	toll David and ton												
ie item De	tail Budget <u>top</u>												
_ANNING	G COSTS												
anning Cost ime		Quantity Unit Cost	Total ti	Describe how the purchase(s) within this element the into the project as described in the Expplication Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?								
efessional rvices	Professional Services for Incident response plan	1 35,000.00	\$ C	One time cost.	Preparation and planning for the setup of the incident response plan and the tabletop exercise.								
			\$										
			\$										
			\$										
			\$										
			\$										
			<u></u>										

\$

Environmental Planning and Historic Preservation (EHP) review?

\$	
\$	
1 \$ 35,000.00 35,000.00	

# **ORGANIZATION COSTS**

<b>ORGANIZA</b> 7	TION COSTS				
Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total into the project as described in the Application	How would your organization sustain this project if grant funding was reduced or discontinued?
Program Management	Contractor Cost: Program and Project management resources		\$ 175.00	\$ Organizing and managing the completion of the project, 8,750.00 while ensuring that it delivers the expected results on time, on budget, and within scope. 50 hours at \$175 per hour.	One time cost.
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
		50	\$	\$	
			175.00	8,750.00	

# **EQUIPMENT COSTS**

EQUIF MENT COSTS						
Equipment Line Item Cost Name Description Quantity	Unit <sub>T</sub> Cost	otal	purchase(s) within this element tie into the project as described in the	project if	https://www.fema.gov/grants/tools/authorized-	AEL Number - Search https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
	\$	\$				
0	\$	\$				
0	پ 0.00	0.00				

# **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	element tie into the project as described in	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
0.00	0.00	

# **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	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?	Do you plan to coordinate this exercise with the State Exercise Officer?
Professional Services	Services for tabletop exercise	1	\$ 25,000.00 \$ 2	25,000.00	Enhance the response and resilience of critical systems. Ensure the continuity of operations.	One time cost.	Yes
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		1	\$ 25,000.00 \$ 2	25,000.00	)		0
Total		1 9	\$ 25,000.00 \$2	5,000.00	)		0

# Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required? ✓	Attached Documents * CCSD Comprehensive Annual Financial Report
Travel Policy	✓	CCSD Travel Policy
Payroll Policy	✓	CCSD Payroll Policy
Procurement Policy	<b>✓</b>	CCSD Procurement Policy
Milestones download template	✓	CCSD Milestones
Capabilities Assessment download template	✓	CCSD Capabilities Assessment

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

Application ID: 449733

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems' Contact us at Questions @ ZoomGrants com
@Z0002-2023 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:	Incident response tabletop
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Consulting Package	45 days after award
2	Vendor completes interviews	60 days after award
3	Tabletop exercise completed	90 days after award
4		
5		
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

**Clark County School District** 

# **CONTINGENT** - Multi Factor Authentication for 500 CCSD Critical Employees

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

<b>\$ 76,918.98</b> Requested
Submitted: 8/30/2023 1:58:39 PM (Pacific)
Project Contact Dirk Florence floreda@nv.ccsd.net Tel: 702-799-5272
Additional Contacts

### **Clark County School District**

5100 W Sahara Ave Las Vegas, NV 89146 United States

Telephone 702-799-2273

Fax Web

### Pre-A

Dirk Florence		EIN 88 6000030
oreda@nv.ccsd.net	Chief Information Officer	UEI SRBYQ7XFBYA6
<sup>-</sup> el: 702-799-5272	Marilyn Delmont delmom@nv.ccsd.net	SAM Expires
Additional Contacts	<u>aomenio, marcanie.</u>	
sbajiv@nv.ccsd.net, delmom@nv.ccsd.net, jonescv1@nv.ccsd.net, sharon.reynolds@kudelskisecurity.ccsd.net, sharon.reynolds.net, shar	om	
e-Application <u>top</u>		
<ol> <li>Is your organization one of the following types of entities?: County, municipality, city intrastate district, council of government, regional government entity, agency or instruvillage, or other public entity, tribe, or authorized tribal organization.</li> <li>Yes</li> </ol>		
□ No		
2. All funds granted under the State and Local Cybersecurity Grant Program must focus aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).	s on managing and reducing systemic	cyber risk. Does your project proposal
□ No		
of the grant. If you do not send representation to the required meetings, your applicati Meeting dates are to be determined and will be communicated to SLCGP applicants as soon a   I understand and agree.		
4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined to be free and open competition. Applicants are also required to follow the socioeccenterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entity provide a preference for the purchase, acquisition, or use of goods, products, or matering procurement must be pre-approved in writing by the Division of Emergency Management You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement power.	ed that NRS 332.115 is less restrictive onomic steps in soliciting small and m ties should also, to the greatest exten ials produced in the United States, per ent (DEM) in advance of the procurem:	than 2 C.F.R. Part 200. All procurement inority businesses, women's business t t practicable under a federal award, r 2 C.F.R. Part 200.322. Any sole source ent.
5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant available (or expected to be available) to fund that same activity.	reduces their own agency's funds for	an activity because federal funds are
✓ 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 20% cost share requirement for FY 20 requirement.	023 SLCGP. Please acknowledge your	understanding and agreement of this
✓ I understand and agree.		
7. Each jurisdiction must complete its own application. The submitter of the grant applissue a grant. Subgrantees may not pass through or subgrant funds to other agencies/o		Without an application, DEM is unable to

### 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.





2. T	here are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.  Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
	Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
~	Objective 3: Implement security protections commensurate with risk.  Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	lease select which of the SLCGP program elements your project addresses. ects 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.
<b>✓</b>	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.
2	<ul><li>11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.</li><li>12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)</li></ul>
	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.
Wha Purd com Mult	escribe your project in detail.  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project improve cybersecurity protection for your agency?  It would you like to do? Why? How does this project impr
In re	esponse to question 1: There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.
Impl	ow does your project align with the objective selected in Question 2? ementation of Multi Factor Authentication will protect staff user accounts from compromise and provide additional protections against ransomware risks to the district. School icts across the country are experiencing cyber attacks.
Red with	ow does your project align with the program element(s) selected in Question 3?  uce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts in CCSD. Deploying Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the % of rural communities that Clark County School District provides critical services to.
Des Soft	escribe, in detail, how, and by whom, the proposed project will be implemented.  cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  ware as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of s to test the Multifactor Authentication with. Once validated, then CCSD staff will begin to onboard in phases until complete.
	escribe, in a few sentences, the desired outcome(s) of your project. critical district employees will have multi factor authentication protected accounts.
are M&/	lanagement & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you retaining. If NO, enter "N/A"  A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, rejects of the grant).
N/A	sight of those involved in the operational aspects of the grant)
	Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning Historic Preservation (EHP) review?
mor	Previews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for e information on EHP reviews. Yes
	No Yes
	REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the ersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission

The Regulated Services AND Member Ships: All Security and subject line is an authority 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.

https self-a Cybe durin https	://www.cisa.gov/topics/cybossessment designed to me rsecurity Framework and is g the first year of the awar ://www.cisecurity.org/ms-is	er-threats- easure gap s sponsore d/subawa ac/service	and-advisons and capa ed by DHS ard period capa es/ncsr (cis	ories/cyber abilities of and the Man of performan ecurity.org		al
✓		_			res and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP res or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our	
<b>12. Is</b> <b>cann</b> o No.		n any par	rt of it be re	educed or	expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why i	it
Curre	ntly scaled down to most criti	cal accour	nts totaling 5	500. Clark (	County School District has approx. 40,000 employees.	
	rovide the 5-digit zip code project location could be differ S					
proje	uild or Sustain: Select "bui ct strictly maintains a core Build Sustain				tarting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if the nt level.	
	Yes				s? ole cities). Select "No" if the project primarily supports a single entity.	
16. PI Each	lease select all applicable p selection should have an acc Planning - Development of po- information Organization - Individual team Equipment - Equipment, supp Training - Content and method	companying plicies, plan as, an overa plies, and s ds of delive	g item in the ns, procedur all organizat systems that ery that com	e line item of es, mutual tional struct t comply with rele		
Line Item Det	tail Budget <u>top</u>					
PLANNING	G COSTS					
Planning Cost Name	Line Item Description	Quantity	Unit Cost		scribe how the purchase(s) within this element tie into the project this project if grant funding was reduced or discontinued?	in
Program Management	Contractor Cost: Program and Project management resources	150	175.00 26,	250.00 ass enh	nning, oversight and project management to attain milestone delivery One time cost. ociated with: Adopt and use best practices and methodologies to ance cybersecurity – Multi Factor Authentication. 150 hours at \$175 hour.	
				\$		
				\$		
				\$		
				\$		
				\$		
				\$		
				\$		
				\$		
				\$		
				Φ.		
		150		\$ <b>\$</b>		
		150	175.00 26,	\$		
ORGANIZA	ATION COSTS	150	175.00 26,	\$		
Organizationa Cost Name	ll Line Item Description	n Quantit	y Unit Cos	\$ ,250.00	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?	
Organizationa	ı	n Quantit	y Unit Cos	\$ ,250.00	al into the project as described in the Application project if grant funding was reduced or	
Organizationa Cost Name	Line Item Description  Professional Services	n Quantit	y Unit Cos \$ 20,000.0	\$,250.00  St Total  0 20,000.0	al into the project as described in the Application Questions section.  Integration expertise to enhance cybersecurity - Multi O Factor Authentication  project if grant funding was reduced or discontinued?  One time cost.	
Organizationa Cost Name	Line Item Description  Professional Services	n Quantit	y Unit Cos \$ 20,000.0	\$ 250.00  St Total  S 9 9 0 20,000.0	al into the project as described in the Application Questions section.  Integration expertise to enhance cybersecurity - Multi O Factor Authentication  project if grant funding was reduced or discontinued?  One time cost.	

\$

\$

\$

	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
1	\$	\$
	20,000.00 20,0	0,000.00

# **EQUIPMENT COSTS**

	MENT COS	,10					
Equipment Cost Name	t Line Item Description	Quantity Unit Co	<b>st</b> Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	project if	equipment-list to find AEL info	AEL Number - Search - https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
	Multifactor Authentication – 500 accounts				to other district priorities.	Applications, SAAS	04AP-11-SAAS
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$				
			\$ \$ 98 30,668.98				

# TRAINING COSTS

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

# **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	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
Total	0 \$ 0.00 \$0.	.00

### Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	CCSD Comprehensive Annual Report
Travel Policy	<b>✓</b>	CCSD Travel Policy
Payroll Policy	~	CCSD Payroll Policy
Procurement Policy	✓	CCSD Procurement Policy
Milestones download template	✓	CCSD Milestones
Capabilities Assessment download template	✓	CCSD Capabilities Assessment

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

Application ID: 449732

Become a <u>Ian of ZoomGrants</u> on Facebook
Problems? Contact us at <u>Questions 87 ZoomGrants com</u>
£2002-2023 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants log are trademarks of GrantAnalyst.com, LLC.
<u>Locout</u> | <u>Browser</u>

	Applicant Name	Clark County School District
	Project Name:	Multifactor Authentication
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	purchase Software as a Service	45 days after award
2	implement Sandbox environment and test	60 days after award
3	begin onboarding accounts	90 days after award
4	reach 50% deployment	120 days after award
5	complete deployment	180 days after award
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

### **Clark County School District Network Security**

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

\$ 1,291,781.26 Requeste	\$	1	,291	,781	.26	Red	uested
--------------------------	----	---	------	------	-----	-----	--------

Submitted: 8/29/2023 3:05:21 PM (Pacific)

### **Project Contact**

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

### **Additional Contacts**

abajiv@nv.ccsd.net, delmom@nv.ccsd.net, jonescv1@nv.ccsd.net, sharon.reynolds@kudelskisecurity.comainstance. The sharon of the

### 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

EIN 88 6000030 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, intra	istate
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.	

- ✓ 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. 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 preapproved 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 20% cost share requirement for FY 2023 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.

### 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 2023 SLCGP. Please select the objective with which your project most closely aligns.

	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.
	ease select which of the SLCGP program elements your project addresses. scts 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.
	<ul><li>11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.</li><li>12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)</li></ul>
	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.
	<ul><li>15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.</li><li>16. Distribute funds, items, services, capabilities, or activities to local governments.</li></ul>
traffic	otected datacenter applications, critical services and student data are susceptible to cyber security attacks and are at risk. Deploy new capability to monitor, audit, track network cand ensure continuity of communications to these key resources. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.  sponse to question 1: There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.
	ow does your project align with the objective selected in Question 2?  ect datacenter applications, critical services and student data that are currently susceptible to cyber security attacks and are at risk.
Incre Unpr	bw does your project align with the program element(s) selected in Question 3? ase security posture by installing new next-generation firewalls in front of all datacenter resources. Currently, only certain data center resources are protected by firewalls. otected datacenter applications, critical services and student data are susceptible to cyber security attacks and are at risk. Deploy new capability to monitor, audit, track network and ensure continuity of communications to these key resources. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.
<b>7. De</b> Desc Purch	esscribe, in detail, how, and by whom, the proposed project will be implemented.  Secribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The proposed project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The proposed project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The project will be accomplished. Identify who (i.e., staff, contractor) w
Abilit	escribe, in a few sentences, the desired outcome(s) of your project.  y to detect and block malicious traffic to unprotected data center resources. Monitor, audit and track network traffic and activity to and from data center resources. Ensure continuity mmunications and data network within the data center and out to schools. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers.
	anagement & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are
M&A	ning. If NO, enter "NIA"  costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of a involved in the operational aspects of the grant)
	obes this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and
EHP more	oric Preservation (EHP) review? reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for information on EHP reviews.
	Yes No
4	

	Our agency has not yet siç s awarded	gned up for t	he Cyber Hyg	jiene Serv	vices or Nationwide Cybersecurity Re	eview (NCSR), but understands w	e will be requi	red to sign up for them if our project
<b>12. Is</b> canno No.		Can any pa	art of it be re	educed o	r expanded? Describe the ways i	n which the project can be red	uced or expa	anded, or the reasons why it
	rewall sizing is based on t I resources for students a			g through	n the datacenter and out to schools	currently. Scaling down or reducin	g the firewall o	capacity would block access to
	rovide the 5-digit zip co roject location could be di							
projec ✓ E	ct strictly maintains a co				starting a new capability, or the irent level.	ntent of the project is to close	a capability (	gap. Select "sustain" if the
	/es				ns? Itiple cities). Select "No" if the projec	t primarily supports a single entit	<i>i</i> .	
Each   F	selection should have an Planning - Development of Information Organization - Individual to Equipment - Equipment, s Fraining - Content and met	accompanyi f policies, pla eams, an ove upplies, and thods of deliv	ing item in the ans, procedure erall organizat systems that very that com	e line item es, mutua ional stru- t comply v ply with re	elevant training standards	her publications; also involves the	collection and	
Line Item Det	ail Budget <u>top</u>							
PLANNING	COSTS							How would your organization
Planning Cost Name	Line Item Description G		Unit To		ribe how the purchase(s) within tribed in the Application Question		as	sustain this project if grant funding was reduced or discontinued?
Management	Contractor Cost: Program and Project management resources	1,200 17	<b>5.00</b> 210,000	0.00 Deplo comn	ning, oversight and project managen by new capability to monitor, audit, to nunications to these key resources. ng to critical resources for students	ack network traffic and ensure co Mitigate risks and cybersecurity	ntinuity of hreats	: Reduce funding to other district priorities.
				\$				
				\$				
				\$				
				\$				
				\$ \$				
				\$ \$				
				\$				
		1,200 17	<b>5.00</b> 210,000	\$				
ORGANIZA	ATION COSTS							
Organizational Cost Name	Line Item Description	Quantity	Unit Cost		Describe how the purchase(s) wi project as described in the Appli			l your organization sustain this rant funding was reduced or ed?
Consulting Servi	ices Professional Service to implement.	es 1	\$ 70,999.00 7 \$	0,999.00	Installation and configuration of firet traffic. Mitigate risks and cybersecuresources for students and teachers	rity threats relating to critical	N/A - One ti	ime cost.
			\$	\$				
			\$	\$				

\$

\$

\$

\$

\$

\$

	\$	\$	_	
	\$	\$		
	\$	\$		
	\$	\$		
	1 \$	\$		
	70,999.00 70,	999.00		
<b>EQUIPMENT COSTS</b>				
	Describ	o how		

_ ~ ~	MEINI COSIS						
	t Line Item e Description <sup>Quantit</sup>	y Unit Cost	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?	equipment-list to find AEL info	AEL Number - Search - https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Firewall	Virtual 6 Firewalls and Licensing	\$ 5,513.51	33,081.06	6 Deploy new capability to monitor, audit, track network traffic and ensure continuity of communications to these key resources. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers.	Recurring software maintenance is 15,550.92 total. CCSD would reduce funding to other district priorities.		05NP-00-FWAL
Firewall	Hardware 2 Firewalls and Licensing			Deploy new capability to monitor, audit, track network traffic and ensure continuity of communications to these key resources. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers	Recurring software maintenance is 329,175 total. CCSD would reduce funding to other district priorities.		05NP-00-FWAL
		\$	\$				
		\$	\$				
		\$	\$				
		\$ \$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
	8	\$ 494,364.11 1	010 782 26				
		494,304.11 1	,010,782.26	)			

# **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.	project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			

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

# **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total ti	escribe how the purchase(s) within this element e into the project as described in the pplication 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 top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	~	CCSD Comprehensive Annual Financial Report
Travel Policy	✓	CCSD Travel Policy
Payroll Policy	✓	CCSD Payroll Policy
Procurement Policy	✓	CCSD Procurement Policy
Milestones download template	✓	CCSD Milestones
Capabilities Assessment download template	✓	CCSD Capabilities Assessment CCSD Capabilities Assessment

 $<sup>^*</sup>$  ZoomGrants  $^{\text{\tiny TM}}$  is not responsible for the content of uploaded documents.

Application ID: 449664

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems? Contact us at Questions @ ZoomGrants com
@2002-2023 Grant/harlyst.com. All rights reserved.
"ZoomGrants' and the ZoomGrants log are trademarks of Grant/Analyst.com, LLC.
Locol | Browser

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

_	the project at each pride or the project.		
	Applicant Name	Clark County School District	
	Project Name:	Multifactor Authentication Will req	uest title be corrected if project
	Project Funding Stream:	FY 2023 SLCGP is funde	d - AJ 09/11/23
	Milestone Description*	Date of Expected Completion	
	Purchase Firewalls	45 days after award	
2	Receive hardware	120 days after award	
3	Install, configure and test firewalls	180 days after award	
4	Go Live traffic	210 days after award	
į			
•			
-			
8			
9			
1			

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

# FFY 2023 State and Local Cybersecurity Grant Program (SLCGP) Deadline: 8/31/2023

## **Clark County School District Security Awareness Training SAAS**

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

\$ 459,550.00 Requested
Submitted: 8/29/2023 3:57:55 PM (Pacific)
Project Contact Dirk Florence floreda@nv.ccsd.net Tel: 702-799-5272
Additional Contacts

### Pre-A

159,550.00 Requested		
	Clark County School District	
bmitted: 8/29/2023 3:57:55 PM (Pacific)	5100 W Sahara Ave Las Vegas, NV 89146	Telephone 702-799-2273 Fax
pject Contact	United States	Web
k Florence	Chief Information Officer	EIN 88 6000030 UEI SRBYQ7XFBYA6
<u>eda@nv.ccsd.net</u> : 702-799-5272	Marilyn Delmont	SAM Expires
: 702-199-5272	delmom@nv.ccsd.net	CAW Expires
ditional Contacts  ajiv@nv.ccsd.net,delmom@nv.ccsd.net,jonescv1@nv.ccsd.net,sharon.reynolds@kudelskisecurity.com		
Application <u>top</u>		
1. Is your organization one of the following types of entities?: County, municipality, city, to intrastate district, council of government, regional government entity, agency or instrume village, or other public entity, tribe, or authorized tribal organization.		
✓ Yes		
□ No		
2. All funds granted under the State and Local Cybersecurity Grant Program must focus o aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).  ▼ Yes	n managing and reducing systemic	cyber risk. Does your project proposal
□ No		
3. In order for your application to be considered, you must attend open meetings to testify of the grant. If you do not send representation to the required meetings, your application Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the I understand and agree.	will not be considered.	curity Task Force. This is a requiremen
4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PU GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has		
All procurement must be free and open competition. Applicants are also required to follow women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All	w the socioeconomic steps in solicit non-federal entities should also, to cts, or materials produced in the Ur ncy Management (DEM) in advance	ing small and minority businesses, the greatest extent practicable under a ited States, per 2 C.F.R. Part 200.322. of the procurement.
federal award, provide a preference for the purchase, acquisition, or use of goods, production and source procurement must be pre-approved in writing by the Division of Emerger	v and EEMA's contract provisions quide	in the "Pescurce Document" tah
	y and FEMA's contract provisions guide	, in the "Resource Document" tab.
Any sole source procurement must be pre-approved in writing by the Division of Emerger You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement polici  ✓ I understand and agree.  5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant recavailable (or expected to be available) to fund that same activity.		
Any sole source procurement must be pre-approved in writing by the Division of Emerger You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement polici I understand and agree.  5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant recommendation.		
Any sole source procurement must be pre-approved in writing by the Division of Emerger You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policivariant in understand and agree.  5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant recavailable (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 20% cost share requirement for FY 2023 requirement.	duces their own agency's funds for	an activity because federal funds are
Any sole source procurement must be pre-approved in writing by the Division of Emerger You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy    I understand and agree.  5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant recavailable (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 20% cost share requirement for FY 2023	duces their own agency's funds for	an activity because federal funds are

### 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	<ol> <li>There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.</li> <li>Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to</li> </ol>
	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.
	<ul> <li>□ Objective 3: Implement security protections commensurate with risk.</li> <li>■ Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.</li> </ul>
	Objective 4. Ensure organization personner are appropriately trained in cybersecurity, commensurate with responsibility.
	B. 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.
	<ul> <li>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.</li> </ul>
	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.
	<ul> <li>☐ 11. Enhance capabilities to share cycle threat indicators and related information between the state, local governments within the state, and clisa.</li> <li>☐ 12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)</li> </ul>
	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	l. Describe your project in detail.
١	What would you like to do? Why? How does this project improve cybersecurity protection for your agency?
	Purchase SaaS security awareness platform and Enhance the response and resilience of information systems through user security awareness training and phishing testing.
	mplement threat mitigation practices against social engineering through user security awareness training. Increase cybersecurity hygiene training to the district. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.
1	n response to question 1: There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.
	i. How does your project align with the objective selected in Question 2? Ensure staff are appropriately trained in cybersecurity through the use of a security awareness training platform.
E	6. How does your project align with the program element(s) selected in Question 3? Enhance the response and resilience of information systems through user security awareness training and phishing testing. Implement threat mitigation practices against social engineering through user security awareness training. Increase cybersecurity hygiene training to the district. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.
-	. Describe, in detail, how, and by whom, the proposed project will be implemented.
<i>L</i>	Describe, in detail, now, and by wholn, 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.  Purchase SaaS platform for security awareness and phishing testing. Utilize vendor implementation and configuration services. Test phishing testing and security awareness campaigns with pilot group. Go live with full platform functionality.
	B. Describe, in a few sentences, the desired outcome(s) of your project.  Enhance security awareness for 40,000 district employees and perform phishing testing regularly to track progress.
<b>)</b>	D. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, by oversight of those involved in the operational aspects of the grant)
	N/A
1	0. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning
a	and Historic Preservation (EHP) review?
	EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment
	or more information on EHP reviews.  Yes
	□ Yes  ✓ No
1	1. 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

Techn MS-IS	nology Cybersecurity F	ar of the awa	ard/subaw	sored by Dariod	DHS and the MS-ISAC. Entities and their subrecipients of performance and annually. For more information,	
☐ ( <b>☑</b> (	Our agency is already pa	rticipating in th	ne Cyber H	lygiene Ser	vices and Nationwide Cybersecurity Review (NCSR), either vices or Nationwide Cybersecurity Review (NCSR), but un	
12. Is canno No.		? Can any pa	rt of it be	reduced o	or expanded? Describe the ways in which the project	can be reduced or expanded, or the reasons why it
The Sa	aaS platform is provision	ned based on t	he number	r of employe	ees in the district.	
	rovide the 5-digit zip coroject location could be o					
projec	ct strictly maintains a d				starting a new capability, or the intent of the project rent level.	is to close a capability gap. Select "sustain" if the
15. Is Select	this project shareable t "Yes" if the project sup				ons? ultiple cities). Select "No" if the project primarily supports a	a single entity.
<u> </u>						
Each :	selection should have ar	n accompanyii	ng item in t	the line iten	oment, training, and exercise (POETE) elements for wan detail budget table on the next tab al aid agreements, strategies, and other publications; also	
ir	nformation				cture, and leadership at each level in the structure	,
<b>✓</b> E	Equipment - Equipment,	supplies, and	systems th	nat comply	with relevant standards	
□ E	Exercises - Hands-on act		•		elevant training standards plans, allow members to improve their own performance,	and identify opportunities to improve capabilities to
r	espond to real events					
ne Item Det	ail Budget top					
I ANNING	COSTS					
LANNING lanning Cost ame	COSTS  Line Item Description	n Quantity	Unit Cost	Total i	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?
lanning Cost		150	Cost	**Total i	into the project as described in the Application	project if grant funding was reduced or
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	Total i	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	Total i (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	**Total   ***********************************	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	Total	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	Cost	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150 s	Cost	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150	175.00	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame	Line Item Description Contractor Cost: Program and Project	150 s	175.00	Total i (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance	project if grant funding was reduced or discontinued?
lanning Cost ame rogram anagement	Line Item Description  Contractor Cost: Program and Project management resource	150 s	Cost 175.00	Total i ( ) \$ 1 26,250.00 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance security awareness of staff. 150 hours at \$175 per hour.	project if grant funding was reduced or discontinued?  Reduce funding to other district priorities.
lanning Cost ame rogram anagement	Line Item Description  Contractor Cost: Program and Project management resource	150 s	175.00	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance security awareness of staff. 150 hours at \$175 per hour.	project if grant funding was reduced or discontinued?  Reduce funding to other district priorities.
lanning Cost ame rogram anagement	Contractor Cost: Program and Project management resource  ATION COSTS Cost Line Item	150 s	175.00  175.00  Unit Total cost \$ \$	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance security awareness of staff. 150 hours at \$175 per hour.	project if grant funding was reduced or discontinued?  Reduce funding to other district priorities.  How would your organization sustain this project if
lanning Cost ame rogram anagement	Contractor Cost: Program and Project management resource  ATION COSTS Cost Line Item	150 s	175.00  175.00  Unit Total cost \$ \$ \$ \$	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance security awareness of staff. 150 hours at \$175 per hour.	project if grant funding was reduced or discontinued?  Reduce funding to other district priorities.  How would your organization sustain this project if
lanning Cost ame rogram anagement	Contractor Cost: Program and Project management resource  ATION COSTS Cost Line Item	150 s	175.00  175.00  Unit Total cost \$ \$	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance security awareness of staff. 150 hours at \$175 per hour.	project if grant funding was reduced or discontinued?  Reduce funding to other district priorities.  How would your organization sustain this project if
lanning Cost ame rogram anagement	Contractor Cost: Program and Project management resource  ATION COSTS Cost Line Item	150 s	175.00  175.00  Unit Total cost \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	Total i ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	into the project as described in the Application Questions section.  Planning, oversight and project management to enhance security awareness of staff. 150 hours at \$175 per hour.	project if grant funding was reduced or discontinued?  Reduce funding to other district priorities.  How would your organization sustain this project if

\$	\$	
•	<u></u>	
<b>D</b>	ф	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
0 \$ 0.00	\$	
	0.00	

# **EQUIPMENT COSTS**

	MENT COOL							
Equipment Cost Name	t Line Item Description Qua	antity	Unit Cost	Total	purchase(s) within this element tie into the project as described in the	organization sustain this project if grant funding was reduced	equipment-list to find AEL info	AEL Number - Search · https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Security Awareness Platform	Security as a service - Security Awareness Platform – 24 month term	1 4	\$ 400,000.00 400,0	00.00	security	Reduce funding to other district priorities.	Applications, SAAS	04AP-11-SAAS
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$ \$				
		1	<b>D</b>	ф				
			ت 1 <b>00,000.00</b> 400,0	00.00				

# **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
Consulting Services	Implementation Services	1	\$ 33,300.00		Enhance security awareness of staff.	One time cost.	Yes
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		1	\$	\$			0
			33,300.00	33,300.00			

# **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	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?	Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$			
			\$	\$			

	\$	\$	
	\$	\$	
	\$	\$	
	\$	\$	
	\$	\$	
	\$	\$	
	\$	\$	
	\$	\$	
	*		
	\$	\$	
	\$	\$	
	\$	\$	
	\$	\$	
	0 \$ 0.00	\$	0
		0.00	ŭ
Total	0 \$ 0.00 \$0	0.00	0

### Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	CCSD Comprehensive Annual Financial Report
Travel Policy	✓	CCSD Travel Policy
Payroll Policy	✓	CCSD Payroll Policy
Procurement Policy	✓	CCSD Procurement Policy
Milestones download template	✓	CCSD Milestones
Capabilities Assessment download template	✓	CCSD Capabilities Assessment CCSD Capabilities Assessment

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

Application ID: 449665

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems? Contact us at Questions 2 ZoomGrants com
62002-2023 GrantAnalyst.com. All rights reserved.

"ZoomGrants' and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

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

	Applicant Name	Clark County School District
	Project Name:	Security Awareness
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase SaaS	45 days after award
2	Implement and Configure	90 days after award
3	System go live	120 days after award
4		
5		
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

<b>SUSTAIN</b> - Multi Factor Authenticati	on for ALL Employees	
Jump to: Pre-Application Application Questions Line Item	n Detail Budget Document Uploads	
2,800.00 Requested	Clark County School District	
itted: 8/29/2023 2:26:01 PM (Pacific)	5100 W Sahara Ave Las Vegas, NV 89146	Telephone 702-799-2273 Fax
ct Contact  Torence	United States	Web EIN 886000030
a@nv.ccsd.net	Chief Information Officer	UEI SRBYQ7XFBYA6
02-799-5272	Marilyn Delmont delmom@nv.ccsd.net	SAM Expires
ional Contacts @nv.ccsd.net,delmom@nv.ccsd.net,jonescv1@nv.ccsd.net,sharon.reynolds@kudelskisecurity.com		
pplication <u>top</u>		
public entity, tribe, or authorized tribal organization.		
<ul> <li>✓ Yes</li> <li>No</li> <li>2. All funds granted under the State and Local Cybersecurity Grant Program must focus or in achieving this goal? (If not, the project is not eligible for SLCGP funding).</li> <li>✓ Yes</li> </ul>	n managing and reducing systemic	cyber risk. Does your project propo
<ul> <li>✓ Yes</li> <li>No</li> <li>2. All funds granted under the State and Local Cybersecurity Grant Program must focus or in achieving this goal? (If not, the project is not eligible for SLCGP funding).</li> </ul>	n managing and reducing systemic	cyber risk. Does your project propo
<ul> <li>✓ Yes</li> <li>No</li> <li>2. All funds granted under the State and Local Cybersecurity Grant Program must focus or in achieving this goal? (If not, the project is not eligible for SLCGP funding).</li> <li>✓ Yes</li> </ul>	in front of the Governor's Cybersed	
<ul> <li>✓ Yes         No     </li> <li>2. All funds granted under the State and Local Cybersecurity Grant Program must focus or in achieving this goal? (If not, the project is not eligible for SLCGP funding).</li> <li>✓ Yes         No     </li> <li>3. In order for your application to be considered, you must attend open meetings to testify the grant. If you do not send representation to the required meetings, your application will Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the</li> </ul>	in front of the Governor's Cybersed I not be considered.  In not be considered.  In a considered.  In	PURCHASING: LOCAL GOVERNME than 2 C.F.R. Part 200. All procuren nority businesses, women's busine practicable under a federal award 2 C.F.R. Part 200.322. Any sole sou
<ul> <li>✓ Yes</li></ul>	in front of the Governor's Cybersed I not be considered. The dates are known.  RCHASING: STATE and/or NRS 332, that NRS 332.115 is less restrictive mic steps in soliciting small and mishould also, to the greatest extent produced in the United States, per (DEM) in advance of the procureme of and FEMA's contract provisions guide	PURCHASING: LOCAL GOVERNME than 2 C.F.R. Part 200. All procuren nority businesses, women's busines practicable under a federal award, 2 C.F.R. Part 200.322. Any sole south, in the "Resource Document" tab.
<ul> <li>✓ Yes   □ No</li> <li>2. All funds granted under the State and Local Cybersecurity Grant Program must focus or in achieving this goal? (If not, the project is not eligible for SLCGP funding).</li> <li>✓ Yes   □ No</li> <li>3. In order for your application to be considered, you must attend open meetings to testify the grant. If you do not send representation to the required meetings, your application will Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the I understand and agree.</li> <li>4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PUF Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined must be free and open competition. Applicants are also required to follow the socioeconenterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities provide a preference for the purchase, acquisition, or use of goods, products, or materials procurement must be pre-approved in writing by the Division of Emergency Management You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy I understand and agree.</li> <li>5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant red</li> </ul>	in front of the Governor's Cybersed I not be considered. The dates are known.  RCHASING: STATE and/or NRS 332, that NRS 332.115 is less restrictive mic steps in soliciting small and mishould also, to the greatest extent produced in the United States, per (DEM) in advance of the procureme of and FEMA's contract provisions guide	PURCHASING: LOCAL GOVERNME than 2 C.F.R. Part 200. All procuren nority businesses, women's busines practicable under a federal award, 2 C.F.R. Part 200.322. Any sole south, in the "Resource Document" tab.
<ul> <li>Yes</li></ul>	in front of the Governor's Cybersed I not be considered. The dates are known.  RCHASING: STATE and/or NRS 332, that NRS 332.115 is less restrictive mic steps in soliciting small and mi should also, to the greatest extent produced in the United States, per (DEM) in advance of the procureme and FEMA's contract provisions guide luces their own agency's funds for a light state of the procureme and states of the procureme a	PURCHASING: LOCAL GOVERNME than 2 C.F.R. Part 200. All procuren nority businesses, women's busine practicable under a federal award 2 C.F.R. Part 200.322. Any sole sount. In the "Resource Document" tab.

### Application Questions top

✓ I understand and agree.

1. Is this agency considered a rural area	(an area encompassing a	population of less than 50,0	)00 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 2023 SLCGP. Please select the objective with which your project most closely aligns.

workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolister the knowledge, skills, and abilities of parsonned of the state to local governments within the state, to address ophersecurity fivests. and ophersecurity threats use and local governments within the state in the event of an incident working those communications or data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident working those communications or data networks within the present of the state.    11. Enhance capabilities to share opter threat indicators and related information between the state, local governments within the state, and CISA.     12. Leverage ophersecurity services offered by CISA. (See Question 12 for further details on these services.)   13. Implement an information technology and operational technology modernization cybersecurity threats. Local governments within the state, and CISA.     14. Develop and coordinate strategies to address ophersecurity introduced the present of the state of the present of the state of the present of the state of the		
Oppositive 2. Undesteard after current cybersocarulty positive and areas for improvement based on continuous stating, evaluation, and structured assessments.  Oppositive 4. Ensure organization personnel area appropriately trained in systems and store in the state of the state o		
S. Please select which of the SL-COP program elements your project addresses.  The please ray gain will come the contemporary project addresses.  When the contemporary project addresses.  The please ray gain will come the contemporary project addresses.  When the contemporary project addresses.  Personal the delivery of safe, recognizable, and trustworthy orline services by the state to local governments within the state.  The project proje		
3. Please select which of the SLCOP program elements your project addresses. Propose may align with more than one determinate programs, applications, and user accounts comed or operated by, or on behalf of, the state or local governments within the state, and the information schrology dependent of the programs of technology.  2. Moreins, ack, and trade reheaves from Grand actively transiting our traveling legacy information systems, applications, and user accounts owned or operated by, or on behalf the information schrology and the programs of the prog	~	
Projects may align with more sharn one element.  1. Manage, monto, and track information systems, explications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and information technology desployed on those information systems, excluding legacy information reports and information technology desployed on those information systems, excluding legacy information reports and information technology and are no target sequented by if the state or local governments within the state.  2. Monitor, and and track redworks, and read reads on the state or local governments within the state.  3. Enhance trap process of continuous ejemeneutry withing or towned or operated by, or on behalf the state or local governments within the state.  4. Implement process of continuous ejemeneutry intended in a dense reliable of the state or local governments within the state.  5. Enhance the reliable of state, segritation, and user accounts comined or operated by or on behalf of, the state or local governments within the state.  6. Promote the reliable of state, recipitation, and user accounts owned or operated by or on behalf of, the state or local governments within the state.  6. Promote the reliable of state, recipitation, and destructions of the state or local governments within the state.  7. Ensure continuity of operations of the state or local governments within the state, including through the use of the government within the state or local governments w		Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
Nimitage, 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 betwology data systems and information betwology data are no longer supported by the minimal methods of the state of the systems of technology.  2. Monitor, south, and that chemotory designation systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybenocrupir yellows and opheracentry fivens.    Implement a process of continuous cybenecutity vulnerability sasessments and threat miligation practices princitized by degree of risk to address opheracentry with earth of the state or local governments within the state, against cybenocrupir yellows and cybenocrupity threats.   Implement a process of continuous cybenecutity vulnerability sasessments and threat miligation practices princitized by degree of risk to address opheracentry with an expension of the state or local governments within the state, and cybenocrupity intension in the state or local governments within the state, and cybenocrupity intensions in the state or local governments within the state, in the event of a cybenocoruly incident, including by conducting exercises to practice responding to cybenocoruly incident.   In the state or local governments within the state, in the event of a cybenocoruly incident, including by conducting exercises to practice responding to cybenocoruly incident.   In the state or local governments within the state, in the event of a cybenocoruly incident, including by conducting exercises to practice responding to cybenocoruly incident.   In the state or local governments within the state, enhance recruitment and resettion of order to the state or local governments within the state, enhance recruitment and resettion of order to the state or local governments within the state, enhance recruitment and resettion of order to the state or local governments wi		
S. Behance the preparation, response, and eachery smalling or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf the states or local governments within the state.   S. Behance 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 operated private and states of local governments within the state, against operated systems, applications, and user accounts owned or operated by, or on behalf of the state or local governments within the state, or operated by the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf of the state or local governments within the state, or operated by or on behalf or the state or local governments within the state, or operation of the state or local governments within the state, or operated by one operated by one operated by the state or local governments within the state, or operated by one operated		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
Se 2. Enhances the preparation, response, and realismos of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against explorements in season of the state of local governments within the state, adopt and user accounts owned or operated by or on behalf of, the state or local governments within the state, adopt and user best practices and methodologies to enhance cybersecurity.  S. 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 or local governments within the state, adopt and user best practices and methodologies to enhance cybersecurity.  S. Ensure that the state or local governments within the state, control in the state or local governments within the state, or hoster certuration and reterior endors for fortice or local stop or local state or local governments within the state, inchancer certuration and reterior endors for fortice or local governments within the state, fundament or local state or local governments within the state, fundament or local state or local governments within the state, fundament in local state or local governments within the state, fundament or local state or local state or local government within the state or local governments within the state or local governments within the state or local governments within the state or local government or local state or local state or local government within the state or local government within the state or local government within the state or local governments within the state or local government within the state		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,
A Implement a process of continuous opteneously vulnerability assessments and threat militigation practices prioritized by depice of risk to address cybernecutry finks and opteneously threats on information systems, applications, and user accounts sowed or operated by, nor obeating in the state of local governments within the state, adopt and use best practices and methodologies to enhance cybernecutry.  6. Promote the delivery of staff, recognizable, and trustworthy online services by the state or local governments within the state, in the event of a cybersecutry incident, including by conducting exercises to practice responding to a cybersecutry incident, and the state or local governments within the state, in the event of a cybersecutry incident, including by conducting exercises to practice responding to a cybersecutry incident.  8. Use the National Initiative of Cybersecutry Education (NICE) Workforce Framework for Cybersecutry incident, and the state or local governments within the state, or and cybersecutry indicates of the state or local governments within the state, or and cybersecutry indicates and cybersecutry indicates or the state or local governments within the state, or and cybersecutry indicates and replace to the generate degree possible, opherasecutry in feed and cybersecutry indicates and miles and cybersecutry indicates and cybersecutry indicates and miles and cybersecutry indicates and miles and cybersecutry indicates and miles and cybersecutry indicates and cybersecutry indicates and cybersecutry indicates and cybersecutry indicates and miles and cybersecutry indicates and miles and cybersecutry indicates and cybersecutry indicates and cybersecutry indicates and cybersecutry indicates and cybersecutry indicate	<b>✓</b>	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
P. Promote the delivery of safe, recognizable, and frustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.   P. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity developed by NIST to identify and militigate any gaps in the cybersecurity workforces of the state or local governments within the state, in the event of a cybersecurity developed by NIST to identify and militigate any gaps in the cybersecurity workforces of the state or local governments within the state, in additional continuity of communications of the state of local governments within the state, in additional continuity of communications or data network within the present in event of an incident involving those communications or data network within the jurisdiction of the state and local governments within the state in the event of an incident involving those communications or data network within the jurisdiction of the state.  10. Assess and militiage, 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 state, local governments within the state, and CISA.  11. Enhance capabilities to have cyber threat information systems within the state that the cyber of the state.  12. Loverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)  13. Implement an information technology and operational statespace to a charge-capability of the cybersecurity risks and cybersecurity risks and cybersecurity proposes that ensures alignment between information technology and operational statespace to advantage adjacent states in a consultate. Cybersecurity propose cybersecurity risks and cybersecurity freets within the state.  13. Ensurement and incharged and condentate strategies to address explores societies and c		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.
S. 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.    S. Use the National initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and militiative developments within the state, in the event of a personnel of the state or local governments within the state, to address cybersecurity fishs and cybersecurity threats, such as through cybersecurity hygiene training.   S. Ensures continuity of communications and state networks within the jurisdiction of the state and local governments within the state in the event of an incident involving those communications or data networks. With 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. Within the jurisdiction of the state.   10. Assess and mitigate, is 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 between the state, local governments within the state, and CISA.   11. Exhance capubilities to have cyber threat indicators and related information between the state, local governments within the state, and CISA.   13. Implement an information technology and operational technology ordersecurity relevant technology projections to the consulted cybersecurity principle or progree cybersecurity principle and conditions technology ordersecurity risks and cybersecurity principle or the consulted. Cybersecurity Principle or an incident consulting relations or advantage and personal personal should be consulted. Cybersecurity Principle or an incident consulting advantage and personal	~	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
□ 8. Use the National Initiative for Cybernecurity Education (NICE) Workforce Framework for Cybernecurity developed by NIST to identify and mitigate any gaps in the cybernecurity workforces of the state or local governments within the state, to address cybernecurity risks and cybernecurity threats, such as through cybernecurity 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, cybernecurity risks and cybernecurity 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 cybernecurity services offered by CISA, (See Question 12 for further details on these services.)  13. Implement an information technology and operational technology represents the comment of th		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
involving those communications or data networks.    10. Assess and miligate. to the greatest degree possible, cybersecurity risks and oybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.   11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.   12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)   13. Implement an information technology and operational technology and operational technology cybersecurity services offered by CISA. (See Question 12 for further details on these services.)   14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity review process that ensures alignment between information technology and operational technology plant in the state of the coordinate strategies to address 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. Distribute funds, items, services, capabilities, or activities to local governments.   16. Distribute funds, items, services, services, capabilities, or activities to local governments.   16. Distribute funds, items, services, capabilities to local governments.   17. Ensure adequate access to, and participation in, cybersecurity protection for your agency?   Purchase and implement Multi Factor Authentication for Clark County School District Employees protecting student, employee, and district data. Reduce likelihood of account compromise resulting in manormavare land of account compromise. Benefits the 7.24% of rural communities the Clark County School District Employees protecting student, employee, and district data. Reduce likelihood of account compromise control services to.   16. Libertal county are experienc		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
which may impact the performance of information systems within the jurisdiction of the state.    11. Enhance capabilities to share opber threst indicators and related information between the state, local governments within the state, and CISA.   12. Leverage optersecurity services offered by CISA. (See Question 12 for further details on these services.)   13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology objectives.   14. Develop and coordinate strategies to address optersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state shou be consulted. Ophersecurity 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.   17. Ensure adequate access to, and participation in cybersecurity services and programs by rural areas within the state.   18. 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 Multi Factor Authentication for Clark County School District Employees protecting student, employee, and district data. Reduce likelihood of account compromise resulting in ransonware estates. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Deploying protects align with the objective selected in Question 2? Implementation of Multi Factor Authentication with protect staff user accounts from compromise and provide additional protections against ransonware risks to the district. School districts across the country are experiencing cyber attacks.		
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)   13. Implement an information technology and operational technology probesecurity objectives.   14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state show 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.   17. Ensure adequate access to, and participation in, cybersecurity protection for pour agency?   18. Purchase and implement Multi Factor Authentication of Information Systems, applications, and user accounts within CCSD. Purchase and implement full Factor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Deploying Multifactor Authentication and account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Deploying Multifactor Authentication and will reduce the risk of ransomware and account compromise. Benefits the 7.24% of rural communities the Clark County School District provides critical services to.  18. How does your project align with the objective selected in Question 2?  18. How does your project align with the objective selected in Question 3?  18. How does your project align with the program element(s) selected in Question 3?  18. How does your project align with the program element(s) selected in Question 3?  18. How does your project align with the program element(s) selected in Question 3?  18. How does your project align with the program element of the project will be implemented.  29. Despribe, in a fe	_	which may impact the performance of information systems within the jurisdiction of the state.
12. Implementa in information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology objectives.		
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state shou be consulted. Ophersecurity 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.   16. Distribute funds, items, services, capabilities, or activities to local governments.   16. Distribute funds, items, services, capabilities, or activities to local governments.   17. Distribute funds, items, services, capabilities, or activities to local governments.   18. Distribute funds, items, services, capabilities, or activities to local governments.   18. Distribute funds, items, services, capabilities, or activities to local governments.   18. Distribute funds, items, services, capabilities, or activities to local governments.   18. Distribute funds, items, services, capabilities, or activities to local governments.   18. Distribute funds, items, services, capabilities, or activities to local governments.   18. Distribute funds, items, governments,		13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and
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 Multi Factor Authentication for Clark County School District Employees protecting student, employee, and district data. Reduce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Deploying Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24% of rural communities the Clark County School District provides critical services to.  In response to question 1: 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? Implementation of Multi Factor Authentication will protect staff user accounts from compromise and provide additional protections against ransomware risks to the district. School districts across the country are experiencing cyber attacks.  6. How does your project align with the program element(s) selected in Question 3? Reduce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.  7. Describe, in detail, how, and by whom, the proposed project will be implemented.  Describe his process by which the project will be accomplished identify who (i.e., staff, contractor) will perform the work. Software as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of users to test the Multifactor Authentication with. Once validated, then CCSD Enterprise Informat		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.
What would you like to do? Why? How does this project improve cybersecurity protection for your agency?  Purchase and implement Multi Factor Authentication for Clark County School District Employees protecting student, employee, and district data. Reduce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication or Clark County School District provides critical services to.  In response to question 1: 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?  Implementation of Multi Factor Authentication will protect staff user accounts from compromise and provide additional protections against ransomware risks to the district. School districts across the country are experiencing cyber attacks.  6. How does your project align with the program element(s) selected in Question 3?  Reduce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication essential resulting in ransomware attack. Multifactor Authentication in a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24 of rural communities that Clark County School District provides critical services to.  7. Describe, in detail, how, and by whom, the proposed project will be implemented.  Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  Software as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of users to test the Multifactor Authentication with. Once validated, then CCSD Staff will begin to onboard in phases until complete.  8. Describe, in a few sentences, the desired outcome(s) of your project.  All 40,000 district employees will have multi factor authentication protected accounts.  9. Management & Administration (M&A) may be re	<b>✓</b>	
5. How does your project align with the objective selected in Question 2? Implementation of Multi Factor Authentication will protect staff user accounts from compromise and provide additional protections against ransomware risks to the district. School districts across the country are experiencing cyber attacks.  6. How does your project align with the program element(s) selected in Question 3? Reduce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Delpolying Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24 of rural communities that Clark County School District provides critical services to.  7. Describe, in detail, how, and by whom, the proposed project will be implemented.  Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  Software as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of users to test the Multifactor Authentication with. Once validated, then CCSD staff will begin to onboard in phases until complete.  8. Describe, in a few sentences, the desired outcome(s) of your project.  All 40,000 district employees will have multi factor authentication protected accounts.  9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "NA"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversign of those involved in the operational aspects of the grant)  N/A  10. Does this project require new construction, renovation, retrofitting,	What Purd com Mult Clar	at would you like to do? Why? How does this project improve cybersecurity protection for your agency? chase and implement Multi Factor Authentication for Clark County School District Employees protecting student, employee, and district data. Reduce likelihood of account apromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Deploying tifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24% of rural communities that rk County School District provides critical services to.
Implementation of Multi Factor Authentication will protect staff user accounts from compromise and provide additional protections against ransomware risks to the district. School districts across the country are experiencing cyber attacks.  6. How does your project align with the program element(s) selected in Question 3?  Reduce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Deploying Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24 of rural communities that Clark County School District provides critical services to.  7. Describe, in detail, how, and by whom, the proposed project will be implemented. Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  Software as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of users to test the Multifactor Authentication with. Once validated, then CCSD staff will begin to onboard in phases until complete.  8. Describe, in a few sentences, the desired outcome(s) of your project.  All 40,000 district employees will have multi factor authentication protected accounts.  9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "NIA"  MAA costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversigl of those involved in the operational aspects of the grant)  N/A  10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Envi	In re	esponse to question 1: There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.
Reduce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts within CCSD. Deploying Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24's of rural communities that Clark County School District provides critical services to.  7. Describe, in detail, how, and by whom, the proposed project will be implemented.  Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  Software as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of users to test the Multifactor Authentication with. Once validated, then CCSD staff will begin to onboard in phases until complete.  8. Describe, in a few sentences, the desired outcome(s) of your project.  All 40,000 district employees will have multi factor authentication protected accounts.  9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversign of those involved in the operational aspects of the grant)  N/A  10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?  EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for	Impl	lementation of Multi Factor Authentication will protect staff user accounts from compromise and provide additional protections against ransomware risks to the district. School
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  Software as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of users to test the Multifactor Authentication with. Once validated, then CCSD staff will begin to onboard in phases until complete.  8. Describe, in a few sentences, the desired outcome(s) of your project.  All 40,000 district employees will have multi factor authentication protected accounts.  9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversign of those involved in the operational aspects of the grant)  N/A  10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?  EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for	Red withi	duce likelihood of account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, applications, and user accounts in CCSD. Deploying Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransomware and account compromise. Benefits the 7.24%
All 40,000 district employees will have multi factor authentication protected accounts.  9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversign of those involved in the operational aspects of the grant)  N/A  10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?  EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for	Des Soft	scribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work. tware as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will select a small test group of
are retaining. If NO, enter "N/A"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversign of those involved in the operational aspects of the grant)  N/A  10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?  EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for		
and Historic Preservation (EHP) review?  EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for	are M&A of th	retaining. If NO, enter "N/A"  A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight hose involved in the operational aspects of the grant)
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for		
The information on EHP reviews.  ☐ Yes  ☑ No	EHF more	P reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for re information on EHP reviews.  Yes
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 requirementCyber 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 recommen 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	Cyb and asse way exec regi bod http self-	Dersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission approval of a grant but is a post-award requirementCyber Hygiene Services Web Application Scanning is an "internet scanning-asa-service." This service esses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ys to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by cuting continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To ister for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services - SLCGP" to get started. Indicate in the lyof your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: os://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous, annual assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology

	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).									
<del>.</del>				•	ne Services and Nationwide Cybersecurity Review (NCSR), either on our control of the control of	own or as a	condition of FY 2022 SLCGP			
	Our agency has not yet project is awarded	signed up f	or the Cyl	ber Hygie	ne Services or Nationwide Cybersecurity Review (NCSR), but understands	we will be r	required to sign up for them if our			
12. Is canno Yes		le? Can any	part of	it be red	uced or expanded? Describe the ways in which the project can be r	reduced or	expanded, or the reasons why it			
Vice F		nistrators and			s. The MFA software is purchased based on the capacity of users. The proative accounts, reducing the software capacity to support 20,500 critical a					
The p	13. Provide the 5-digit zip code where the project will be executed. The project location could be different than the sub-recipient address.									
89146							West and the state of the state			
proje	ct strictly maintains				ses on starting a new capability, or the intent of the project is to closing/current level.	se a capabi	ility gap. Select "Sustain" if the			
					sdictions? .g., multiple cities). Select "No" if the project primarily supports a single en	ntity.				
<b>✓</b> 1										
					equipment, training, and exercise (POETE) elements for which fun ne item detail budget table on the next tab	nding is bei	ng sought for this project.			
	Planning - Developmer information	t of policies,	plans, pi	rocedures	, mutual aid agreements, strategies, and other publications; also involves	the collection	n and analysis of intelligence and			
					nal structure, and leadership at each level in the structure omply with relevant standards					
			•		omply with relevant standards with relevant training standards					
	Exercises - Hands-on a to real events	activities whi	ch enhan	ce knowle	edge of plans, allow members to improve their own performance, and ident	tify opportuni	ities to improve capabilities to respond			
Line Item Det	ail Budget <u>top</u>									
DI ANNING	COCTC									
PLANNING						Hov	v would your organization sustain			
Planning Cost Name	Line Item Description	Quantity	Unit Cost	Tota	Describe how the purchase(s) within this element tie into the proje described in the Application Questions section.	this	project if grant funding was uced or discontinued?			
Program Management	Contractor Cost: Program and Project management resources	250	175.00		Planning, oversight and project management to attain milestone delivery associated with: Adopt and use best practices and methodologies to entropy cybersecurity – Multifactor Authentication. 250 hours at \$175 per hour.		time cost.			
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
	\$ \$									
	250 \$									
			175.00	43,750.00						
ORGANIZA	ATION COSTS									
Organizationa Cost Name		ription Qu	antity U	nit Cost	Total into the project as described in the Application		your organization sustain this rant funding was reduced or			
Professional Services	Professional Ser	vices to	1 2	\$	\$ Integration expertise to enhance cybersecurity - Multi Factor 20,000.00 Authentication					
COLVICOS	implement WIFA		2	\$	\$					
				\$	\$					
				\$	\$					
				\$	\$					
				\$ \$	\$					

# **EQUIPMENT COSTS**

Equipment Line Item Cost Name Description  Which Cost Name Description of Cuestions of Cuest	L@OII II	WEIGHT COS	J 1 O						
Authentication			Quantity	Unit Cost	Total	how the purchase(s) within this element tie into the project as described in the Application Questions	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-
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	MFA	Authentication – 40,000			9,050.00	best practices and methodologies to enhance cybersecurity – Multi Factor	to other district priorities.		04AP-11-SAAS
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$				\$	\$				
\$ \$ \$ \$ \$ \$ \$ \$				\$					
\$ \$ \$ \$ 1 <b>\$</b> \$				\$					
\$ \$ 1 <b>\$</b> \$									
1 \$ \$				\$					
· · · · · · · · · · · · · · · · · · ·				*					
				τ					

# **TRAINING COSTS**

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?	Do you plan to coordinate this training with the State Training Officer?
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		0	\$ 0.00	\$ 0.00			0

# **EXERCISE COSTS**

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?
		\$	\$		
		\$	\$		
		\$	\$		
		\$	\$		
		Oliantity		Description Quantity Cost Total element tie into the project as described in the	Line Item Quantity Total element tie into the project as described in the project if grant funding was reduced or

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

### Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	CCSD Comprehensive Annual Financial Report
Travel Policy	✓	CCSD Travel Policy
Payroll Policy	✓	CCSD Payroll Policy
Procurement Policy	✓	CCSD Procurement Policy
Milestones download template	✓	CCSD Milestones
Capabilities Assessment	✓	CCSD Capabilities Assessment Update
download template		CCSD Capabilities Assessment

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

Application ID: 449654

Become a fan of ZoomGrants <sup>11</sup> on Facebook
Problems? Contact us at <u>Ouestions ® ZoomGrants com</u>
@2002-2023 GrantAnalyst.com. All rights reserved.

\*ZoomGrants\* and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Locout | Browser

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

	Applicant Name	Clark County School District
	Project Name:	Multifactor Authentication
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	purchase Software as a Service	45 days after award
2	implement Sandbox environment and test	60 days after award
3	begin onboarding accounts	90 days after award
4	reach 50% deployment	180 days after award
5	complete deployment	360 days after award
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

Y 2023 State and Local Cybersecurity Grant Program (SLCGP) adline: 8/31/2023		
("CONTINGE	Ely Shoshone Tribe  NT" Migrate to a .gov internet do	main
	Application Questions Line Item Detail Budget Docum	
\$ 28,487.90 Requested	Ely Shoshone Tribe	
Submitted: 8/28/2023 2:24:02 PM (Pacific)	505 S Pioche Hwy Ely, NV 89301	Telephone (775) 289-3013 Fax
Project Contact Michael Dalton	United States	Web EIN 94 2398696
daltonm@elyshoshonetribe.com Tel: (775) 289-7989	Finance Director Sarah Balares balaress@elyshoshonetribe.com	UEI PHLGX6MG6UK1 SAM Expires
Additional Contacts none entered	valatess & erystrostrottettibe.com	
re-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.  Yes  No  2. All funds granted under the State and Local Cybersecurity Gra achieving this goal? (If not, the project is not eligible for SLCGP Yes  No  3. In order for your application to be considered, you must attend you do not send representation to the required meetings, your application.	estrumentality of a local government, rural communi- int Program must focus on managing and reducing s funding).	ty, unincorporated town or village, or other public entity, ystemic cyber risk. Does your project proposal aid in
Meeting dates are to be determined and will be communicated to SLC  ✓ I understand and agree.  4. All procurement is required to be compliant with Nevada Revis legal opinion, locals may not use NRS 332.115 because it has be competition. Applicants are also required to follow the socioecor firms per 2 C.F.R. Part 200.321. All non-federal entities should alsuse of goods, products, or materials produced in the United State Emergency Management (DEM) in advance of the procurement. You may view FEMA's written legal opinion on NRS 332.115, along wit ✓ I understand and agree.	ed Statute (NRS) 333, PURCHASING: STATE and/or Nen determined that NRS 332.115 is less restrictive the nomic steps in soliciting small and minority business so, to the greatest extent practicable under a federal es, per 2 C.F.R. Part 200.322. Any sole source procur	an 2 C.F.R. Part 200. All procurement must be free and open ses, women's business enterprises, and labor surplus area I award, provide a preference for the purchase, acquisition, or ement must be pre-approved in writing by the Division of
<ul> <li>Supplanting is prohibited under this grant. Supplanting occurs expected to be available) to fund that same activity.</li> <li>I attest that funding for this project does not currently exist within</li> </ul>		unds for an activity because federal funds are available (or
6. Entities applying as a subgrantee must meet a 20% cost share  ✓ I understand and agree.	requirement for FY 2023 SLCGP. Please acknowled	ge your understanding and agreement of this requirement.
<ol> <li>Each jurisdiction must complete its own application. The subr Subgrantees may not pass through or subgrant funds to other ag I understand and agree.</li> </ol>		funds. Without an application, DEM is unable to issue a grant.
oplication 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 supp Nevadans.  Yes  No		rrative what percentage of your project will directly benefit rural
There are four (4) objectives for FY 2023 SLCGP. Please select     Objective 1: Develop and establish appropriate governance struct incidents and ensure continuity of operations.		aligns.  resecurity plans, to improve capabilities to respond to cybersecurity
<ul> <li>Objective 2: Understand their current cybersecurity posture and a</li> <li>✓ Objective 3: Implement security protections commensurate with r</li> <li>Objective 4: Ensure organization personnel are appropriately train</li> </ul>	risk.	ation, and structured assessments.
OSJOSTIO TO ELICUTO OT GENERAL DE LA CONTROL ATO APPROPRIATORY MAIN		

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	on
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 local governments within the state.	or
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.	е
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.	
<ul> <li>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.</li> <li>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</li> </ul>	
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	s
local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.  9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving	
those communications or data networks.  10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may	
impact the performance of information systems within the jurisdiction of the state.  11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.	
☐ 12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)	
12. Levelage cybersecurity services oriered by Crox. (See Question 12 for future 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.	
<ul> <li>15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.</li> <li>16. Distribute funds, items, services, capabilities, or activities to local governments.</li> </ul>	
— 10. Distribute futius, ficinis, services, capabilities, or activities to local governments.	
<ul> <li>4. Describe your project in detail.</li> <li>What would you like to do? Why? How does this project improve cybersecurity protection for your agency?</li> <li>The migration to a .gov domain will increase trust with partners that the Ely Shoshone Tribe government communications are authentic and will improve tribal collective cybersecurity. Using .gov also provides security benefits, like two-factor authentication on the .gov registrar and notifications of DNS changes to administrators.</li> <li>5. How does your project align with the objective selected in Question 2?</li> </ul>	
The Ely Shoshone Tribe (Tribe) project - Migration to a .gov internet domain. Currently, the Tribe is utilizing the domain elyshoshonetribe.com within Google Workspace. The migration achieves Objective 3: "Implement security protections commensurate with risk." and Element 5, "Ensure that the state or local governments within the state adopt and use best practices and methodologi to enhance cybersecurity," and Element 6: "Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the us of the .gov internet domain"	
6. How does your project align with the program element(s) selected in Question 3? Sample Evidence of Implementation: The Ely Shoshone Trine operates only the .gov internet domain and does not use .com, .org, or any other domain.	
7. Describe, in detail, how, and by whom, the proposed project will be implemented.  Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  The Ely Shoshone Tribe will contract with a cyber security consultant to implement the Ely Shoshone Project - migrating to a .gov internet domain.	
8. Describe, in a few sentences, the desired outcome(s) of your project.  Migrate to a .gov internet domain.	
The process to accomplish the Project.  1. Registration for .gov domain  2. Purchase and install Microsoft Office 365 G3 GCC  3. Migration from Google Workforce to Microsoft Office  4. Network Support	
The Requested \$28,487.90 will serve the Ely Shoshone Tribe. The Ely Shoshone Tribe is within White Pine County, Nevada, that is classified as a rural community.	
This project is a new project and has not been budgeted from outside sources.	
9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are	
retaining. If NO, enter "N/A"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)  1356.57	
10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?  EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for more information on EHP reviews.  Yes	
■ No  11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is:	

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).

✓ (	<ul> <li>Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP</li> <li>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</li> </ul>											
	12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot. This project can not be scaled down; the project is to migrate the existing elyshoshonetribe.com to the .gov website and email address.											
The p	13. Provide the 5-digit zip code where the project will be executed.  The project location could be different than the sub-recipient address. 89301											
maint	14. Build or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current level.    Build   Sustain											
	Sustain this project share	able or den	alovablo to ot	har juriedictions?								
	et "Yes" if the project Yes				). Select "No" if the project primarily supports a	single entity.						
						nich funding is being sought for this project.						
	Planning - Developr	ment of polic	ies, plans, pro		ements, strategies, and other publications; also i	nvolves the collection and analysis of intelligence and information						
	•		-	anizational structure, and s that comply with releva	leadership at each level in the structure nt standards							
_	o .		,	t comply with relevant trai	•	nd identify opportunities to improve capabilities to respond to real						
	events			· ····································	, , , , , , , , , , , , , , , , , , , ,							
Line Item Deta	oil Budget ton											
Line item Deta	ali Buuget <u>lop</u>											
DI ANNING	COSTS											
PLANNING Planning Cost		Quantity	Unit Total	Describe how the purch	nase(s) within this element tie into the project	t as How would your organization sustain this project if grant						
Name	Description	Quantity	Cost S	described in the Applica	ation Questions section.	funding was reduced or discontinued?						
			\$									
			\$									
			\$									
			\$									
			\$									
			\$									
			\$									
			\$									
			\$									
		0	0.00 \$									
			0.00									
	ATION COST	5		Describe how	the purchase(s) within this element tie into							
Organizational Name	Cost Line Item Description	Quant	tity Unit Cost		described in the Application Questions	How would your organization sustain this project if grant funding was reduced or discontinued?						
M&A Costs	Grant Administratio		1 \$ 1,356.57		vill be covered through everyday budget planning	<ul> <li>Grant administration will involve quarterly progress reporting, quarterly financial reporting, and maintaining the cyber hygiene services.</li> </ul>						
			\$	\$								
			\$	\$								
			\$ \$	\$ \$								
			\$	\$								
			\$ \$	\$								
			\$	\$								
			\$ \$	\$								
			\$	\$								
			\$	\$								
			1 \$ 1,356.57	\$ 1,356.57								
EOLUBRATI	UT COSTS											
EQUIPMEN	A1 CO212				How would							
				Describe how the purchase(s) within	your organization							
				parando(o) withill								

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	this element tie into the project as described in the Application Questions section.	project if	equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Windows Server	Windows Server and Licensing	1	\$ 3,374.08		This will promote the delivery of safe, recognizable and trustworthy online services by the state of local governments within the State, including through the use of the .gov domain	time purchase that does not require monthly		04HW-01-INHW
O365 Licensing	G3 Licensing for 53 Users	53	\$ 276.00		this will promote the delivery of safe, recognizable and trustworthy online services by the State and Local Governments within the State including through the use of the .gov internet domain	This expense will be covered through normal budget planning	Software as a service	04AP-11-SAAS
Email Backup/Archiving	Email Backup/Archiving Software		\$ 60.00		This will ensure in the event of a disaster, emails are backed up and archived with unlimited cloud storage. Implement Security protections commensurate with risk	will be covered	Software as a service	04AP-11-SAAS
Email Spam Protection	Email Spam Protection Software	53	\$ 60.00		This provides protection against spam/viruses/phishing emails. Implement security protections commensurate with risk	this expense will be covered through normal budget planning	Software as a service	04AP-11-SAAS
Email Migration Software	Used to migrate from gmail to O365	53	\$ 15.00	\$ 795.00	This will promote the delivery of safe, recognizable and trustworthy online services by the state or local government within the state. including through the use of the .gov internet domain	time purchase that doesn't require monthly	Software as a service	04AP-11-SAAS
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
		213	\$ 3,785.08 2	\$ 25,157.08				
			,	,				

# TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	nroject as described in the Application Oligetions 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?
O365 End USer Training	Provide Training to all g end users on how to use O365	13	\$ 149.00		Through training, this will ensure that the state or local governments within the state adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.		
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		13	\$ 149.00	\$ 1,974.25			0

EXERCIS	SE COSTS						
Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total in	Describe how the purchase(s) within this element tie not 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 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 * 2021 Single Audit - Ely Shoshone Tribe
Travel Policy	✓	Ely Shoshone Tribe - Travel Policy
Payroll Policy	~	Ely Shoshone Tribe - General Payroll Policies
Procurement Policy	✓	Ely SHoshone Tribe - Procurement Policy
Milestones download template	~	Ely Shoshone Tribe - Project Milestone
Capabilities Assessment download template	✓	Ely Shoshone Tribe - Capabilities Assessment

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

Application ID: 449563

Become a jan of ZoomGrants <sup>10</sup> on Farebook
Probleme? Contact us at <u>Questions ® ZoomGrants com</u>
©2002-2023 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants og one trademarks of GrantAnalyst.com, LLC.
LCDOL | Browser

	Applicant Name	Ely Shoshone Tribe
	Project Name:	Migrate to a .gov internet domain
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Obtain dot Gov domain	1-Nov
2	Obtain/configure server for DNS	1-Dec
3	Obtain O365 G3 Licensing	15-Dec
4	Setup O365 Tenant	15-Dec
5	Setup Users in O365	20-Dec
6	Verify Domain in O365	29-Dec
7	Setup Security in O365	5-Jan
8	Setup Email Backup/Archiving	5-Jan
9	Setup Email Spam Protection	5-Jan
10	Train End Users on O365	8-Jan

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

### **Nevada Department of Corrections Network Security Firewall System Upgrades**

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

\$ 482,477.81 Requested	Nevada Department of Corrections		
Submitted: 8/31/2023 4:03:22 PM (Pacific)	5500 Snyder Avenue, Building 89 89701, NV 89706	Telephone Fax	17759775608
Project Contact	United States	Web	www.doc.nv.gov
Lisa Lucas  llucas@doc.nv.gov	Director	EIN UEI	886000022 F66UTU4ATHJ1
Tel: 7759775608	James Dzurenda <u>jdzurenda@doc.nv.gov</u>	SAM Expire	es
Additional Contacts cfranklin@doc.nv.gov			

### Pre-A

ject Contact	United States	vveb www.doc.nv.gov	
Lucas	D'accton	EIN 886000022	
as@doc.nv.gov	Director James Dzurenda	UEI F66UTU4ATHJ1	
7759775608	jdzurenda@doc.nv.gov	SAM Expires	
litianal Cantasta	<u>juzurenda@doc.nv.gov</u>		
litional Contacts nklin@doc.nv.gov			
ikiin@doc.nv.gov			
application top			
		nship, local public authority, school district, special district, ir overnment, rural community, unincorporated town or village,	
2. All funds granted under the State and Local Cybers in achieving this goal? (If not, the project is not eligib  Yes  No		ing and reducing systemic cyber risk. Does your project propo	osal aid
3. In order for your application to be considered, you the grant. If you do not send representation to the red Meeting dates are to be determined and will be communic.  I understand and agree.	quired meetings, your application will not be		nent of
Per FEMA legal opinion, locals may not use NRS 332. must be free and open competition. Applicants are all enterprises, and labor surplus area firms per 2 C.F.R. provide a preference for the purchase, acquisition, or procurement must be pre-approved in writing by the I	115 because it has been determined that NRS so required to follow the socioeconomic step Part 200.321. All non-federal entities should use of goods, products, or materials product Division of Emergency Management (DEM) in	IG: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNME 332.115 is less restrictive than 2 C.F.R. Part 200. All procuren is in soliciting small and minority businesses, women's busine also, to the greatest extent practicable under a federal awarded in the United States, per 2 C.F.R. Part 200.322. Any sole sour advance of the procurement.  MA's contract provisions guide, in the "Resource Document" tab.	nent ess I,
<ul> <li>Supplanting is prohibited under this grant. Supplan available (or expected to be available) to fund that sa</li> <li>I attest that funding for this project does not currently</li> </ul>	ame activity.	eir own agency's funds for an activity because federal funds a	re
<ul> <li>6. Entities applying as a subgrantee must meet a 20% requirement.</li> <li>I understand and agree.</li> </ul>	cost share requirement for FY 2023 SLCGP.	Please acknowledge your understanding and agreement of thi	is
<ol> <li>Each jurisdiction must complete its own application issue a grant. Subgrantees may not pass through or s</li> <li>I understand and agree.</li> </ol>		be the recipient of funds. Without an application, DEM is unabs.	ble to

#### 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



2. 11	Displice 1: Design and establish appropriate generators are under a design and appropriate as a second at the propriate generators are under a propriate generators as a second at the propriate generators are under a propriate generators as a propriate generator as a prop
	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.
4	Objective 3: Implement security protections commensurate with risk.
	Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	lease select which of the SLCGP program elements your project addresses. ects may align with more than one element.
<b>✓</b>	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.
<b>✓</b>	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.
<b>~</b>	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.
<b>✓</b>	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.
4	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.
1/2	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.
1	12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
	13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
<b>✓</b>	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.
1	15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
1	16. Distribute funds, items, services, capabilities, or activities to local governments.
4. D	escribe your project in detail.

What would you like to do? Why? How does this project improve cybersecurity protection for your agency? 70% of this project is in rural areas.

Nevada Department of Corrections has security hardware that is aging and in need of replacement. Some of the security appliances are over 8 years old and nearing end of life. The industry recommended lifecycle refresh for security hardware is 5-7 years and when appliances are in production beyond this timeline the following risks may occur: appliances cannot run updated versions of software code, current software code patches and bug fixes will not occur, hardware will not be eligible for break/fix support in case of an outage. This jeopardizes the organization's security as a whole. A firewall hardware refresh offers several cybersecurity benefits:

- \* Advanced Threat Prevention: The updated hardware often comes with enhanced processing power and memory, enabling the firewall to handle more complex threat prevention tasks. This includes real-time analysis of traffic and the ability to identify and block advanced threats such as zero-day exploits and malware.
- \* Higher Performance: Newer hardware typically provides better performance and throughput, allowing the firewall to process network traffic more efficiently. This is crucial for maintaining network speeds while ensuring thorough inspection of traffic for potential threats.
- \* Improved User Experience: Upgraded hardware can result in reduced latency and faster response times for applications and services. This contributes to a positive user experience without compromising security measures.
- \* Enhanced SSL Decryption: Advanced hardware can handle the computational demands of SSL/TLS decryption, enabling the firewall to inspect encrypted traffic for hidden threats. This is becoming increasingly important as more online communications are encrypted.
- \* Centralized Management: A hardware refresh might also come with improvements to the management interface, making it easier for administrators to configure policies, monitor threats, and respond to incidents across the network.
- \* Regulatory Compliance: Up-to-date firewall hardware often supports the latest security standards and protocols, helping organizations maintain compliance with industry and regulatory requirements.
- \* Reduced Risk: By staying current with firewall hardware, organizations can minimize the risk of vulnerabilities associated with outdated systems. Regular hardware updates can help prevent security gaps that attackers might exploit.

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

Implementing security protections commensurate with risk involves tailoring your cybersecurity measures to the specific threats and vulnerabilities your organization faces. Here's how the benefits of a firewall hardware refresh can be aligned with risk mitigation strategies:

- \* Threat Prevention Customization: With advanced threat prevention capabilities offered by the firewall hardware refresh, you can configure specific policies and rules based on the most relevant threats to your organization. This customization ensures that your firewall is focused on addressing the risks that matter most to your environment.
- \* Performance Optimization: By leveraging the higher performance of the updated hardware, you can ensure that security inspections do not slow down network traffic. This prevents the trade-off between security and performance, allowing you to comprehensively protect your network without compromising its functionality.
- \* Targeted Visibility: Enhanced visibility tools provided by the firewall can be used to monitor traffic patterns and identify anomalous behavior. This allows you to pinpoint potential security incidents or risks more effectively and respond in a targeted manner.
- \* Encrypted Traffic Inspection: With the ability to handle SSL decryption efficiently, you can inspect encrypted traffic for hidden threats. This is crucial as attackers increasingly use encryption to evade detection.
- \* Efficient Management and Response: A refreshed firewall management interface can streamline policy configuration and threat response. This allows your security team to allocate resources effectively and respond promptly to emerging risks.
- \* Implementing the necessary steps to align security measures with relevant compliance requirements.
- \* Mitigating Known Vulnerabilities: Regular hardware updates mitigate known vulnerabilities that could be exploited by attackers. This proactive approach reduces the risk of security breaches.
- \* Advanced Threat Prevention: The updated hardware often comes with enhanced processing power and memory, enabling the firewall to handle more complex threat prevention tasks.

This in	cludes real-time analysis	of traffic and the ability t	to identify and block advanced thr	eats such as zero-day explo	oits and malware.
A new facilita goals;	rer, upgraded firewall hard te continuous vulnerability	dware and management s y assessment and threat	t mitigation, and promote the adop	d capabilities that enhance a ption of best practices to enh	in organization's preparation against cyber risks and threats, nance cybersecurity. Here's how the firewalls could achieve these threat mitigation, adopting best practices to enhance
Descri Impler the ha	ibe the process by which a mentation and deployment	the project will be accome twill be completed by a color would assist NDOC will be the project with the project will be accome to the project will be accome.		contractor) will perform the vel as well as vendor professi	work. ional service. NDOC personnel will travel to each location to install Manager would oversee the project build, and provide planning and
The de compli outcor	iance and reporting, secuine of this firewall refresh p	roject include: improved s ire remote access, integr project will center around	security, advanced threat detection ration with security ecosystem, re-	silience and high availability cybersecurity defenses, enh	enhanced visibility, improved performance, efficient management, r, future-readiness, and cost-efficiency. Ultimately, the desired nancing network performance, and ensuring alignment with current nent.
are re M&A o	taining. If NO, enter "N/	/A" costs but are necessary	costs incurred in direct support o		u be retaining funds for M&A? If YES, enter the amount you ence of the grant (i.e., financial management, reporting, oversight
and H EHP r more i	listoric Preservation (EH reviews are required for Al information on EHP review ('es	HP) review? NY project that disrupts	-	•	cture which would necessitate an Environmental Planning tring nails in walls. Please see the EHP Guidance attachment for
<b>✓</b> N	10				
Cyber and a asses: ways execu regist body https: self-at Cyber the fir https:	resecurity and Infrastruct pproval of a grant but is ses the "health" of your to enhance security in a string continuous scans of the form of your email that you a silfwww.cisa.gov/topics/c sessment designed to resecurity Framework and rest year of the award/sulci//www.cisecurity.org/ms	ture Security Agency (( s a post-award require r publicly accessible w accordance with indus of public, static IPs for mail vulnerability_infor are requesting this serv cyber-threats-and-advis measure gaps and cap d is sponsored by DHS blaward period of perfes-isac/services/ncsr (cis ticipating in the Cyber Hy	CISA). For these required servicementCyber Hygiene Service web applications by checking for stry and government best pract accessible services and vulne @cisa.dhs.gov with the subjectivice as part of the SLGCP. For sories/cyber-hygiene-services. pabilities of a SLT's cybersecul S and the MS-ISAC. Entities and formance and annually. For motisecurity.org).	ces and memberships, ple is Web Application Scan or known vulnerabilities a tices and standards. Vulni- trabilities. This service pro- t line "Requesting Cyber I more information, visit CI Nationwide Cybersecurit rity programs. It is based if their subrecipients shou re information, visit Natio ybersecurity Review (NCSR	ticipate in a limited number of free services by the base note that participation is not required for submission uning is an "internet scanning-as-a-service." This service and weak configurations. Additionally, CISA can recommend erability Scanning evaluates external network presence by ovides weekly vulnerability reports and ad-hoc alerts. To Hygiene Services – SLCGP" to get started. Indicate in the ISA's Cyber Hygiene Information Page: by Review (NCSR)– The NCSR is a free, anonymous, annual on the National Institute of Standards and Technology and complete the NCSR, administered by the MS-ISAC, during inwide Cybersecurity Review (NCSR)  1), either on our own or as a condition of FY 2022 SLCGP but understands we will be required to sign up for them if our
canno	ot.		•		project can be reduced or expanded, or the reasons why it
	ense and support years do	•	Hardward, nooriood, a 12pp	of the devices and III	3
	rovide the 5-digit zip cooroject location could be di				
projec	ct strictly maintains a co			ility, or the intent of the p	roject is to close a capability gap. Select "sustain" if the
	res , , , , , , , , , , , , , , , , , , ,		jurisdictions? is (e.g., multiple cities). Select "No	o" if the project primarily sup	ports a single entity.
16. Ple Each : F ii C C	ease select all applicab selection should have an a Planning - Development of information Drganization - Individual te Equipment - Equipment, so Fraining - Content and met	accompanying item in the f policies, plans, procedureams, an overall organization supplies, and systems that thods of delivery that controls of the	the line item detail budget table on ures, mutual aid agreements, strat ational structure, and leadership a lat comply with relevant standards mply with relevant training standar	the next tab egies, and other publication t each level in the structure ds	s for which funding is being sought for this project.  s; also involves the collection and analysis of intelligence and
	Exercises - Hands-on activo real events	vities which enhance kno	owledge of plans, allow members	to improve their own penoiri	nance, and identify opportunities to improve capabilities to respond
Line Item Det	ail Budget <u>top</u>				
PLANNING	COSTS				
Planning Cost Name	Line Item Description	Quantity Unit Cost	Describe how the purch Total element tie into the pro Application Questions s	ject as described in the	How would your organization sustain this project if grant funding was reduced or discontinued?
Project	Project Management &	1	\$ Devise plan to coordinate	with locations, IT staff, and	Utilizing existing permanent NDOC position instead of

Management	Vendor consulting	14,277.46 14,277.46 vendor to deploy	hardware and configure devices.	professional services. Extend timelines to complete installations at each location when IT staff is available.
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		1 \$ 14,277.46 14,277.46		
		, , , , , , , , , , , , , , , , , , , ,		

### **ORGANIZATION COSTS**

OTTO/ TITLE	1011 00010					
Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Tota	Describe how the purchase(s) within this elemen tie into the project as described in the Application Questions section.	t How would your organization sustain this project if grant funding was reduced or discontinued?
Staffing	2 X NDOC staff hourly rate	240	\$ 45.12	\$ 10,828.80	Configure and deploy hardware.	Utilizing existing permanent NDOC positions.
Travel	2 X NDOC staff travel expenses	2	\$ 2,000.00		Deploy hardware at all NDOC locations.	Utilizing existing NDOC Travel funding. Reduce number of staff traveling if needed. Limit overnight travel and, when available, drive instead of fly to destination.
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		242	\$	\$		
			2,045.12	14,828.80		

### **EQUIPMENT COSTS**

	nt Line Item e Description	Quantity	· Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	organization sustain this project if grant funding was reduced	equipment-list to find AEL info	AEL Number - Search  https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
HA Cable	SFP+ FORM FACTOR, 10GB DIRECT ATTACH TWIN- AX PASSI VE CABLE WITH 2 TRANSCEIVER ENDS AND 5M OF CABLE P ERMANENTLY BONDED AS	3	\$ 245.09	\$ 735.27	Required part to connect HA devices together.	One time purchase.	HARDWARE, COMPUTER, INTEG	04HW-01-INHW
Facility Firewall	FIREWALL DEVICES	14	\$ 7,395.14	\$ 103,531.96	Firewall provides network security.	One time purchase.	FIREWALL, NETWORK	05NP-00-FWAL
HA URL Filtering	ADVANCED URL FILTERING SUBSCRIPTION, FOR ONE (1) DEVICE IN AN HA PAIR,	6	\$ 8,802.31		Required software for firewall, provides additional security features.		SOFTWARE, NETWORK	04SW-04-NETW
Firewall URL Filtering	ADVANCED URL FILTERING SUBSCRIPTION,	8	\$ 9,364.16		Required software for firewall,		SOFTWARE, NETWORK	04SW-04-NETW

	FOR ONE (1) DEVICE				provides additional security features.	NDOC base budget.			
Support	PREMIUM SUPPORT, 5 YEARS (60 MONTHS) TERM	14	\$ 8,095.00 1	113,330.00	Required to maintain firewall uptime.	Reduce from 5 years to 1 years. Add to NDOC base budget.	SOFTWARE, NETWORK	04SW-04-NE	TW
Antivirus	ADVANCED THREAT, FOR ONE (1) DEVICE, 5 YEARS (60 MONTHS) TERM	8	\$ 8,802.31	70,418.48	Required software for firewall, provides additional security features.		SOFTWARE, NETWORK	04SW-04-NE	TW
Camp Firewalls	FIREWALL DEVICES	5	\$ 1,295.00	6,475.00	Firewall provides network security.	One time purchase.	FIREWALL, NETWORK	05NP-00-FW	AL
Camp Firewall URL Filtering	ADVANCED URL FILTERING SUBSCRIPTION, 5 YEA RS (60 MONTHS) TERM	5	\$ 1,526.01	7,630.05	Required software for firewall, provides additional security features.		SOFTWARE, NETWORK	04SW-04-NE	TW
Camp Firewall Support	PREMIUM SUPPORT, 5 YEARS (60 MONTHS) TERM	5	\$ 1,320.00	6,600.00	Required software for firewall, provides additional security features.		SOFTWARE, NETWORK	04SW-04-NE	TW
Camp equipment rack	RACK MOUNTABLE TRAY FOR UP TO TWO DEVICESAND 4 PO WER ADAPTERS FOR A 2 POST RACK MOUNT	5			Hardware for camp mounting firewalls.	One time purchase.	HARDWARE, COMPUTER, INTEG	04HW-01-INH	łW
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
		73	\$ 46,934.85 4	\$ 136,897.05					

### TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total ele	escribe how the purchase(s) within this ement tie into the project as described in the oplication 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?
IT Staff Training		150	\$ 109.83		ovide NDOC IT training for hardware configurational document best practices.	Reduce training hours. One time purchase.	No
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		150	\$ 109.83	\$ 16,474.50			0

## **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Describe how the purchase(s) Total element tie into the project as Application Questions section	s described in the project if grant fundi	anization sustain this Do you plan to coordinate thing was reduced or exercise with the State Exercise Office	ate
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			

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

### Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	Single Audit Report
Travel Policy	~	State Administrative Manual
Payroll Policy	~	State Administrative Manual
Procurement Policy	✓	State Administrative Manual
Milestones download template	✓	NDOC Grant Milestones
Capabilities Assessment download template	✓	NDOC Capabilities Assessment

<sup>\*</sup> ZoomGrants™ is not responsible for the content of uploaded documents.

Application ID: 448611

Become a <u>fan of ZoomGrants™</u> on Facebook
Problems? Contact us at <u>Questions® ZoomGrants com</u>
©2002-2023 Grant/hanlyst.com. All rights reserved.

"ZoomGrants" and the ZoomGrants log are trademarks of Grant/Analyst.com, LLC.
<u>Logout</u> | <u>Browser</u>

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

	Applicant Name	Nevada Department of Corrections
	Project Name:	Network Security
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Submit Grant Application	31-Aug
2	Performance Start Date	1-Dec
3	Project delivery plan and schedule	
4	Project team members introduction	
5	Technical Requirements	
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

### **Nevada Secretary of State Nevada Secretary of State Project Orion-Cyber Vault**

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

<b>\$ 1,000,000.00</b> Requested	Nevada Secretary of State		
Submitted: 8/30/2023 3:49:36 PM (Pacific)	101 N Carson St	Telephone	775-684-5709
	Carson City, NV 89701	Fax	
Project Contact	United States	Web	https://www.nvsos.gov/sos
Shauna Bakkedahl		EIN	886000022
shauna.b@sos.nv.gov	ASO 3	UEI	
Tel: 775-230-8686	Ashley Griffitts	SAM Expire	es
	dalea@sos.nv.gov		
Additional Contacts			
none entered			

Application Questions top

Yes ✓ No

benefit rural Nevadans.

mitted: 8/30/2023 3:49:36 PM (Pacific)  ject Contact una Bakkedahl una.b@sos.nv.gov 775-230-8686  litional Contacts e entered	101 N Carson St Carson City, NV 89701 United States  ASO 3 Ashley Griffitts dalea@sos.nv.gov	Telephone Fax Web EIN UEI SAM Expire	775-684-5709 https://www.nvsos.gov/sos 886000022
Application <u>top</u>			
Is your organization one of the following types of entities?: district, council of government, regional government entity, as public entity, tribe, or authorized tribal organization.  ✓ Yes  No			
2. All funds granted under the State and Local Cybersecurity G in achieving this goal? (If not, the project is not eligible for SL  ✓ Yes  No		systemic cyl	ber risk. Does your project proposal aid
3. In order for your application to be considered, you must atte the grant. If you do not send representation to the required me Meeting dates are to be determined and will be communicated to St I understand and agree.	eetings, your application will not be considered.	Cybersecur	ity Task Force. This is a requirement of
4. All procurement is required to be compliant with Nevada Rev Per FEMA legal opinion, locals may not use NRS 332.115 beca must be free and open competition. Applicants are also requirenterprises, and labor surplus area firms per 2 C.F.R. Part 200. provide a preference for the purchase, acquisition, or use of genocurement must be pre-approved in writing by the Division of You may view FEMA's written legal opinion on NRS 332.115, along understand and agree.	use it has been determined that NRS 332.115 is less re ed to follow the socioeconomic steps in soliciting sm .321. All non-federal entities should also, to the great oods, products, or materials produced in the United S of Emergency Management (DEM) in advance of the p	estrictive tha all and mino est extent pr tates, per 2 ( rocurement	an 2 C.F.R. Part 200. All procurement rity businesses, women's business racticable under a federal award, C.F.R. Part 200.322. Any sole source
<ul> <li>5. Supplanting is prohibited under this grant. Supplanting occavailable (or expected to be available) to fund that same activ</li> <li>I attest that funding for this project does not currently exist with</li> </ul>	rity.	unds for an	activity because federal funds are
Entities applying as a subgrantee must meet a 20% cost sharequirement.  I understand and agree.	are requirement for FY 2023 SLCGP. Please acknowled	dge your und	derstanding and agreement of this
<ul> <li>7. Each jurisdiction must complete its own application. The suissue a grant. Subgrantees may not pass through or subgrant I understand and agree.</li> </ul>		f funds. With	hout an application, DEM is unable to

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

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

<ol> <li>There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.</li> <li>Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respective incidents and ensure continuity of operations.</li> </ol>	pond 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 within the state 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 or the state or local governments within the state.	n behalf of,
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 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.	s and
<ul> <li>5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.</li> <li>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 into domain.</li> </ul>	ernet
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 practic responding to a cybersecurity incident.	ce
<ul> <li>8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cyb workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and ability personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.</li> <li>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 extension of the state and local governments.</li> </ul>	ities of
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 degrada	
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.	illori oi
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)	
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology operational technology cybersecurity objectives.	y and
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.	ate should
<ul> <li>15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.</li> <li>16. Distribute funds, items, services, capabilities, or activities to local governments.</li> </ul>	
<ul> <li>4. Describe your project in detail.</li> <li>What would you like to do? Why? How does this project improve cybersecurity protection for your agency?</li> <li>Cyber recovery vault - This is a disaster recovery solution that will facilitate real time backups, reducing the time to restore to minutes vs. days. This will be used for both the licensing portal and processing systems. Quickly identify clean copies of data for the purpose of recovery. Isolation, immutable backups, comprehensive scanning, and detail reporting allows the Cyber Recovery Secretary of State's Office, Nevada to recover critical systems with confidence.</li> <li>5. How does your project align with the objective selected in Question 2?</li> </ul>	
The Cyber Vault is an air-gapped data backup and ransomware recovery solution. This does not replace our current backup hardware, this product is specifically meeting the having an immutable, offline backup of our most precious data.	gap of not
6. How does your project align with the program element(s) selected in Question 3?  The Cyber Vault is an automated "operational air gap," through which ingestion of data and management of the process is automated and policy-driven, requiring no manual in This operational air gap delivers network isolation, inaccessible from production and from unsecured networks. It will eliminate production-accessible management interfaces to be compromised. The cyber-Vault deployed within the secured vault environment (Switch Facility), which automates data synchronization between the vault and production so creating immutable copies with locked retention policies. Additionally, the Vault will run analytics designed to detect potential issues early.	that can
7. Describe, in detail, how, and by whom, the proposed project will be implemented.  Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  This is software that will be installed by the vendor at the Switch facility where it will be stored in an air-gapped environment.	
8. Describe, in a few sentences, the desired outcome(s) of your project.  This will provide the Secretary of State the to an isolated recovery solution that will minimize the downtime, expense, and lost revenue by providing a resilient backup to critical path to recovery from a cyber event.	al data and
9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amo	unt you
are retaining. If NO, enter "N/A"  M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, of those involved in the operational aspects of the grant)  N/A	oversight
10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Pla	anning
and Historic Preservation (EHP) review?  EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachmore information on EHP reviews.	ment for
<ul><li>✓ Yes</li><li>✓ No</li></ul>	
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 subm and approval of a grant but is a post-award requirementCyber Hygiene Services Web Application Scanning is an "internet scanning-as-a-service." This se assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can rec aways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network prese executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services - SLCGP" to get started. Indicate	ervice commend ence by s. To

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).

		not yet signed	-				er on our own or as a condition of FY 2022 SLCGP inderstands we will be required to sign up for them if our			
		aleable? Car	any par	t of it be re	educed or expanded? Descri	be the ways in which the projec	t can be reduced or expanded, or the reasons why it			
	cannot.  Yes, the project is scalable and can be expanded and offers additional features if needed. No we would not want to reduce the project as it is intended to support all systems date within the Secretary of State.									
	13. Provide the 5-digit zip code where the project will be executed.									
	The project location could be different than the sub-recipient address. 89701									
	14. Build or Sustain: project strictly maint  ☑ Build ☐ Sustain					bility, or the intent of the project	t is to close a capability gap. Select "sustain" if the			
	15. Is this project sha	areable or de	nlovable	to other is	riedictions?					
						lo" if the project primarily supports	a single entity.			
	16. Please select all	applicable p	anning,	organizatio	on, equipment, training, and	exercise (POETE) elements for	which funding is being sought for this project.			
	Each selection should	have an acco	mpanyin	g item in the	e line item detail budget table o	n the next tab	involves the collection and analysis of intelligence and			
	Organization - Inc			-	tional structure, and leadership					
					t comply with relevant standard ply with relevant training standa					
	Exercises - Hand						and identify opportunities to improve capabilities to respond			
	to real events									
l ine Ite	m Detail Budget <i>top</i>									
Line ite	in Detail Budget <u>lop</u>									
	NING COSTS		Unit	Dosor	ibe how the nurshace(s) with	ain this alamant tip into the	How would your organization custoin this project if			
Name	Cost Line Item Description	Quantity	Unit T		ibe how the purchase(s) with at as described in the Applica		How would your organization sustain this project if grant funding was reduced or discontinued?			
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
				\$						
		0	0.00	\$ 0.00						
ORGA	NIZATION COS	STS								
Organiza	ational Cost Line Iten	) Oua	atitv			) within this element tie into the				
Name	Descripti	on	, с	st s	project as described in the Ap	oplication Questions section.	grant funding was reduced or discontinued?			
				\$ \$						
				\$ \$						
				\$ \$						
				\$ \$ \$ \$						
				\$ \$						
				\$ \$						
				\$ \$						
				\$ \$ \$ \$						
				\$ \$						
				\$ \$						
			0 6 5	\$ \$						
			0 \$ 0	0.00						

EQUIPN	MENT COSTS					
Equipment		Unit Cost T	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	organization sustain this project if grant funding was reduced	equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Dell Cyber Vault	Data 1 Protection Software	\$ 1,000,000.00 1,000,000	critical data within the Secretary of	All updates and patches will be handled through the budget here at the SOS.	System, Intrusion Detecti	05NP-00-IDPS
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
		\$	\$			
	1	\$ 1,000,000.00 1,000,000	\$			
		1,000,000.00	7.00			

### **TRAINING COSTS**

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

### **EXERCISE COSTS**

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	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?	Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			

	\$ \$	
	\$ \$	
	<b>0</b> \$ 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 * A133 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	Milestones
Capabilities Assessment download template	✓	

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

Application ID: 449040

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems? Contact us at <u>Questions ® ZoomGrants com</u>
©2002-2023 GrantAnsilyst.com. All rights reserved.

"ZoomGrants' and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

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

	Applicant Name	Nevada Secretary of State
	Project Name:	Project Orion
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase of Cyber Vault Software	7/1/2024
2	Installation of software	7/1/2024
3		
4		
5		
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

# Nye County CONTINGENCY Nye County Firewall Upgrade

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

\$ 62,219.49 Requested

Submitted: 8/30/2023 10:04:09 AM (Pacific)

Project Contact Stephani Elliott

sdelliott@nyecountynv.gov

Tel: (775) 277-0706 or (775) 751-6355

**Additional Contacts** 

dplazenby@nyecountynv.gov,Jemccutcheon@nyecountynv.gov

#### Nye County

101 Radar Rd PO Box 153 Tonopah, NV 89049 United States

Chair, Board of Nye County Commissioners

Bruce Jabbour

bijabbour@nyecountynv.gov

Telephone (775) 482-8192 or (775) 751-7075 Fax (775) 482-8198 or (775) 751-7093

Web www.nyecountynv.gov EIN 886000111

EIN 886000111 UEI DN3MR2UV3DM7

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.

Yes

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. 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 20% cost share requirement for FY 2023 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.

#### 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 2023 SLCGP. Please select the objective with which your project most closely aligns.	
Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.	ond
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 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 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.	and
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 interdomain.	rnet
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.	е
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, sk and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hyginalized.	
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 degradati of which may impact the performance of information systems within the jurisdiction of the state.	on
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.	
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)	
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology operational technology cybersecurity objectives.	and
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.	е
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 upgrade one of our current firewalls, consolidate our current web filter into the new upgraded firewall and add an extended retention logging and reporting server for activity and events on the firewall. This upgrade with extended logging will better allow us to monitor, audit and track activity and security events as well as review for changes in state, correlation and reporting of events to help identify, assess and mitigate cybersecurity risks. The improved processing and memory performance of the upgraded device will also allow for inspection of SSL secure web traffic in addition to running Intrusion Detection and Advanced Threat Protection on the same device.

100% of this funding will support rural communities throughout Nye County.

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

This project aligns with objective #3 in question 2: "Implement security protections commensurate with risk" by helping to identify, assess and mitigate cybersecurity risks.

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

An upgraded firewall will increase protection for Nye County's network from unauthorized access by outside entities with malicious intent. Network stability not only ensures continuity of government operations, but it also ensures continuity of communications for our public safety sector to allow them to continue to protect all citizens of Nye County. Additionally, network stability enables the County to maintain web-based applications that our citizens rely on to communicate with and receive information from the County. This added security will help the IT department to meet all 7 program elements selected in question 3.

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

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

Nye County IT will obtain cost estimates for upgraded firewall appliance and subscription. In coordination with Nye County IT, Nye County DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants Administration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County DEM will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County Finance/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases.

Upon receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants Administration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT will install the firewall software. Upon completion of project, Finance/Grants Administration will submit close out financial reports and Nye County DEM will submit project close out report.

Quarterly Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye County Finance/Grants Administration.

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

The desired outcomes will be to enhance our web filtering capability thru inspection of SSL Secure web traffic, consolidate both devices into a single device adding the enhanced logging server that will enable us to review, analyze and retain both web and firewall traffic for post event auditing and correlation to help reduce our risk and help work together with other agencies by reviewing historic trend information relating to security events.

## 9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"

M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
\$2,963

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental

EHP r	re information on Yes	ed for ANY p	oroject that disn	พ? upts the environment or a structure, including small things like putting	g nails in walls. Please see the EHP Guidance attachment
11. Ri Cyber subm Thiss can re netwo and a starte Page: anony Stand admir Cyber	EQUIRED SERVICES carries and appro- cervice assesses accommend ways or k presence by d-hoc alerts. To d. Indicate in the https://www.cis/mous, annual s ards and Technolistered by the Misecurity Review Dur agency is alre	rastructure to val of a grathe "health is to enhance executing or register for e body of you.a.gov/topics.elf-assessmology Cyber MS-ISAC, du (NCSR) http. ady participa of yet signed	Security Agen  nt but is a pose  of your public  of your public  security in a  continuous scat  these service  our email that  skylober-threats  ent designed  security Fram  ring the first  os://www.cisecting in the Cybo	All SLCGP recipients and subrecipients are required to particicy (CISA). For these required services and memberships, please t-award requirementCyber Hygiene Services—Web Applications by checking for known vulner coordance with industry and government best practices and stins of public, static IPs for accessible services and vulnerabilities, email vulnerability_info@cisa.dhs.gov with the subject line for actions are requesting this service as part of the SLGCP. For more cand-advisories/cyber-hygiene-servicesNationwide Cybersector measure gaps and capabilities of a SLT's cybersecurity progression of the award/subaward period of performance and annual curity.org/ms-isac/services/ncsr (cisecurity.org).  For Hygiene Services and Nationwide Cybersecurity Review (NCSR), or the Hygiene Services or Nationwide Cybersecurity Review (NCSR), but the subject in the sub	se note that participation is not required for tion Scanning is an "internet scanning-as-a-service." rabilities and weak configurations. Additionally, CISA tandards. Vulnerability Scanning evaluates external less. This service provides weekly vulnerability reports "Requesting Cyber Hygiene Services – SLCGP" to get a information, visit CISA's Cyber Hygiene Information curity Review (NCSR)– The NCSR is a free, grams. It is based on the National Institute of Itheir subrecipients should complete the NCSR, ly. For more information, visit Nationwide either on our own or as a condition of FY 2022 SLCGP
	this project sca		any part of it	be reduced or expanded? Describe the ways in which the pro	ject can be reduced or expanded, or the reasons why
13. Pr	ovide the 5-digi	t zip code w	here the proj	of the logging server cannot be scaled down as removing any one cert will be executedrecipient address.	component would render the intent ineffective.
89060 14. Bu projec	uild or Sustain: S	Select "build	l" if this proje	et focuses on starting a new capability, or the intent of the proj s existing/current level.	ject is to close a capability gap. Select "sustain" if the
15. ls	this project sha t "Yes" if the proje ('es			her jurisdictions? tions (e.g., multiple cities). Select "No" if the project primarily suppor	rts a single entity.
Each .	selection should he Planning - Develop Information Drganization - Indi Equipment - Equip Fraining - Content	oment of policy vidual teams oment, supplicand methods son activities	mpanying item cies, plans, pro , an overall org es, and system s of delivery tha	ization, equipment, training, and exercise (POETE) elements for in the line item detail budget table on the next tab cedures, mutual aid agreements, strategies, and other publications; an anizational structure, and leadership at each level in the structure is that comply with relevant standards at comply with relevant training standards at knowledge of plans, allow members to improve their own performance.	also involves the collection and analysis of intelligence and
Line Item Det	ail Budget <u>top</u>				
PLANNING Planning Cost Name		Quantity		escribe how the purchase(s) within this element tie into the roject as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			\$		3
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
		0	0.00 \$		
			0.00		
	ATION COS	18		Describe househousehousefoly within this six	How would your organization sustain this
Organizational Cost Name	I Line Item Description	Quanti	ty Unit Cost	Total Describe how the purchase(s) within this element tie in project as described in the Application Questions secti	nroject if grant funding was reduced or

\$ The firewall upgrade, consolidation, and addition of the logging server Would not be necessary

5% M&A

M&A

2,963.0	2,963.00 cannot be scaled down as removing any one component would render the intent ineffective.
	\$ \$
	\$ \$
	\$ \$
	\$
	<b>\$</b> \$
	\$ \$
	\$
	<b>\$</b> \$
	<b>\$</b> \$
	<b>\$</b> \$
	\$
	\$ \$
	\$ \$
1 8	\$ \$
2,963.0	<b>00</b> 2,963.00

#### **EQUIPMENT COSTS**

EQUIPIV	IENI COST	3					
Equipment Cost Name	Line Item Qua Description	intity (	Jnit Cost To	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	AEL Number - Search - https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Firewall appliance	Firewall appliance	1 1	\$   <b>3,176.47</b> 13,176	\$ Update 6.47 current firewall	Seek alternate grant funding	Firewall, network	05NP-00-FWAL
Firewall advanced threat protection subscription	Firewall subscription	1 4	\$ <b>16,080.02</b> 46,080	\$ Provide .02 advanced threat protection, energize updates, instant replacement malware protection, advanced remote, insights subscriptions for 36 months	grant funding	Firewall, network	05NP-00-FWAL
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$ \$	\$			
			\$ \$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		2 5	\$ 59,256.49 59,256	\$ 5.49			

### 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?
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		

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

### Document Uploads $\underline{top}$

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	~	Nye County Audit Year Ending June 2021
Travel Policy	✓	Nye County Comprehensive Financial Management Policy
Payroll Policy	~	Nye County Personnel Policy Manual
Procurement Policy	~	Nye County Comprehensive Financial Management Policy
Milestones download template	✓	Nye County FY23 SLCGP Milestones
Capabilities Assessment download template	~	Nye County FY23 SLCGP Capabilities Assessment

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

Application ID: 448079

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems? Contact us at <u>Questions @ ZoomGrants com</u>
@2002-2023 Grant/hanlyst.com. All rights reserved.

"ZoomGrants' and the ZoomGrants logo are trademarks of Grant/Analyst.com, LLC.
Loout | Browser

	Applicant Name	Nye County DEM/IT
	Project Name:	CONTINGENCY Nye County Firewall Upgrade
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	BOCC Grant Acceptance	1 month after receipt of grant approval
2	Request Bids/Quotes	1 month after BOCC acceptance
3	Review bids/quotes and select vendor	1 month after requesting bids/quotes
4	DA Review contract	2 weeks after selecting vendor
5	BOCC or County Manager approve/accept contract	3 weeks after DA review
6	Issue Purchase Order	2 weeks after County acceptance of contract
7	IT Receive and install upgraded firewall	3 weeks after Purchase Order issuance
8	Pay Invoice	1 week after receipt & installation of software
9	Submit RFR/Close out grant	1 month after invoice payment
10		

<sup>\*</sup>Please add additional rows as necessary for your project



### FF

✓ No

Powered by ZoomGrants™ and		
Nevada Office of the Military, Division of Emergency Management		
FFY 2023 State and Local Cybersecurity Grant Program (SLO Deadline: 8/31/2023	CGP)	
State of	Nevada - Office of Cyber Defense Coordination	
00	CDC SLTT Resources Program	
lump to: Pre-Application	Application Questions Line Item Detail Budget Documen	t Unloade
oump to: <u>i re Application</u>	<u>Elife tiell betail budget</u>	t Opious
\$ 228,800.00 Requested	State of Nevada - Office of Cyber Defense Coordination	
Submitted: 8/31/2023 2:11:25 PM (Pacific)	EEE Weight West	Telephone 7754316360
Project Contact	555 Wright Way Carson City, NV 89711	Fax Web
Dianne Haigney	United States	EIN 866000022
dhaigney@ocdc.nv.gov		UEI MAZGIADTHWV7
Tel: 7754316360	Administrator	SAM Expires
A LIPPO and Company	Aakin Patel aakin.patel@ocdc.nv.gov	
Additional Contacts aakin.patel@ocdc.nv.gov,everettw@ocdc.nv.gov	addin.pater@ocac.nv.gov	
daminpator@oddc.inv.gov,ovorottiv@oddc.inv.gov		
Pre-Application <u>top</u>		
intrastate district, council of government, regional govern village, or other public entity, tribe, or authorized tribal of yes \square No  2. All funds granted under the State and Local Cyberseculaid in achieving this goal? (If not, the project is not eligible yes) yes \square No  3. In order for your application to be considered, you must of the grant. If you do not send representation to the requiver dates are to be determined and will be communicated yellow I understand and agree.  4. All procurement is required to be compliant with Nevad Per FEMA legal opinion, locals may not use NRS 332.115 must be free and open competition. Applicants are also renterprises, and labor surplus area firms per 2 C.F.R. Par provide a preference for the purchase, acquisition, or use procurement must be pre-approved in writing by the Diviy You may view FEMA's written legal opinion on NRS 332.115, and yellow y	organization.  Arity Grant Program must focus on managing and reducir on the for SLCGP funding).  Ast attend open meetings to testify in front of the Governouired meetings, your application will not be considered. As to SLCGP applicants as soon as the dates are known.  As Revised Statute (NRS) 333, PURCHASING: STATE and because it has been determined that NRS 332.115 is less to 200.321. All non-federal entities should also, to the great of goods, products, or materials produced in the United sion of Emergency Management (DEM) in advance of the along with DEM's procurement policy and FEMA's contract programs of the great of goods.	ng systemic cyber risk. Does your project proposal or's Cybersecurity Task Force. This is a requirement of the cybersecurity Task Force. The cybersecurity Task Force. The cyber
✓ I attest that funding for this project does not currently exis	st within our agency's budget	
<ol> <li>Entities applying as a subgrantee must meet a 20% cost requirement.</li> <li>I understand and agree.</li> </ol>	st share requirement for FY 2023 SLCGP. Please acknow	ledge your understanding and agreement of this
<ol> <li>Each jurisdiction must complete its own application. T issue a grant. Subgrantees may not pass through or subgrantees.</li> <li>I understand and agree.</li> </ol>		t of funds. Without an application, DEM is unable to
Application Questions top		
<ul> <li>1. Is this agency considered a rural area (an area encomp         If your agency is not considered a rural area, but your project to         benefit rural Nevadans.</li></ul>		r narrative what percentage of your project will directly

	re are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns. bjective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to  //bersecurity incidents and ensure continuity of operations.
	bjective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
_	bjective 3: Implement security protections commensurate with risk.
<b>✓</b> 0	bjective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	se select which of the SLCGP program elements your project addresses.
1. th	s may align with more than one element.  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 e information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the
_	anufacturer of the systems or technology.  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
O	, the state or local governments within the state.
	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 overnments within the state, against cybersecurity risks and cybersecurity threats.
c;	Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and bersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
	Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.  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
d	omain.
re	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 sponding to a cybersecurity incident.
c; a	Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the prescurity 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 aining.
	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 cident involving those communications or data networks.
	D. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of hich may impact the performance of information systems within the jurisdiction of the state.
_	<ol> <li>Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.</li> <li>Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)</li> </ol>
_	B. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and
	perational technology cybersecurity objectives.  4. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state
	nould be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
_	<ol> <li>Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.</li> <li>Distribute funds, items, services, capabilities, or activities to local governments.</li> </ol>
areas. commu Ve are	a shared area within the OCDC where training, education, outreach and technical threat analysis are available to all entities in our area of responsibility, including those in rural tallows those using the project become aware of risks and work on implementing security protections to counter them. Additionally, part of the aim of the project is to improve nication between entities to easily share information with each other in order to enhance the state's capabilities to react across the board to threats detected within an entity. 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 they choose to use it. We anticipate rural funding allocation to exceed 80%. The needs of the rural areas will drive our products direction.
his pr	does your project align with the objective selected in Question 2? oject will allow us to create a set of programs, tools, and projects to train and assist the staff of our SLTT partner entities in deploying their cybersecurity programs effectively p them develop a roadmap of what is needed, and how to proceed in addressing that roadmap.
By allo	does your project align with the program element(s) selected in Question 3? wing entities in our area of responsibility access to this project, we are enabling them to enhance the preparation, response, and resilience of information systems, tions, 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.
Descrii The pro	cribe, in detail, how, and by whom, the proposed project will be implemented.  be the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.  bject will be implemented by OCDC staff, in conjunction with contractor resources where needed. We will reach out for further expertise with a contractor when they are unable ne work internally.
he de	cribe, in a few sentences, the desired outcome(s) of your project.  sired outcome of this project would be the ability to assist all entities in our area of responsibility, including those in the rural areas, to work together in sharing information in the enhance the state's resources and capabilities to react across the board to threats detected, and have a good, centralized location with resources for cyberthreat training, on, outreach and technical threat analysis.
	agement & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you aining. If NO, enter "N/A"
	osts are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, the operational aspects of the grant)
nd Hi EHP re	es this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning storic Preservation (EHP) review?  Eviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for the project that the project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for the project that the project that disrupts the environment or a structure, including small things like putting nails in walls.
□ Y	
<b>✓</b> N	0
Cybers and ap	QUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the security and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission proval of a grant but is a post-award requirement. "Cyber Hygiene Services" Web Application Scanning is an "internet scanning-as-a-service." This service es the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can

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:

1		, , ,						_	(1100D) TI 1100	D : (
self-asse Cyberse	essment designed curity Framework	d to measure cand is spon	gaps and o sored by D	capabilities	of a SLT's MS-ISAC.	s cyberse . Entities	esNationwide Cybersecuri ecurity programs. It is based and their subrecipients shou lly. For more information, vis	on the Na	tional Institute of Sete the NCSR, adm	inistered by the MS-ISAC,
https://w	ww.cisecurity.org	g/ms-isac/serv	vices/ncsr	(cisecurity.	org).					
Our	agency is already	participating in	n the Cyber	Hygiene Se	ervices and	Nationwid	le Cybersecurity Review (NCSF	R), either or	n our own or as a co	ndition of FY 2022 SLCGP
	agency has not ye ect is awarded	et signed up fo	r the Cyber	Hygiene Se	ervices or N	ationwide	Cybersecurity Review (NCSR),	but unders	stands we will be red	quired to sign up for them if our
12. Is thi cannot.	is project scaleat	ole? Can any	part of it b	e reduced	or expand	ed? Desc	cribe the ways in which the p	oroject ca	n be reduced or ex	cpanded, or the reasons why it
	•	ays: If we expa	nded the pr	oject, we we	ould be able	e to do mo	ore training and outreach progra	ams. If we	reduced the project,	we would cut back on training ar
	ide the 5-digit zipect location could b									
<b>project s</b> <b>☑</b> Buil	strictly maintains						pability, or the intent of the p	oroject is t	to close a capabilit	y gap. Select "sustain" if the
☐ Sus	stain is project shareal	nle or denlova	able to oth	er jurisdict	ions?					
	es" if the project s					s). Select	"No" if the project primarily sup	pports a sir	ngle entity.	
□ NO										
Each sele	ection should have	an accompan	nying item ir	n the line ite	m detail bu	dget table				y sought for this project.  and analysis of intelligence and
info	rmation							10, 0100 1111	orved the delicotion	and analysis of intelligence and
	anization - Individu ipment - Equipme		•				ip at each level in the structure			
	ning - Content and		-							
✓ Exe	ercises - Hands-on	activities which					ers to improve their own perform	nance, and	d identify opportunitie	es to improve capabilities to
resp	oond to real events									
Line Item Detail	Budget top									
PLANNING (	COSTS									How would your organization
Planning Cost Name	Line Item Desc	ription		Quantity (	Unit Cost	Total	Describe how the purchase( into the project as described Questions section.			How would your organization sustain this project if grant funding was reduced or discontinued?
Cybersecurity Policy Resource Repository	Create and main templates that pa to build out their relevant to their	artner agencies cybersecurity	s can use	1 2	20,000.00 2	20,000.00	This will allow us to directly sustate of Nevada become better templates to help build their cy ensuring they are better protect attacks.	cyber awa	are by sharing policy y policies, thus	Work at finding alternate funding within our budget or via other grants.
						\$				
						\$				
						\$				
						\$				
						\$				
						\$				
						\$				
						\$				
						\$				
						\$				
						\$				
				1 2	20,000.00 2	\$ \$ \$				
					20,000.00 2	\$ \$ \$				
ORGANIZAT	TION COSTS			2	·	\$ \$	urobaco(a) within this start	44 610 link-		
ORGANIZAT Organizational Co		Quantity	Unit Cost	Z Total t	Describe ho	\$ \$ \$20,000.00	urchase(s) within this elemen ibed in the Application Ques			organization sustain this proje vas reduced or discontinued?
Organizational Co	ost Line Item Description	Quantity 1	\$	Total t	Describe he he project section.	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		tions hin our	if grant funding w	
Organizational Co	Description  Community	Quantity 1	\$ 10,000.00 \$	Total ti s \$ T 10,000.00 a	Describe he he project section.	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	ibed in the Application Ques each out to the communities wit	tions hin our	if grant funding we Work at finding alte	vas reduced or discontinued?
Organizational Co	Description  Community	Quantity 1	\$ 10,000.00 \$ \$	Total ti s \$ T 10,000.00 a	Describe he he project section.	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	ibed in the Application Ques each out to the communities wit	tions hin our	if grant funding we Work at finding alte	vas reduced or discontinued?
Organizational Co	Description  Community	Quantity 1	\$ 10,000.00 \$ \$	Total t \$ \$ T 10,000.00 a \$ \$	Describe he he project section.	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	ibed in the Application Ques each out to the communities wit	tions hin our	if grant funding we Work at finding alte	vas reduced or discontinued?
Organizational Co	Description  Community	Quantity 1	\$ 10,000.00 \$ \$	Total ti s \$ T 10,000.00 a	Describe he he project section.	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	ibed in the Application Ques each out to the communities wit	tions hin our	if grant funding we Work at finding alte	vas reduced or discontinued?

	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
1	\$	\$
	10,000.00	10,000.00

### **EQUIPMENT COSTS**

EQUIPME	ENT COS	13						
	Line Item Description	Quantity U	nit Cost	Total		organization sustain this project if grant funding was reduced	equipment-list to find AEL info	AEL Number - Search - https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Cybersecurity Lab	Hardware and software for performing malware testing, security assessments, and security evaluations of various tools in use by partner entities		\$ 1,000.00 84		This would be used to directly support deployment of the project with partner entities, and to provide hands on support for their technical needs to get the project online. This would include travel for the rural entities.	deployment of support projects.	Hardware, Computer, Integ	04HW-01-INHW
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
		1	\$	\$				
		84	,000.00 84					

### **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit Cost	Tota	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?	coordinate this training with the State Training Officer?
Training for Incident Responders	Training Vouchers	4	\$ 8,700.00		Would allow us to train our incident responders to better assist SLTT entities dealing with cybersecurity.	Either seek alternate sources of funding, or wait until the next legislative appropriation cycle. While waiting for additional funding, we would use contractor/consultant help, but not be able to have direct training.	No
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			

		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
4	1	\$	\$	0
	8,700.0	34,80	0.00	

### **EXERCISE COSTS**

EXERCI	SE COS13				
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 project if grant funding reduced or discontinued?	ng was exercise with the
Conference	Create a cyber conference for our partner entities throughout Nevada.	1	\$ 50,000.00 \$ 5	000.00 This will provide much needed networking and collaboration between the states partners with the our budget or via other gran ultimate goal of cyber entities within the state working together to create solutions and share expertise with on another.  Work at finding alternate fur our budget or via other gran funding could include charg and vendors for attending the	ts. This ing attendees
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
			\$	\$	
		1	\$ 50,000.00 \$ 5	000.00	0
Total		1 \$	\$ 50,000.00 \$50	000.00	0

#### Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	<u>A-133 FY 2021</u>
Travel Policy	~	State Travel Policy
		OCDC Travel Policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	~	Procurement Policy
Milestones	✓	Grant Milestones
download template		
Capabilities Assessment	~	<u>Capabilities Assessment</u>
download template		

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

Application ID: 449707

Become a [an of ZoomGrants\*\*\* on Facebook
Problems\* Contact us at Questions 87 ZoomGrants com
62002-2023 GrantAnalyst.com. All rights reserved.

"ZoomGrants\* and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Annlicant Name	Office of Cyber Defense Coordination
		·
		OCDC SLTT Resources Program
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Plan State Cyber Conference	Winter 2023 / Spring 2024
2	Purchase Hardware and Software for	
	Cybersecurity Lab	December 2023
3	Create Cybersecurity Policy Resource	
3	Repository	Spring 2024
4	Send OCDC Incident responders to Training	
	classes	Spring/Summer 2024
5	Schedule Community Outreach programs	January 2024
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

#### State of Nevada - Office of Cyber Defense Coordination 2023 OCDC Statewide SOC/SEIM/ISAC Program

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

	1		
<b>\$ 163,700.00</b> Requested	State of Nevada - Office of Cyber Defense Coordination		
Submitted: 8/31/2023 2:10:52 PM (Pacific)	555 Wright Way	Telephone Fax	7754316360
Project Contact	Carson City, NV 89711	Web	
Dianne Haigney	United States	EIN	866000022
dhaigney@ocdc.nv.gov		UEI	MAZGIADTHWV7
Tel: 7754316360	Administrator	SAM Expire	es
	Aakin Patel		
Additional Contacts	aakin.patel@ocdc.nv.gov		
aakin.patel@ocdc.nv.gov,everettw@ocdc.nv.gov			

#### Pre-App

olication <u>top</u>
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 o village, or other public entity, tribe, or authorized tribal organization.  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 Povised Statute (NDS) 222. DUDCHASING: STATE and/or NDS 222. DUDCHASING: LOCAL

GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the

. 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 20% cost share requirement for FY 2023 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.

#### 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 2023 SLCGP. Please select the objective with which your project most closely aligns.
<ul> <li>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.</li> </ul>
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.
<ul> <li>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.</li> </ul>
7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
16. Distribute funds, items, services, capabilities, or activities to local governments.
4. Describe your project in detail.  What would you like to do? Why? How does this project improve cybersecurity protection for your agency?  Create a shared technical threat analysis and alert management tool for use by all entities in the state of Nevada, including rural entities. This project will also serve as the functional base for the implementation of a shared statewide SEIM (Security Event and Incident Management) and SOC (Security Operations Center) once fully deployed. It allows entities making use of this tool to become aware of risks and work on implementing security protections to counter them. This project directly allows entities to manage, monitor and track their cybersecurity related activities on information technology systems, including legacy systems, deployed within entities that will participate. It will also be used to monitor network traffic and activity and allow for enhanced response and resilience through actively blocking traffic and activities that are detected and determined to be malicious. Additionally, part of the aim of the project is to allow entities to easily share 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 cyberthreat activity indicators. We are focusing our efforts entirely on what would most benefit 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.
All The distribution and raises and discount to oncoon by the first and raise and announced products discount.

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

By creating a shared technical threat analysis and alert management tool that will be used by all entities in the state of Nevada, including the rural entities, we are assisting 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. This will also allow smaller entities the ability to acquire much needed hardware and software that their current budgets do not allow.

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

By 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.

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

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

The project will be implemented by OCDC staff, in conjunction with contractor resources where needed. The OCDC currently has an Open Source Engineer on staff, who will be doing the bulk of the implementation and configuration for these tools. We will reach out for further expertise with a contractor when they are unable to do the work internally.

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

The desired outcome of this project would be the ability to assist all entities in the state of Nevada, including those in the rural areas, to 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 cyberthreat activity indicators.

## 9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"

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

N/A

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

EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance attachment for more information on EHP reviews.

Yes

Cyberse submiss This serican recc network and addistarted. Page: ht anonym Standard adminis Cyberse Out of the project of the	curity and Infrastructure ion and approval of a gravice assesses the "health ommend ways to enhance presence by executing once alerts. To register for Indicate in the body of y tips://www.cisa.gov/topicous, annual self-assessing and Technology Cybetered by the MS-ISAC, dicurity Review (NCSR) htt agency is already participated as a graph as not yet signed in multiple ways: Makerural/partner entities as we did to the 5-digit zip code went location could be different and or Sustain: Select "build ect strictly maintains a cold distain is project shareable or dives" if the project supports is see select all applicable prection should have an accompaning - Development of poll information lanization - Individual teams uppending - Content and method	Security Agant but is a paragraph of the security in continuous so these services are these services are the security in continuous so these services are the security Francisco and the security Francisco at the security Franci	ency (CISA). If ost-award recoblicly access accordance ocans of public ces, email vultat you are required to measure amework and it year of the accurity.org/m ober Hygiene Siber Hygien	For these quiremen ible web a with indu- try, static If nerability uesting the prices/cybo gaps and is sponso award/sul s-isac/sel ervices or If or expansions to specific prices or If or expansions to specific pri	applications by checking for known vulnastry and government best practices and vulnerability info@cisa.dhs.gov with the subject line his service as part of the SLGCP. For moer-hygiene-servicesNationwide Cyberset capabilities of a SLT's cybersecurity propered by DHS and the MS-ISAC. Entities an abaward period of performance and annuaryices/ncsr (cisecurity.org).  Ind Nationwide Cybersecurity Review (NCSR), but the MS-ISAC in the propered by DHS and the MS-ISAC. Entities an abaward period of performance and annuaryices/ncsr (cisecurity.org).  Ind Nationwide Cybersecurity Review (NCSR), but the propered development of the necessary tools. Subsets.  Indeed? Describe the ways in which the propered development of the necessary tools. Subsets.  Indeed:  It is a new capability, or the intent of the propered to the propered primarily support to the propered to the proper	ase note to ation Scaerabilities standards ties. This "Reques re informaceurity Regurants. It did their sually. For meither on out understandize or compared to the standards of	that participation is not required for anning is an "internet scanning-as-a-service." is and weak configurations. Additionally, CISA is. Vulnerability Scanning evaluates external eservice provides weekly vulnerability reports string Cyber Hygiene Services – SLCGP" to get ation, visit CISA's Cyber Hygiene Information eview (NCSR). The NCSR is a free, is based on the National Institute of abrecipients should complete the NCSR, more information, visit Nationwide our own or as a condition of FY 2022 SLCGP trands we will be required to sign up for them if our be reduced or expanded, or the reasons empletely cover hardware/software licensing or close a capability gap. Select "sustain" if
Line Item Detai	l Budget <u>top</u>						
PLANNING ( Planning Cost Li	ine Item	Unit	Describe hov	w the pur	chase(s) within this element tie into the	How wo	ould your organization sustain this project if
_	escription Quantity	Cost Total			n the Application Questions section.		nding was reduced or discontinued?
		\$					
		\$					
		\$					
		\$					
		\$					
		\$ \$					
		\$					
		\$					
		\$					
		\$ \$					
	0	0.00 \$					
		0.00					
ORGANIZAT	TION COSTS						
Organizational Cost Name	Line Item Description	Quantit	y Unit Cost	Total t	Describe how the purchase(s) within this ie into the project as described in the Ap Questions section.		How would your organization sustain this project if grant funding was reduced or discontinued?
Direct Support for Partner Entities	Working with all state entities, including rural, t ensure smoother	1	\$ 20,000.00 2	0,000.00 <b>t</b>	Would be used to directly support the deploy he project with partner entities and provide has support for the technical needs required to ge	ands on	Work at finding alternative funding within our budget and request partner entities to assist in financially.

**✓** No

	deployments of support projects.				project online. This would include travel to relevant rural entities for direct support.	
Contractor / Consulting Services	Support and consulting	1	\$ 47,400.00		Will provide the specialty expertise needed to get most of the objectives implemented and guide our in-house staff through the process so they can sustain the project going forward.	Seek alternative sources of funding or wait until the next legislative appropriation cycle. We'd have to work without direct training, but with contractor/consultant help.
Cyber Partner Outreach	Cyber outreach with our partner agencies throughout the state including rural entities.	1	\$ 7,500.00		Allow us to start outreach programs so entities throughout the state so they are aware of our support and service. Provide easy-to-use data/threat sharing mechanisms all partners will have access to.	Find alternate funding within our budget or via other grants.
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		3	\$	\$		
			74,900.00	74,900.00		

### **EQUIPMENT COSTS**

	t Line Item Description Quantity	Unit Cost Tot	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	organization sustain this project if grant funding was reduced	equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Hardware Servers	Servers to 1 run log analysis and collection tools.	\$ 18,000.00 18,000.0		cycle.	Hardware, Computer, Integ	04HW01-1NHW
Software Licensing	Software 6 Licenses	\$ 6,000.00 36,000.0	This of software is key to our log collection and threat analysis portions of the project.	Use the opensource, unsupported version at first and then request legislative appropriations in the next cycle.	System, Security, Informa	05NP00-SIEM
			\$			
			\$			
		·	\$ \$			
		·	\$			
			\$ \$			
		·	\$			
		\$	\$			
		\$	\$			
		·	\$			
			\$			
		·	\$			
	7	\$ 24,000.00 54,000.0	0			

### **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
Training for SOC / SEIM	Training Vouchers	4	\$ 8,700.00 3	\$ Would allow us to create useful 44,800.00 threat sharing intelligence to	Either seek alternate sources of funding, or wait until the next legislative appropriation cycle. While waiting for	No

Analysts			distribute amongst our partner entities throughout the state.	additional funding, we would use contractor/consultant help, but not be able to have direct training.
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
	4	\$	\$	0
	8	,700.00 34,80	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	0.00			0
Total		0	\$ 0.00				0

### Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required?	Attached Documents * A-133 FY 2021
Travel Policy	✓	State Travel Policy  OCDC Travel Policy
Payroll Policy	<b>✓</b>	DPS Payroll Policy
Procurement Policy	<b>✓</b>	Procurement Policy
Milestones download template	✓	Grant Milestones
Capabilities Assessment download template	✓	<u>Capabilities Assessment</u>

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

Application ID: 449706

Become a fan of Zoom/Grants™ on Facebook
Problems? Contact us at Questions® Zoom/Grants.com
@2002-2023 Grant/Analyst.com. All rights reserved.
"Zoom/Grants" and the Zoom/Grants logo are trademarks of Grant/Analyst.com, LLC.

ı	Applicant Name	Office of Cyber Defense Coordination
	Project Name:	2023 OCDC Statewide SOC-SEIM/ISAC Program
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Hire contractor/consulting firm	Winter 2023
2	Purchase Hardware servers and Software	
	Licenses	Summer 2024
3	Schedule and plan outreach programs	Spring 2024
4	Schedule deployment for partner entities	Summer/Fall 2024
5	Schedule training for SOC/SEIM Analysts	Summer 2024
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

#### State of Nevada - Office of Cyber Defense Coordination **OCDC Support Staff Kickstart**

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

\$	51	0,0	000.	.00	Req	uested
----	----	-----	------	-----	-----	--------

Submitted: 8/31/2023 2:10:14 PM (Pacific)

#### **Project Contact**

Dianne Haigney dhaigney@ocdc.nv.gov Tel: 7754316360

#### **Additional Contacts**

aakin.patel@ocdc.nv.gov,everettw@ocdc.nv.gov

#### State of Nevada - Office of Cyber Defense Coordination

555 Wright Way Carson City, NV 89711 **United States** 

#### Administrator

Aakin Patel aakin.patel@ocdc.nv.gov Telephone 7754316360

Fax Web

866000022

EIN UEI MAZGIADTHWV7

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, specia
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.

Yes

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. 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 20% cost share requirement for FY 2023 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.

olicati	on Questions <u>top</u>
l	. Is this agency considered a rural area (an area encompassing a population of less than 50,000 people)?  f 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 be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage of your project will be provided by the select "No" and indicate in your narrative what percentage is not your project will be provided by the select "No" and indicate in your narrative what percentage is not your project will be provided by the select "No" and indicate in your narrative what percentage is not your project will be provided by the select "No" and your project will be provided by the
	Yes
	▼ No
2	. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
	<ul> <li>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.</li> </ul>
	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.
	. Please select which of the SLCGP program elements your project addresses. Projects may align with more than one element.
	■ 1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
	2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
	3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
	4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
	5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
	6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
	7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
	8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
	9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
	10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
	11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
	12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
	13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
	14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
	▼ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
	16. Distribute funds, items, services, capabilities, or activities to local governments.
V C S tl	Describe your project in detail.  What would you like to do? Why? How does this project improve cybersecurity protection for your agency?  Create an Incident Response Team comprised of an IT Manager, Forensic/Malware Engineer and a Security Resource Analyst. This team will be available to assist all SLTT partners in the state of Nevada, including the rural entities. This project will serve as the functional base for assisting these SLTT partners in the event of a cyber protection and activity protections to counter these threats and attacks. It 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 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 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, 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?

By creating an Incident Response Team that will be available to assist all entities in the state of Nevada, including the rural entities, we will be able 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. This will also allow smaller entities, with limited budgets, the ability to receive much needed 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?

By 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. 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 hire appropriate staffing and create an Incident Response Team comprised of an IT Manager, Forensic/Malware Engineer and a Security Resource Analyst.

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

The desired outcome of this project would be the ability to assist all entities in the state of Nevada when they are in need of assistance due to a cyber threat and/or attack. The project will also assist the state's partner agencies, including those in the rural areas, to 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 cyberthreat activity indicators.

				aspects of the grant		a consequence or the grant (i.e., financial management,
Envir EHP	onmental Plann reviews are requi	ing and Hist red for ANY	toric Preservation project that disrupts	(EHP) review?	,	sting structure which would necessitate an gs like putting nails in walls. Please see the EHP Guidance
attacr	nment for more in Yes	tormation on	EHP reviews.			
~						
the C for su as-a-s config Vulne vulne with t as pa hygie capali spons award https	ybersecurity an ubmission and a service." This segurations. Additerability Scannirerabilities. This ethe subject line art of the SLGCP ene-servicesNoilities of a SLT sored by DHS and subaward peric!//www.cisecurit	d Infrastruct pproval of a ervice assess tionally, CIS. ng evaluates service prov "Requesting. For more i ationwide C 's cybersect' so do ferfor ty.org/ms-isa	ture Security Age grant but is a po ses the "health" of A can recommend external network ides weekly vulnig Cyber Hygiene information, visit ybersecurity Revurity programs. It IAC. Entities and mance and annuac/services/ncsr (of	ncy (CISA). For these st-award requirement your publicly acc if ways to enhance so presence by executability reports and services – SLCGP" CISA's Cyber Hygie ew (NCSR) The Notes based on the Natheir subrecipients ally. For more infor isecurity.org).	se required services and mentCyber Hygiene Services essible web applications by security in accordance with iting continuous scans of put ad-hoc alerts. To register fot oget started. Indicate in the ne Information Page: https://CSR is a free, anonymous, ai onal Institute of Standards a should complete the NCSR, mation, visit Nationwide Cybra strices.	red to participate in a limited number of free services by mberships, please note that participation is not required so.—Web Application Scanning is an "internet scanning-checking for known vulnerabilities and weak ndustry and government best practices and standards. blic, static IPs for accessible services and or these services, email vulnerability_info@cisa.dhs.go be body of your email that you are requesting this servic (www.cisa.gov/topics/cyber-threats-and-advisories/cybernual self-assessment designed to measure gaps and and Technology Cybersecurity Framework and is administered by the MS-ISAC, during the first year of the presecurity Review (NCSR).
:	SLCGP		,			
	Our agency has r them if our projec		up for the Cyber H	lygiene Services or N	ationwide Cybersecurity Review	v (NCSR), but understands we will be required to sign up for
	• •		n any part of it be	reduced or expand	led? Describe the ways in w	hich the project can be reduced or expanded, or the
	ons why it cannot an scale by expar		cing the number of	staffing hired and the	positions needed based on the	e needs of our partner entities.
	project location co	•	where the project ent than the sub-re	will be executed. cipient address.		
<b>✓</b>	<b>ain" if the proje</b> Build Sustain	ct strictly m	aintains a core ca	pability at its existi	ng/current level.	
	t "Yes" if the proj		eployable to othe multiple jurisdictio	•	s). Select "No" if the project pri	imarily supports a single entity.
	No					
proje	ct.		<b>.</b> .			) elements for which funding is being sought for this
		pment of pol			edget table on the next tab eements, strategies, and other	publications; also involves the collection and analysis of
	o .		s, an overall organi	zational structure, and	I leadership at each level in the	structure
_				nat comply with relev		
	<del>-</del>			mply with relevant tra	=	
	Exercises - Hand capabilities to res			owledge of plans, all	ow members to improve their o	wn performance, and identify opportunities to improve
tem De	etail Budget <i>to</i>	n				
nom bo	tun Buuget <u>to</u>	<u> </u>				
NINN	G COSTS		D.	ulha hamati	and a within this of our of the	into
ing Cos	t Line Item Description	Quantity		roject as described	ase(s) within this element tie in the Application Question	
			\$			
			\$			
			\$			
			\$			
			\$			
			\$			
			Φ			

\$

amount you are retaining. If NO, enter "N/A"

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

### **ORGANIZATION COSTS**

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Tota	described in the Application Questions sustain this pro-	ur organization oject if grant funding r discontinued?			
New Hires	Staffing to support SLTT entities and create an incident response team. Team will be an IT Manager, Forensics/Malware Engineer and a Security Resource Analyst	3	\$ 170,000.00 510		By creating an Incident Response Team we We would either can support our SLTT partners within the sources of fundi state of Nevada, to include the rural entities. legislative approwers we can provide immediate assistance when the meantime, we any entity is experiencing a cyber threat or attack.	ng or wait until the next priations cycle and in ve would work within			
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
			\$	\$					
		3	\$	\$					
	<b>170,000.00</b> 510,000.00								

### **EQUIPMENT COSTS**

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

### **TRAINING COSTS**

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

\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
Ф	<b>5</b>	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
\$	\$	
0 \$	\$	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 this project if grant funding was 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
Total			¢ 0 00	0.00		^
Total		U	\$ 0.00	\$U.UU		0

# Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	<u>A-133 FY 2021</u>
Travel Policy	✓	OCDC Travel Policy
		State Travel Policy
Payroll Policy	✓	Payroll Policy
Procurement Policy	✓	Procurement Policy
Milestones	✓	Grant Milestones
download template		
Capabilities Assessment download template	<b>✓</b>	Capabilities Assessment

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

Application ID: 446168

Become a fan of ZoomGrants<sup>13</sup> on Facebook
Problems? Contact us at Questions @ ZoomGrants com
@2002-2023 Grant/harlyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	Office of Cyber Defense Coordination
	Project Name:	OCDC Support Staff Kickstart
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Work with Human Resources to develop	
1	recruitment plan	Winter 2023
2	Hiring Round 1	January 2024
3	Hiring Round 2	March 2024
4	Hiring Round 3	May 2024
5		
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

# Truckee Meadows Water Authority Field Site Network Resiliency & Monitoring

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

\$ 112,353.62 Requested

Submitted: 8/31/2023 2:35:24 PM (Pacific)

Project Contact
Chris Briscoe
cbriscoe@tmwa.com

cbriscoe@tmwa.com Tel: 775-834-8082

**Additional Contacts** 

none entered

**Truckee Meadows Water Authority** 

1355 Capital Blvd Reno

Reno, NV, USA, NV 89502 United States

**Chief Financial Officer** 

Matt Bowman mbowman@tmwa.com Telephone 17758348080

Fax

Web tmwa.com EIN 88 0488450 UEI QC3VDC781ZN5

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.	

✓ Yes

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. 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 20% cost share requirement for FY 2023 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.

#### 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 2023 SLCGP. Please select the objective with which your project most closely aligns.
Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
Objective 3: Implement security protections commensurate with risk.
Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
3. Please select which of the SLCGP program elements your project addresses.  Projects may align with more than one element.
1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Distribute funds, items, services, capabilities, or activities to local governments.
4. Describe your project in detail.  What would you like to do? Why? How does this project improve cybersecurity protection for your agency?

TMWA recently purchased Palo Alto firewalls for our network edge, and the need for additional network resiliency at our field sites has been known. TMWA has tried to resolve issues with various carriers and gateways, but the cost of maintaining multiple private circuits is prohibitive.

Our new strategy is to adopt SD-WAN and Site-to-Site VPNs at our field sites, running atop commodity business internet connections. This strategy requires placing firewall hardware at each site to terminate the connections, as well as centralized management licensing for accessing SD-WAN features.

The goals of this projects are:

- Increase reliability/availability of cyber-physical security monitoring at TMWA's remote field sites
- Increase visibility of network traffic at remote field sites
- Increase fault tolerance for site to site and Internet access business connectivity

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

This project aligns with objective 3 as by implementing firewalls at our field sites would enable us to have secure reliable connections. These sites contain physical security cameras which allow our security team and operations personnel to monitor the security and operations of our critical infrastructure.

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

- 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.
- With the proposed project we would be able to implement SD-WAN and monitor network traffic reliably at these sites. We would also have better traffic visibility with centralized firewall logging of the remote firewalls to the server.
- 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
- -Deploying this solution would enable us to protect data while in transit with encryption for these site-to-site tunnels. TMWA would also be adopting best practices like multi-factor authentication for firewall administration, as these new devices would be integrated and configured with our current multi-factor platform and tools. This would also help harden remote parts of our infrastructure via a next-generation firewall platform, able of more robust network protection.
- 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.
- -Presently, these sites often lose connection, resulting in no physical or IT monitoring. This project would remedy that. The proposed solution would let TMWA leverage multiple and varied types of connectivity circuits to provide redundancy and better performance between these remote sites and our main office locations.

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

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

Staff will physically install the firewalls and WAN switches by placing the devices into pre-existing network racks or cabinets and plugging the devices into power. No contracted labor is expected. Staff will connect to the devices and configure them before enabling the network connections. Staff will leverage existing expertise and knowledge of the concepts and platforms that will be installed and configured, along with vendor documentation and CIS benchmark documentation for supplemental support/reference.

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

- Increase reliability/availability of cyber-physical security monitoring at TMWA's remote field sites
- Increase visibility of network traffic at remote field site
- Increase fault tolerance for site to site and Internet access business connectivity

9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"

ove	rsight of those involved in the			onsequence of the grant (i.e., financial management, reporting,
N/A		ow construction, renovation	a retrofitting or modifications of an existing	g structure which would necessitate an Environmental Planning
and EH	Historic Preservation (EHP) reviews are required for ANY	') review? Y project that disrupts the env		ike putting nails in walls. Please see the EHP Guidance attachment for
	e information on EHP reviews. Yes			
<b>✓</b>	No			
Cyl and ass rec pre aled Ind http self Cyl dur	ersecurity and Infrastructur approval of a grant but is a sases the "health" of your pommend ways to enhance some by executing continuts. To register for these ser cate in the body of your ems://www.cisa.gov/topics/cyk-assessment designed to mersecurity Framework and ing the first year of the awais://www.cisecurity.org/ms-isOur agency is already partici	re Security Agency (CISA). In post-award requirement. Sublicly accessible web appaceurity in accordance with sous scans of public, static vices, email vulnerability_intention and that you are requesting per-threats-and-advisories/ceasure gaps and capabilities is sponsored by DHS and the order of performing in the Cyber Hygiene Statistics of the content of the cyber Hygiene Statistics of the cyber Hygiene Statis	For these required services and membership—Cyber Hygiene Services—Web Application blications by checking for known vulnerabiliting industry and government best practices ar IPs for accessible services and vulnerabilitinfo@cisa.dhs.gov with the subject line "Recthis service as part of the SLGCP. For more cyber-hygiene-services.—Nationwide Cybers so of a SLT's cybersecurity programs. It is the MS-ISAC. Entities and their subrecipients formance and annually. For more informatic y.org).  Services and Nationwide Cybersecurity Review (	to participate in a limited number of free services by the ps, please note that participation is not required for submission in Scanning is an "internet scanning-as-a-service." This service lities and weak configurations. Additionally, CISA can not standards. Vulnerability Scanning evaluates external network it is service provides weekly vulnerability reports and ad-hoc questing Cyber Hygiene Services – SLCGP" to get started. The information, visit CISA's Cyber Hygiene Information Page: security Review (NCSR) The NCSR is a free, anonymous, annual passed on the National Institute of Standards and Technology is should complete the NCSR, administered by the MS-ISAC, on, visit Nationwide Cybersecurity Review (NCSR)  (NCSR), either on our own or as a condition of FY 2022 SLCGP (ICSR), but understands we will be required to sign up for them if our
12.	. ,	an any part of it be reduce	d or expanded? Describe the ways in which	n the project can be reduced or expanded, or the reasons why it
<b>can</b> The	not. current scope of this project is	s all of our field sites that curr		our remote sites may eventually have physical security cameras. The
13.	Provide the 5-digit zip code project location could be diffe	where the project will be	executed.	ouviy.
15. Sel	ject strictly maintains a core Build Sustain  Is this project shareable or eact "Yes" if the project support Yes No  Please select all applicable th selection should have an acc Planning - Development of p information Organization - Individual tear Equipment - Equipment, sup Training - Content and metho	deployable to other jurisdicts multiple jurisdictions (e.g., planning, organization, equecompanying item in the line is colicies, plans, procedures, mums, an overall organizational supplies, and systems that composed of delivery that comply with	current level.  ctions? multiple cities). Select "No" if the project primare tem detail budget table on the next tab utual aid agreements, strategies, and other publications and leadership at each level in the structure, and leadership at each level in the structure in the stru	ements for which funding is being sought for this project.  lications; also involves the collection and analysis of intelligence and
I ANNIN	IG COSTS			
	st Line Item Quantity Description		ow the purchase(s) within this element tie in lescribed in the Application Questions section	
		\$		
		\$ \$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		\$		
		<u>(</u>		
		\$		
		\$		
	0	\$		

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

# **EQUIPMENT COSTS**

EQUIPIN	ENT COS	13						
Equipment Cost Name		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?	equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized equipment-list to find AEL info
and components	Network switches with transceivers, power supplies, and cords	2	\$ 20,987.85		To facilitate	Would need to attempt to add to next FY capital budget cycle, if funds were available.	Hardware, Computer, Integ	04HW-01-INHW
	Licensing and Support for WAN Switches	2	\$ 6,117.83	\$ 12,235.66	Provides support in case of hardware failure or configuration assistance and centralized management.	attempt to add to next FY budget cycle, if funds were available.	Software, Network	04SW-04-NETW
Rugged Next Gen Firewalls	Remote Firewall for field sites	8	\$ 1,541.62		Firewall to connect to internet providing secure reliable access.	Would need to attempt to add to next FY capital budget cycle, if funds were available.	Firewall, Network	05NP-00-FWAL
Advanced URL Filtering	Subscription for firewall feature	8	\$ 723.87		Allows for advanced firewall feature to ensure URL's are safe	Would need to attempt to add to next FY capital budget cycle, if funds were available.	Software, Malware/Anti-vi	05HS-00-MALW
subscription	Subscription for firewall feature	8	\$ 419.01		Allows for software defined WAN connectivity	attempt to add	Software, Network	04SW-04-NETW
	Subscription for support	8	\$ 559.21		Allows for access to	. Would need to attempt to	Firewall, Network	05NP-00-FWAL

Support				technical support	add to next FY capital budget cycle, if funds were available.		
NGFW Malware Subscription	Subscription to prevent malware	8	\$ 419.01	\$ Malware 3,352.08 prevention	Would need to attempt to add to next FY capital budget cycle, if funds were available.	Software, Malware/Anti-vi	05HS-00-MALW
NGFW Central Managemen Software	Central Management t software	1	\$ 5,499.51	\$ Allows for 5,499.51 field firewalls to be centrally managed		System,Patch/Configuratio	005PM-00-PTCH
NGFW Central Managemen Support	Support for central t management software	1	\$ 1,810.77	\$ Support for 1,810.77 central management of firewalls	attempt to add	System,Patch/Configuratio	005PM-00-PTCH
SD-WAN Sub for exisiting NGFW	Subscription for pre- existing firewall to be SD-WAN capable	2	\$ 7,746.83	\$ Existing 15,493.66 firewall does not have SD- WAN feature.	attempt to add	Software,Network	04SW-00-PTCH
NGFW Advanced Threat Prevention	Subscription for firewall feature	8	\$ 754.27	\$ Allows for 6,034.16 threat prevention	Would need to attempt to add to next FY capital budget cycle, if funds were available.	Software, Malware/Anti-vi	05HS-00-MALW
			\$	\$			
			\$	\$			
			\$	\$			
		56	\$	\$			
			46,579.78	112,351.22			

# TRAINING COSTS

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

# **EXERCISE COSTS**

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

	•	
	\$ \$	
	\$ \$	
	\$ \$	
	\$ \$	
	\$ \$	
	\$ \$	
	0 \$ 0.00 \$	0
	<b>0 \$ 0.00</b> \$ 0.00	v
Total	0 \$ 0.00 \$0.00	0

# Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required?	Attached Documents *  TMWA ACFR (includes single audit)
Travel Policy	~	Travel Policy Document
Payroll Policy	✓	TMWA Payroll Memo
Procurement Policy	~	TMWA Disbursement Policy
Milestones download template	✓	Grant Milestone Descriptions and Timeframes Milestones - edit
Capabilities Assessment download template	✓	Capabilities Assessment Capabilities Assessment edit

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

Application ID: 449672

Become a fan of ZoomGrants<sup>111</sup> on Facebook
Problems? Contact us at <u>Questions ® ZoomGrants com</u>
@2002-2023 GrantAnalyst.com. All rights reserved.

"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

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

	Applicant Name	Truckee Meadows Water Authority
	Project Name	Field Site Network Resiliency & Monitoring
	Project Funding Stream	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1 Physical I	nstallation of WAN Switches at Headquarter location	4 weeks after receiving equipment
2 Configura	ation on new switches completed	6 weeks after receiving equipment
4 Multiple	DIA and private circuit ISP handoff connections moved over to new switches	10 Weeks after receiving equipment
4 Deploym	ent of the NGFW Managment VM and initial configuration	2 months after receiving License for VM
5 Initial cor	nfiguration of feild site firewalls - prepped centrally at main office	4 months after receiving Licensing and firewalls
6 Deploym	ent and integration of new firewalls at 2 out of the 8 remote sites	6 months after receiving Licensing and firewalls
7 Deploym	ent and integration of new firewalls at 4 out of the 8 remote sites	8 months after receiving Licensing and firewalls
8 Deploym	ent and integration of new firewalls at 6 out of the 8 remote sites	10 months after receiving Licensing and firewalls
9 Deploym	ent and integration of new firewalls at 8 out of the 8 remote sites	12 months after receiving Licensing and firewalls



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

# Washoe County School District CONTINGENT WCSD Account and File Auditing Software License

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

#### \$ 6,850.00 Requested

Submitted: 8/28/2023 10:33:22 AM (Pacific)

## **Project Contact**

Randy Drake

austin.smith@washoeschools.net

Tel: 7757894617

#### **Additional Contacts**

lohlin@washoeschools.net, radrake@washoeschools.net

#### **Washoe County School District**

425 E 9th St Reno, NV 89512 United States

## **Director of Grants**

Lauren Ohlin

lohlin@washoeschools.net

Telephone 7757893435 Fax 775-333-5012

Web www.washoeschools.net

EIN 8860000919 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.

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. 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 20% cost share requirement for FY 2023 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.

## Application Questions top

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

directly ben	efit rural Nevadans.
Yes	
✓ No	
2. There ar	e four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
Object	tive 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to
respor	nd to cybersecurity incidents and ensure continuity of operations.
Object	tive 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
Object	tive 3: Implement security protections commensurate with risk.
Object	tive 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	elect which of the SLCGP program elements your project addresses.
	ay align with more than one element.
	nage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the
	and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer
	rted by the manufacturer of the systems or technology.
	nitor, 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
	of, the state or local governments within the state.
	nance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local naments within the state, against cybersecurity risks and cybersecurity threats.
	lement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks
	hement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices promitted by degree of risk to address cybersecurity risks /bersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
	sure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
_	
	mote 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 et domain.
7. Ens	sure 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
respor	nding to a cybersecurity incident.
	the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the
	security workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge,
,	and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through
•	security hygiene training.
	sures 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
	nt involving those communications or data networks.
	sess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the dation of which may impact the performance of information systems within the jurisdiction of the state.
	pation of which may impact the penormatice of information systems within the jurisdiction of the state.  The state is the state of the
	verage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
	plement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology perational technology cybersecurity objectives.
14. De	evelop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state
	be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
🗌 15. Er	sure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
☐ 16. Di	stribute funds, items, services, capabilities, or activities to local governments.
	e your project in detail.
What would	I you like to do? Why? How does this project improve cybersecurity protection for your agency?

This project will provide licensing for account and file auditing software that Washoe County School District (WCSD) will use to identify anomalous activities occurring on the network. The cost will include license and support for one year. Account management and auditing solutions are important because they supplement the native logging features in information systems. This will improve WCSD's capability to protect accounts based on risk, as well as allow WCSD 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 WCSD. WCSD is a large, geographically-dispersed public entity. However, WCSD's IT department is relatively small with technicians who must support many schools at the same time. Because of this limitations and frequent movement of personnel, the IT department struggles to audit and monitor accounts and files on key shared resources. This software will improve WCSD's capability to detect and respond to anomalous events. It is critical to provide a safe and secure learning environment for WCSD's 62,000 students, including those in rural areas of Washoe County. This project will allow IT staff to monitor and audit user accounts and enable staff to identify systemic issues and weaknesses in the the monitoring systems.

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

Objective 3: "Implement security protections commensurate with risk." This project helps audit and monitor user accounts and file servers which are frequent targets for bad actors and malicious insiders. Maintaining enhanced oversight of these critical resources could prevent a breach or allow a breach to be investigated long after operating system logs are overwritten on the system.

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

- 1. "Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology." This system will manage, monitor, and track information systems and user accounts to ensure that they are not under attack by a
- 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 monitor, audit, and track key resources in the environment to identify known or suspected breaches.
- 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 monitor and detect potential breaches on key systems. This will improve WCSD's ability to respond to breaches by improving visibility in the system.

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

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

This project will be implemented by internal IT department staff. The IT department already have additional hardware resources that can support this implementation and fielding is covered under the enterprise support licensing. This project involves receiving the license, provisioning computing resources, installing the software, and configuring permissions to audit the environment. Most of these actions can be performed by internal staff using support documentation provided by the vendor.

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

Implement enhanced account and file share monitoring and auditing including activities and membership to privileged groups.

#### 9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"

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

F	Planning and Historic	c Preservati	construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental n (EHP) review?  To ject that disrupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance	
á	attachment for more in  Yes			
	✓ No			
S S S S V V H V S S S S S S S S S S S S	cybersecurity and Insubmission and appriervice." This service. Additionally, CISA candidates external neweekly vulnerability dygiene Services – Sisit CISA's Cyber Hy Review (NCSR).— The wased on the National subrecipients should note information, visual course.	frastructure roval of a grae assesses the assesses the twork preserports and SLCGP" to grae linear Information NCSR is a fall Institute of a complete the sit Nationwice ady participal code of the sit Nationwice and participal roval of a graef participal code of the sit Nationwice and participal roval	EMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Security Agency (CISA). For these required services and memberships, please note that participation is not required for the but is a post-award requirement. "Cyber Hygiene Services-" Web Application Scanning is an "internet scanning-as-a-e" (health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. It is dead to enhance security in accordance with industry and government best practices and standards. Vulnerability Scannice by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides defined hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber t started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information ation Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity ee, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their exposed and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their exposed by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For exposed cybersecurity Review (NCSR), https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).	nning r on, s or
	our project is awa	arded		
	2. Is this project sca why it cannot.	aleable? Car	any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasor	ns
			pport additional information systems, but licensing typically covers a set amount of systems. The project allows IT staff to monitor and . The scope could expand or contract if we drastically increase or decrease our resource usage.	į
7	•	•	here the project will be executed.  In than the sub-recipient address.	
t			" if this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustain re capability at its existing/current level.	ı" if
3			ployable to other jurisdictions? nultiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.	
	Each selection should Planning - Develor and information	have an accomposition	anning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project in the line item detail budget table on the next tab item. Procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelliger an overall organizational structure, and leadership at each level in the structure	
	The second secon		es, and systems that comply with relevant standards	
	•	ls-on activities	of delivery that comply with relevant training standards which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities	s to
Line Item	n Detail Budget <u>tor</u>	2		
PLANN	IING COSTS			
Planning Name	Cost Line Item  Description	Quantity	Unit Total Describe how the purchase(s) within this element tie into the Cost Total project as described in the Application Questions section. How would your organization sustain this project grant funding was reduced or discontinued?	ct if
			\$ \$	
			\$	
			\$	
			\$	
			\$	
			\$	
			\$ \$	
			\$	
			\$	
		0	0.00 \$ 0.00	

Orgai Name		nal Cost Line Item Description	Quanti		ost Total th		e purchase(s) within this element tie into escribed in the Application Questions	How would your organization sustain this project if grant funding was reduced or discontinued?
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$			
					\$ \$ \$ \$			
					\$ \$			
			(	0 \$ 0.				
					0.00			
EQL	JIPM	ENT COSTS			Describe			
					how the	How would		
					purchase(s)	your		
					within this element tie	organization	AEI Nama Ca	AEI Nombre C
Equip	ment	Line Item Quantity	Unit	Total	into the	sustain this project if	AEL Name - Search https://www.fema.gov/grants/tools/authori	AEL Number - Search zed- https://www.fema.gov/grants/tools/authorized-
Cost	Name	Description Quantity	Cost		project as described	grant funding	equipment-list to find AEL info	equipment-list to find AEL info
					in the	was reduced		
					Application	or discontinued?	•	
					Questions section.			
Direct	orv	Software 1	\$		This	WCSD will	Software, Risk Management	04AP-04-RISK
Auditi			2,860.00 2,8			sustain this	John Ward, Nisk Warlagement	OHAI OH KIOK
Softwa		directory			will enhance			
Licens		services auditing			WCSD's monitoring	incorporating this cost into		
30030	inplion	additing				the ongoing		
					capabilities.	operating		
					The native	budget.		
					logging capabilities			
					of windows			
					operating			
					systems are very limited	•		
					and this			
					software will			
					allow for			
					significantly improved			
					visibility and			
					log			
					retention. These are			
					critical to			
					responding			
					to and investigating			
					investigating cyber			
					attacks.			
Cloud		Software 1	\$		This	WCSD will	Software, Risk Management	04AP-04-RISK
Direct		licensing for cloud	995.00			sustain this		
Auditi		cioua directory			will enhance WCSD's	incorporating		
Licens		services			monitoring			
		auditing				the ongoing		
					capabilities. The native			
					logging	Juuget.		
					capabilities			
					of windows			
					operating systems are			
					very limited			
					and this			
					software will			
					allow for significantly			
					improved			
					visibility and log			

File Directory Auditing Software	Software licensing for file server auditing	1 \$ 2,995.00 2,995	retention. These are critical to responding to and investigating cyber attacks. \$ This .00 purchase will enhance WCSD's	WCSD will sustain this	Software, Risk Management	04AP-04-RISK	
Conware			monitoring	this cost into the ongoing operating budget.			
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		\$	\$				
		3 \$ 6,850.00 6,850	\$				

# **TRAINING COSTS**

LIXAIIVIII	0 00313						
Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		0	\$	\$			0
			0.00	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
		0.00	
Total	0 \$ 0.00 \$0		0

# Document Uploads top

Documents Requested * A-133 Audit (Most Current)	Required?	Attached Documents * FY22 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	✓	Payroll Policy Payroll Regulation
Procurement Policy	✓	Procurement Policy
Milestones download template	✓	Auditing Software Milestones
Capabilities Assessment download template	✓	WCSD Capabilities

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

Application ID: 448914

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems? Contact us at Questions® ZoomGrants com
©2002-2023 GrantAnalyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

_			
	Applicant Name	Washoe County School District	
	Project Name:	WCSD Account and File Auditing Soft	ware License
	Project Funding Stream:	FY 2023 SLCGP	
	Milestone Description*	Date of Expected Completion	
1	Purchase Software	15 days after award	
2	Receive license	30 days after award	
3	Perform installation with vendor support	60 days after award	
4	Ensure operation and begin monitoring	75 days after award	
5	Review system usage and confirm operation	90 days after award	
6			
7			
8			
9			
10			

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

# Washoe County School District CONTINGENT Email Security System

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

\$ 249,750.00 Requested

Submitted: 8/28/2023 10:32:42 AM (Pacific)

Project Contact Randy Drake

austin.smith@washoeschools.net

Tel: 7757894617

Additional Contacts

lohlin@washoeschools.net, radrake@washoeschools.net

**Washoe County School District** 

425 E 9th St Reno, NV 89512 United States

Director of Grants
Lauren Ohlin

Iohlin@washoeschools.net

Telephone 7757893435 Fax 775-333-5012

Web www.washoeschools.net

EIN 8860000919 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.

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. 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 20% cost share requirement for FY 2023 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.

## 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 2023 SLCGP. Please select the objective with which your project most closely aligns.
Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
✓ Objective 3: Implement security protections commensurate with risk.
Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
3. Please select which of the SLCGP program elements your project addresses.  Projects may align with more than one element.
1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
16. Distribute funds, items, services, capabilities, or activities to local governments.
4. Describe your project in detail.

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

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

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

This project will be implemented by WCSD's internal IT staff. Because WCSD's enterprise email system is hosted, we will integrate the environment with a vendor solution that is provided by their isolated cloud environment. This project will primarily be performed by internal staff working in coordination with a vendor to ensure mail flow is not impacted while ensuring their system gains visibility to our organization's email system. This work is performed in a centralized console and does not require on-hands installation of new equipment, systems, or software.

Imple	ement an email se	ecurity solution	to protect al	I users from internal and external email threats including malware, phishing, and business email compromise.
9. M	anagement & Ad	Iministration	(M&A) may	be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the
	unt you are reta			essary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting,
	sight of those invo			
10. [	Does this project	t require new	constructio	n, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental
	ning and Histori reviews are requ			iew? srupts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance
	chment for more in	nformation on	EHP reviews.	
<b>✓</b>	Yes No			
Cybe subr serv Add eval weel Hygi visit Revi base subr more	ersecurity and Ir mission and app ice." This servic itionally, CISA cuates external nextly vulnerability iene Services — CISA's Cyber Heed on the Nation eccipients should information, viour agency is all	nfrastructure roval of a grae assesses that an recommen an recommen etwork prese reports and SLCGP" to grygiene Informen CSR is a fall Institute of discomplete the sit Nationwide ready participanot yet signed	Security Agint but is a per "health" of the ways to end ways to end of the ways the ways to end of the ways the ways to end of	PS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the ency (CISA). For these required services and memberships, please note that participation is not required for ost-award requirementCyber Hygiene Services Web Application Scanning is an "internet scanning-as-a-of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Inhance security in accordance with industry and government best practices and standards. Vulnerability Scanning uting continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides s. To register for these services, email vulnerability-info@cisa.dhs.gov with the subject line "Requesting Cyber dictate in the body of your email that you are requesting this service as part of the SLGCP. For more information, https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity rous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their ministered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For urity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
<b>why</b> This threa	it cannot. project will supports, such as busin	ort ingress/egre less email con	ess, as well a apromise, cor	it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons is intra-organization email security. This is critical because most email threats come from outside the organization, but internal me from inside the organization (intra-org). This project will cover all staff and student accounts. Limiting implementation to
just s	staff members, ra	ther than inclu	ding student	accounts, would drastically degrade WCSD's capabilities in the event of a compromise of student accounts.
	project location c			oject will be executed. ub-recipient address.
14. F	Build or Sustain:	Select "build	l" if this pro	ject focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if
the ¡ ☑				y at its existing/current level.
_				
Sele	ct "Yes" if the pro Yes			other jurisdictions? dictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
			_	
Each	n selection should	have an acco	mpanying ite	anization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.  m in the line item detail budget table on the next tab  rocedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence
		dividual teams	, an overall o	rganizational structure, and leadership at each level in the structure
✓				ems that comply with relevant standards
	•		•	hat comply with relevant training standards nee knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to
_	respond to real e			
Line Item De	etail Budget <u>to</u>	<u>0</u>		
PLANNIN	G COSTS			
Planning Cos		Quantity	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?
			\$	
			\$	
			\$	
			\$	
			\$	
			\$	
			\$ \$	
			\$	
			¢	

	\$
	\$
0 0.00	\$
	0.00

# **ORGANIZATION COSTS**

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

## **EQUIPMENT COSTS**

<b>EQUIPMENT COSTS</b>					
Equipment Line Item Cost Name Description Quantity	Unit 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	AEL Number - Search https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
Email Software 75,000 Security licensing for software email License security product, including cloud portal and vendor support	\$ \$ 3.33 249,750.00	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	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.		04AP-11-SAAS

		other organizations.
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
	\$	\$
7	75,000 \$ 3.33 249,75	\$ 0.00

# **TRAINING COSTS**

Training 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 training with the State Training Officer?
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		0	\$ 0.00	\$ 0.00			0

# **EXERCISE COSTS**

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

# Document Uploads $\underline{top}$

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	FY22 Audit
Travel Policy	✓	<u>Travel Policy</u>
Payroll Policy	~	Payroll Policy
		Payroll Regulation

Procurement Policy	✓	Procurement Policy
Milestones download template	✓	Email milestones
Capabilities Assessment	✓	WCSD Capabilities Assessment
download template		

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

Application ID: 448906

Become a lan of ZoomGrants<sup>111</sup> on Facebook
Problems? Contact us at Questions of ZoomGrants com
©2002-2023 Grant/harlyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

	Applicant Name	Washoe County School District
	Project Name:	Email Security System
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Software	15 days after award
2	Receive license	30 days after award
3	Perform installation with vendor support	60 days after award
4	Ensure operation and begin monitoring	75 days after award
5	Review system usage and confirm operation	90 days after award
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

## **Washoe County School District SUSTAINED** WCSD Multi-factor Authentication (MFA) License

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

\$ 18,872.00 Requested

Submitted: 8/28/2023 10:33:04 AM (Pacific)

**Project Contact** 

Randy Drake

austin.smith@washoeschools.net

Tel: 7757894617

Additional Contacts

Iohlin@washoeschools.net, radrake@washoeschools.net

**Washoe County School District** 

425 F 9th St Reno, NV 89512 United States

**Director of Grants** Lauren Ohlin

lohlin@washoeschools.net

Telephone 7757893435 Fax 775-333-5012

Web www.washoeschools.net

8860000919 EIN 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 distri	ct,
intrastate district, council of government, regional government entity, agency or instrumentality of a local government, rural community, unincorporated to	wn
or village, or other public entity, tribe, or authorized tribal organization.	

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. 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 20% cost share requirement for FY 2023 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.

## Application Questions top

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

directly benefit much Mayordene
directly benefit rural Nevadans.  Yes
☑ No
2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
<ul> <li>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.</li> </ul>
Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
✓ Objective 3: Implement security protections commensurate with risk.
Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
3. Please select which of the SLCGP program elements your project addresses.  Projects may align with more than one element.
1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
12. Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
☐ 15. Ensure adequate access to, and participation in, cybersecurity services and programs by rural areas within the state.
16. Distribute funds, items, services, capabilities, or activities to local governments.
4. Describe your project in detail.  What would you like to do? Why? How does this project improve cybersecurity protection for your agency?

This project will provide licensing for Multi-Factor Authentication (MFA) software that Washoe County School District (WCSD) will use to protect administrator accounts. MFA is a technology that requires users to prove their identities with multiple factors rather than just a password. WCSD maintains an internal IT department that has MFA implemented for all logins on administrator accounts. This project will expand access to MFA and provide licensing and onboarding to WCSD's existing MFA platform for the remaining users that maintain some level of administrative permissions. WCSD is a large, geographically-dispersed public entity. However WCSD's IT department is relatively small, requiring individual technicians to support many schools. Because of this limitation, IT personnel are unable to provide constant technical support to each school. Therefore, administrative permissions are granted to multiple users on site, as designated by the site Principal. This project will actively support Objective 3: Implement security protections commensurate with risk by specifically protecting administrator accounts that are necessary to perform daily business and a safe and secure learning environment for WCSD's 62,000 students, including those in rural areas of Washoe County. This will allow the IT department to monitor and audit all user accounts. It will also prevent bad actors from compromising systems and immediately pivoting to other systems on a shared network.

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

Objective 3: "Implement security protections commensurate with risk." Implementing MFA for administrator accounts decreases WCSD's risk of having an administrative account compromised. It protects the entire computing environment. WCSD has limited implementation of this system in production currently and this will vastly reduce the lack of oversight on site-based administrators.

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

- 1. "Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology." This capability aligns with the management, monitoring, and tracking of user accounts owned and operated by WCSD. It helps to ensure that WCSD keeps an accurate inventory and auditing on the use of privileged accounts.
- 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 separates multi-factor authentication calls from the operating system and can identify authentication traffic and whether it is successfully passed or failed.
- 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 control prevents the unauthorized misuse and abuse of privileged accounts which could be used to compromise WCSD information systems and accounts.

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

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

This project will be implemented by WCSD's IT department staff. There already exists an implementation of multi-factor authentication using hardware tokens for IT staff. This project involves several key steps that will be extended to all remaining administrators. First, the web portal will be updated with a detailed policy describing when a second prompt is required. The user/agent will be installed on computers, and then the user/agent will be enrolled into the system to ensure that their account triggers the second prompt. This is largely automated, but requires coordination across technology departments and staff.

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

Implement Multi-Factor Authentication (MFA) prioritizing privileged users, internet-facing systems, and cloud accounts.

9. Management & Administration (M&A) may be retained at up to 5% of the total cost of the project. Will you be retaining funds for M&A? If YES, enter the amount you are retaining. If NO, enter "N/A"

				isary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting,	_
N/	rersight of those invo 'A	oivea in the of	perational aspec	xs or the granty	
PI: El- att	anning and Histori HP reviews are requi achment for more ir	ic Preservati ired for ANY	on (EHP) revie project that disri	, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental ew?  upts the environment or a structure, including small things like putting nails in walls. Please see the EHP Guidance	
_	☑ Yes ☑ No				
11 Cy su se Ac ev we Hy	REQUIRED SERV /bersecurity and Ir ibmission and app ervice." This servic dditionally, CISA c raluates external n eekly vulnerability /giene Services - S	nfrastructure roval of a grae assesses the assesses the an recomme etwork presereports and SLCGP" to g	Security Agen ant but is a pos- ne "health" of nd ways to enlance by execut ad-hoc alerts. et started. Indi	S: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the ncy (CISA). For these required services and memberships, please note that participation is not required for st-award requirementCyber Hygiene Services Web Application Scanning is an "internet scanning-as-a-your publicly accessible web applications by checking for known vulnerabilities and weak configurations. hance security in accordance with industry and government best practices and standards. Vulnerability Scanning continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides . To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber icate in the body of your email that you are requesting this service as part of the SLGCP. For more information,	9
Re ba su mo	eview (NCSR) The used on the National ubrecipients should ore information, vi	e NCSR is a fall Institute of complete the sit Nationwich ready participant yet signed	free, anonymou f Standards an he NCSR, admi de Cybersecuri ating in the Cybe	nttps://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity us, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is not Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their inistered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For ity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).  er Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP er Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if	
<b>wl</b> Th	hy it cannot. his project could be s	scaled up to s	upport MFA for	t be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons the entire District staff or staff and students. The current system configuration and license uses minimal additional "signal access should or should not be granted. Improvements will include higher tiers of licensing or integrations with existing	
13		jit zip code v	where the proj	ns in a much more firm "zero trust" methodology.  ject will be executed.  b-recipient address.	
	512				
the	e project strictly m ☑ Build			ect focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if at its existing/current level.	
L	Sustain				
Se				ther jurisdictions? ctions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.	
16	5. Please select all ach selection should Planning - Develor and information	have an acco	ompanying item icies, plans, pro	nization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.  In the line item detail budget table on the next tab  Decedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence ganizational structure, and leadership at each level in the structure	
			_	ns that comply with relevant standards	
	_	ds-on activities		at comply with relevant training standards e knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to	
Line Item	Detail Budget <u>to</u>	<u>0</u>			
	NG COSTS				
Planning C Name	ost Line Item Description	Quantity		Describe how the purchase(s) within this element tie into the How would your organization sustain this project if grant funding was reduced or discontinued?	
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
			\$		
		0	0.00 \$		

# **EQUIPMENT COSTS**

0 \$ 0.00

0.00

EQUIP	MENT COSTS					
	nt Line Item e Description Quantity	, Unit Tota Cost 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?	equipment-list to find AEL info	AEL Number - Search - https://www.fema.gov/grants/tools/authorized- equipment-list to find AEL info
MFA Software License	Software licensing for MFA product including cloud portal and vendor support		allow WCSD to implement MFA for all administrator accounts. Administrators can make	sustain this project through multiple mechanisms. It would reduce the number of administrators in the network to reduce licensing costs. WCSD is can also remove legacy software that requires e elevated permissions to run to reduce the overall license count used which would decrease r costs. After exhausting both avenues, WCSD will allocate funding for this project to support		O5AU-00-BIOM

user's passwords from any other means means
(malware,
phishing,
third-party
breach, etc.).
This makes
WCSD's network significantly more resilient to cyber attacks and adds an additional layer of security across the entire network. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ 700 26.96 18,872.00

# **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit . Cost	Γotal	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

# **EXERCISE COSTS**

Exercise Cost Nam	Line Item e 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?	Do you plan to coordinate this exercise with the State Exercise Officer?
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		

	\$ \$	
	\$ \$	
	\$ \$	
	<b>0</b> \$ <b>0.00</b> \$ 0.00	0
	0.00	
Total	0 \$ 0.00 \$0.00	0

# Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	FY22 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	~	Payroll Policy
		Payroll Regulation
Procurement Policy	~	Procurement Policy
Milestones download template	✓	MFA Milestones
Capabilities Assessment download template	✓	WCSD Capabilities assessment

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

Application ID: 448910

Become a fan of ZoomGrants<sup>TM</sup> on Facebook
Problems? Contact us at Questions@ZoomGrants com
@2002-2023 Grant/nallyst.com. All rights reserved.
"ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnallyst.com, LLC.
Logout | Browser

	Applicant Name	Washoe County School District	
	Project Name:	Multi-Factor Authentication (MFA) L	icense
	Project Funding Stream:	FY 2023 SLCGP	
	Milestone Description*	Date of Expected Completion	
1	System configuration complete	30 days after award	
2	50% of administrators MFA capable	45 days after award	
3	75% of administrators MFA capable	60 days after award	
4	100% of administrators MFA capable	90 days after award	
5			
6			
7			
8			
9			
10			

<sup>\*</sup>Please add additional rows as necessary for your project



Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

#### FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)

Deadline: 8/31/2023

## **Washoe County School District** WCSD Threat Intelligence System

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

\$	37	534	nn	Rec	uested
Ψ	JI.	,,,,,,	·vv	Ver	uesieu

Submitted: 8/28/2023 10:33:49 AM (Pacific)

#### **Project Contact**

Randy Drake

austin.smith@washoeschools.net

Tel: 7757894617

#### **Additional Contacts**

lohlin@washoeschools.net, radrake@washoeschools.net

#### **Washoe County School District**

425 E 9th St Reno, NV 89512 United States

**Director of Grants** 

Lauren Ohlin

Iohlin@washoeschools.net

Telephone 7757893435 775-333-5012 Fax

Web www.washoeschools.net

8860000919 EIN DEA6NNBHBTV3 UEL

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.
✓ 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 proposa 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. 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 20% cost share requirement for FY 2023 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.

#### 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 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.
e Pla	ease select which of the SLCGP program elements your project addresses.
Proje	cts may align with more than one element.
	<ol> <li>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.</li> </ol>
	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 an 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.
	<ol><li>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 internedomain.</li></ol>
	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 hygient 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 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.
_	<ol> <li>Leverage cybersecurity services offered by CISA. (See Question 12 for further details on these services.)</li> <li>Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology are</li> </ol>
	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.
_	
De Vhat	
L. De What his peed source organ WCS	16. Distribute funds, items, services, capabilities, or activities to local governments.  **scribe your project in detail.**  **would you like to do? Why? How does this project improve cybersecurity protection for your agency?  **project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other intelligence sources to identify and respond to cyber attacks. WCSD's project will allow a great platform and geographically-dispersed. However, WCSD has a relatively small IT department with technicians serving many schools at once. This project will allow D to prevent and to respond to cyber threats more efficiently. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for overnent based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's
L. De What Fhis peed source organ WCS mpro	16. Distribute funds, items, services, capabilities, or activities to local governments.  **scribe your project in detail.**  **would you like to do? Why? How does this project improve cybersecurity protection for your agency?  project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other  sees. This will improve cybersecurity for WCSD by allowing the District to analyze and integrate various intelligence sources to identify and respond to cyber attacks. WCSD's  nization is large and geographically-dispersed. However, WCSD has a relatively small IT department with technicians serving many schools at once. This project will allow  D to prevent and to respond to cyber threats more efficiently. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for  swement based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's  comment.
Whate This   eed source organ WCS mprocentifications of the control of the contro	16. Distribute funds, items, services, capabilities, or activities to local governments.  **scribe your project in detail.**  **would you like to do? Why? How does this project improve cybersecurity protection for your agency?  **project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other intelligence sources to identify and respond to cyber attacks. WCSD's inization is large and geographically-dispersed. However, WCSD has a relatively small IT department with technicians serving many schools at once. This project will allow D to prevent and to respond to cyber threats more efficiently. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for overnent based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's
L. Dee Whate This   eed source Triple   for the property   for the pro	16. Distribute funds, items, services, capabilities, or activities to local governments.  **Secribe your project in detail.**  **Would you like to do? Why? How does this project improve cybersecurity protection for your agency?  **Project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other rese. This will improve cybersecurity for WCSD by allowing the District to analyze and integrate various intelligence sources to identify and respond to cyber attacks. WCSD's part as relatively small IT department with technicians serving many schools at once. This project will allow D to prevent and to respond to cyber threats more efficiently. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for provement based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's comment.  **W does your project align with the objective selected in Question 2?**  **project aligns with Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured sesments" by creating the infrastructure for continuous testing, evaluation, and structured sesments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's environment.  **W does your project align with the program element(s) selected in Question 3?**  **polement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and rescurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the sta
I. De What Fhis   eed our corgan west of the property of the p	16. Distribute funds, items, services, capabilities, or activities to local governments.  **Secribe your project in detail.**  **Would you like to do? Why? How does this project improve cybersecurity protection for your agency?  **Project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other rese. This will improve cybersecurity for WCSD by allowing the District to analyze and integrate various intelligence sources to identify and respond to cyber attacks. WCSD's initiation is large and geographically-dispersed. However, WCSD has a relatively small IT department with technicians serving many schools at once. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for overent based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's onment.  **We does your project align with the objective selected in Question 2?**  **project aligns with Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured sements" by creating the infrastructure for continuous testing and assessment of systems in WCSD's environment.  **We does your project align with the program element(s) selected in Question 3?**  **pulpement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and security threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state." This systems that the state or local governments within the state. This syst
I. De What Fhis   Seed & Source Fhis   Seed & Source Fhis   Seed & Seed	16. Distribute funds, items, services, capabilities, or activities to local governments.  **scribe your project in detail.  **would you like to do? Why? How does this project improve cybersecurity protection for your agency?  project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other search is will improve cybersecurity for WCSD by allowing the District to analyze and integrate various intelligence sources to identify and respond to cyber attacks. WCSD in provent and to respond to cyber threats more efficiently. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's observed to the project align with the objective selected in Question 2?  **project aligns with Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured sements" by creating the infrastructure for continuous testing and assessment of systems in WCSD's environment.  **w does your project align with the program element(s) selected in Question 3?  **polement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and rescurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state." This systectively assess WCSD's environment against threat intelligence platforms to ensure that WCSD has an accurate picture of the environment.  **secribe*, in detail*, how, and
I. Dee Whate Fries   I. Dee Whate Fries   I. Dee Whate Fries   I. Dee State Fries   I. This   I.	16. Distribute funds, items, services, capabilities, or activities to local governments.  **scribe your project in detail.  **would you like to do? Why? How does this project improve cybersecurity protection for your agency?  project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other ses. This will improve cybersecurity for WCSD by allowing the District to analyze and integrate various intelligence sources to identify and respond to cyber attacks. WCSD in the interest and to respond to cyber threats more efficiently. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for wement based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing, evaluation, and structured assessment of systems in WCSD's environment.  **work does your project align with the objective selected in Question 2?**  project aligns with Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured sements" by creating the infrastructure for continuous testing and assessment of systems in WCSD's environment.  **work does your project align with the program element(s) selected in Question 3?**  project aligns with Objective 2: "Understand their current cybersecurity plants and assessment of systems in WCSD's environment against threat intelligence plants are consumed that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurit
J. Dee What I Fries I Source or Sour	16. Distribute funds, items, services, capabilities, or activities to local governments.  Secribe your project in detail.  Would you like to do? Why? How does this project improve cybersecurity protection for your agency?  project will provide licensing and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence service, and the infrastructure associated with the cyber intelligence sharing system that will allow WCSD to tap into the state's cyber threat intelligence platform and other ses. This will improve cybersecurity for WCSD by allowing the District to analyze and integrate various intelligence sources to identify and respond to cyber attacks. WCSD by a latelatively small IT department with chroicians serving many schools at once. This project will allow Dto prevent and to respond to cyber threats more efficiently. This project will directly address Objective 2: "Understand their current cybersecurity posture and areas for wement based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing, and assessment of systems in WCSD's environment.  We does your project align with the objective selected in Question 2? project aligns with Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured sements" by creating the infrastructure for continuous testing and assessment of systems in WCSD's environment.  We does your project align with the program element(s) selected in Question 3? publement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and security threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state." This systectively assess WCSD's environment against threat intelligence ba

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

recor netwo and a	mmend ways to ork presence by ad-hoc alerts. To	enhance sed executing corregister for	curity in ac continuous these serv	ssible web applications by checking for known vulnerabilities cordance with industry and government best practices and st scans of public, static IPs for accessible services and vulneral rices, email vulnerability_info@cisa.dhs.gov with the subject li	andards. Vulnerability Scanning evaluates external bilities. This service provides weekly vulnerability reports ne "Requesting Cyber Hygiene Services – SLCGP" to get
Page annu Tech MS-IS	e: https://www.cis ual self-assessme nnology Cybersed SAC, during the	sa.gov/topic ent designed curity Frame first year of	s/cyber-thread to measurework and is the award/	nat you are requesting this service as part of the SLGCP. For reats-and-advisories/cyber-hygiene-servicesNationwide Cybere gaps and capabilities of a SLT's cybersecurity programs. It is s sponsored by DHS and the MS-ISAC. Entities and their subresubaward period of performance and annually. For more infornces (cisecurity.org).	rsecurity Review (NCSR) The NCSR is a free, anonymous, s based on the National Institute of Standards and cipients should complete the NCSR, administered by the
1		ot yet signed		Cyber Hygiene Services and Nationwide Cybersecurity Review (NCS Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR)	
			n any part o	of it be reduced or expanded? Describe the ways in which the	project can be reduced or expanded, or the reasons why it
				ling on the integrations with third-party cyber threat intelligence platfo	orms. It could integrate other sources or remove them and their
	project location co	•		oroject will be executed. sub-recipient address.	
proje <b>✓</b>	ect strictly mainta Build			oject focuses on starting a new capability, or the intent of the tits existing/current level.	project is to close a capability gap. Select "sustain" if the
	Sustain				
Selec	ct "Yes" if the proje Yes			o other jurisdictions? sdictions (e.g., multiple cities). Select "No" if the project primarily su	pports a single entity.
	Please select all a			ganization, equipment, training, and exercise (POETE) elemen tem in the line item detail budget table on the next tab	ts for which funding is being sought for this project.
	information			procedures, mutual aid agreements, strategies, and other publication organizational structure, and leadership at each level in the structure	,
	Training - Content	and method	s of delivery	tems that comply with relevant standards that comply with relevant training standards ance knowledge of plans, allow members to improve their own perfor	mance, and identify opportunities to improve capabilities to
	respond to real ev				, , , , , , , , , , , , , , , , , , , ,
Line Item De	etail Budget <u>top</u>				
PI ANNING	G COSTS				
PLANNING Planning Cost	t Line Item	Quantity	Unit Cost Tot	Describe how the purchase(s) within this element tie into the	
Planning Cost		Quantity	Cost	al Describe how the purchase(s) within this element tie into th project as described in the Application Questions section.	e How would your organization sustain this project if grant funding was reduced or discontinued?
Planning Cost	t Line Item	Quantity	Cost	project as described in the Application Questions section. \$ \$	
Planning Cost	t Line Item	Quantity	Cost	project as described in the Application Questions section.  \$ \$ \$ \$ \$	
Planning Cost	t Line Item	Quantity	Cost	project as described in the Application Questions section. \$ \$ \$	
Planning Cost	t Line Item	Quantity	Cost Total	project as described in the Application Questions section.  \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
Planning Cost	t Line Item	Quantity	Cost Total	project as described in the Application Questions section.  \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
Planning Cost	t Line Item	Quantity	Cost	project as described in the Application Questions section.  \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
Planning Cost	t Line Item	Quantity	Cost	project as described in the Application Questions section.  \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
Planning Cost	t Line Item	Quantity	Cost	project as described in the Application Questions section.  \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
Planning Cost	t Line Item	Quantity	Cost	project as described in the Application Questions section.  project as described in the Application Questions section.  project as described in the Application Questions section.	
Planning Cost Name	t Line Item	0	0.00	project as described in the Application Questions section.  project as described in the Application Questions section.  project as described in the Application Questions section.	
Planning Cost Name  ORGANIZ	t Line Item Description	0 TTS	0.00 0.00	project as described in the Application Questions section.  \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	grant funding was reduced or discontinued?
Planning Cost Name  ORGANIZ Organizationa	LATION COS	0 TTS	0.00 0.00 ntity Unit	project as described in the Application Questions section.  Total Describe how the purchase(s) within this element tie in project as described in the Application Questions section.	grant funding was reduced or discontinued?
Planning Cost Name  ORGANIZ Organizationa	LATION COS	0 TTS	0.00 0.00 ntity Unit	project as described in the Application Questions section.  Total Describe how the purchase(s) within this element tie in project as described in the Application Questions section.	grant funding was reduced or discontinued?
Planning Cost Name  ORGANIZ Organizationa	LATION COS	0 TTS	0.00 0.00 ntity Unit	project as described in the Application Questions section.  Total Describe how the purchase(s) within this element tie in project as described in the Application Questions section.	grant funding was reduced or discontinued?
Planning Cost Name  ORGANIZ Organizationa	LATION COS	0 TTS	0.00 0.0 ntity Unit	project as described in the Application Questions section.  Total Describe how the purchase(s) within this element tie in project as described in the Application Questions section.	grant funding was reduced or discontinued?

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

Part	EQUIPMENT COSTS	
Intelligence   Including   Standard   Stan	Equipment Line Item Cost Name Description  Quantity Unit Cost  Total how the purchase(s) within this element tie into the project as described in the Application Questions  How would your organization sustain this element tie into the project as described in the Application Questions  AEL Name - Search AEL Number - Se project if https://www.fema.gov/grants/tools/authorized- https://www.fema.gov/grants/tools/authorized- https://www.fema.gov/grants/tools/authorized- or discontinued?	.gov/grants/tools/authorized-
Infrastructure infrastructure   1,767.00   3,534.00   the hosted infrastructure   1,767.00   3,534.00   the hosted infrastructure   1,767.00   1,767.00   3,534.00   the hosted infrastructure   1,767.00   1,7	Intelligence License License MFA product including cloud portal and vendor support  License  MFA product including cloud portal and vendor support  Licensing for MFA product including cloud portal and vendor support  Licensing for Licensing for Courter to cyber threat and vendor support  Licensing for MFA product including cloud portal and vendor support  Licensing for Licensin	
	Infrastructure infrastructure  Infrastructure infrastructure  Infrastructure infrastructure infrastructure infrastructure infrastructure to support the system. It is where the actual software and connections costs going to third-party forward. intel sources would take place.  Infrastructure infrastructure infrastructure staff is needed to maintain the systems and maintain the infrastructure connections costs going to third-party forward. intel sources would take place.  Infrastructure review whether review whether infrastructure staff is needed to maintain the systems and maintain the infrastructure connections costs going to the place.  Infrastructure staff is needed to maintain redundant systems and maintain the infrastructure connections costs going to the place.  Infrastructure staff is needed to maintain redundant systems and maintain the infrastructure connections costs going to the place.  Infrastructure staff is needed to maintain redundant systems and maintain the infrastructure connections costs going to the place.  Infrastructure staff is needed to maintain redundant systems and maintain the infrastructure connections costs going to the place.  Infrastructure staff is needed to maintain redundant systems and maintain the infrastructure connections costs going to the place.  Infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to maintain redundant systems and maintain the infrastructure staff is needed to main	

# **TRAINING COSTS**

Training Cost Name	Line Item Description	Quantity	Unit Cost	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?	Do you plan to coordinate the training with the State Training Office	ing
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
		0	\$ 0.00	0.00				0

# **EXERCISE COSTS**

Exercise 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?	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 *	Required?	Attached Documents *
A-133 Audit (Most Current)	✓	FY22 Audit
Travel Policy	✓	Travel Policy
Payroll Policy	✓	Payroll Policy
		Payroll Regulation
Procurement Policy	<b>✓</b>	Procurement Policy
Milestones  download template	✓	<u>Milestones</u>
Capabilities Assessment download template	~	<u>Capabilities Assessment</u>

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

Application ID: 449039

Become a fan of ZoomGrants<sup>11</sup> on Facebook
Problems? Contact us at Questions 2 ZoomGrants com
62002-2023 GrantAnalyst.com. All rights reserved.

"ZoomGrants' and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC.
Logout | Browser

		Washoe County School District
	Project Name: Project Funding Stream:	WCSD Threat Intelligence Platform FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase Infrastructure	15 days after award
2	Receive Licensing, provision infrastructure	30 days after award
3	Perform integration with vendor support	60 days after award
4	Ensure operation and begin monitoring	75 days after award
5	Review system usage and confirm operation	90 days after award
6		
7		
8		
9		
10		

<sup>\*</sup>Please add additional rows as necessary for your project