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

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.

☑ 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?
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.

2. Understand how to provide security awareness training to end-users.
3. Treat and remediate malware infections.
4. Understand the function of and be able to configure and secure enterprise grade firewalls.
5. To design systems from scratch with a security mindset.

Participants who complete the DRI program will be qualified for positions including enterprise defender, information security analyst, cyber-awareness trainer, and security operations analyst.

There is an expected shortfall of 700,000 cybersecurity professionals in 2023 in the United States alone (https://www.linkedin.com/pulse/shortage-cyber-security-professionals-david-rotenberg/). In Nevada, throughout 2022 there were 6,907 people employed in the cybersecurity workforce and 6,902 cybersecurity job openings, a workforce supply/demand ratio of 1.0 (https://www.cyberseek.org/heatmap.html). Many of these jobs do not require 4-year degrees, but technical skills that can be acquired through on-the-job training, industry certifications, community college courses, and modern vocational and skills education programs. Nevada salaries for information security analysts, positions requiring either industry certificates or an associate degree, have a median wage of $83,290 (Nevada Department of Employment, Training, and Rehabilitation).

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
☑ No

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
□ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
This project is scalable, however we would need to find additional sources of match/in-kind funding as the project scales.

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Content Development and Program planning	DRI Salary + fringe – Cyber Expert content planning and development	1	23,443.20	$ 11,721.60	half of a month of time for 1 DRI cyber expert to develop cloud range and curriculum.	We would keep notes, drawings and curriculum for future use.
				$		

			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
			$
	1	**23,443.20**	**$ 11,721.60**

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
In-person Instruction and Hosting	DRI Salary + fringe – Cyber Expert hands-on instruction and initial assessment hosting	1	$ 23,443.20	$ 11,721.60	Half of a month of time for in-person hands on to host 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	$ 66,000.00	2-day Initial CTF assessment in each location to 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	$ 304,392.00	Course and Exam Vouchers for program finalists (20 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	$ 30,439.20	Course and Exam Vouchers for top performers in 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	$ 13,226.40	2 Instructors travelling from Reno to LV and back 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

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Cloud Based Lab	Azure Cloud Based Lab	1	$ 4,950.00	$ 4,950.00	This will be the hands-on demo lab where participants will spin up and harden Windows based systems.	We would seek alternate funding, primarily through grants or gifts to continue funding of this project.		
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				

	$	$
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$
1	$ 4,950.00	$ 4,950.00

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?
Cloud Course and Exam Voucher	Cloud Academy Course and Exam Voucher for Instructors	2	$ 15,219.60	$ 30,439.20	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

** ZoomGrants™ 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

*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 Fire/Emergency Management

Carson City EM / Physical Security Proximity/Camera

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

$ 191,039.10 Requested

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

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

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

Carson City Fire/Emergency Management

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

Business Manager
Dave Aurand
Daurand@carson.org

Telephone	7752837820
Fax	
Web	
EIN	88600189
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.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Installing of all hardware (proximity readers, video cameras, cypher locks, communication boards, and electrical wiring) will be implemented by a vendor. As doors readers are installed by the Vendor, the IT/Cyber Department will monitor the process and approve the installation. IT/Cyber will also monitor, track, investigate, and report any unauthorized attempts to access the centers.
After installation and warranty period are over, the Carson City general fund will be responsible for the ongoing maintenance of the systems.

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

9. Management & Administration (M&A) 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.

☐ Yes

☑ No

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

Yes. Should there not be enough funding from the state, Carson City could implement in phases across several CISA Cyber Security Grant cycles to procure, install, and make operational. The combination of three types of physical security and the three phases of operational completion would allow for scalability.

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

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

89701

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

☑ Build

□ Sustain

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

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

☑ Yes

□ No

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

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
Carson City Fire/Emergency Management	Allowable 5% M& A Costs for grant management staff	1	$ 9,097.10	$ 9,097.10	This funding will be the allowable 5% M & N costs for management of the grants Staff.	We would lose the allowable costs from the grant application.
			$	$		
			$	$		
			$	$		
			$	$		

	$	$
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$
	$	$
1	**$ 9,097.10**	**$ 9,097.10**

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Intrusion Security System, Infrastructure Only	System wiring project for the entire system by square feet	18,024	$ 1.75	$ 31,542.00	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	$ 30,000.00	Hardware required to support the product/service.	After initial install, the maintenance would be general fund	System, Intrusion Detecti	05NP-00-IDPS
Cypher locks	15 high security point cyphers	15	$ 2,000.00	$ 30,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	System, Intrusion Detecti	05NP-00-IDPS
Multi-Directional Sensor Camera	10 Multi-Directional Sensor Cameras for intrusion tracking	10	$ 1,900.00	$ 19,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	Systems, Video Assessment	14SW-01-VIDA
Fish Eye Camera	10 Fish Eye Cameras	10	$ 900.00	$ 9,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	Systems, Video Assessment	14SW-01-VIDA
Standard Camera	6 Standard Surveillance Cameras	6	$ 400.00	$ 2,400.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	Systems, Video Assessment	14SW-01-VIDA
Access Control Proximity Strike pad	20 Proximity Strike pads	20	$ 1,000.00	$ 20,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	System, Credentialing	4AP-05- CRED
Vendor installation	Contractor will install the hardware and software for physical security.	1	$ 40,000.00	$ 40,000.00	The Vendor will install the proximity access, Cypher locks, and video camera security systems.	The program would have to be reduced for initial project development. The ongoing maintenance will be budgeted for in the city general fund.		
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		18,092	**$ 51,201.75**	**$ 181,942.00**				

TRAINING COSTS

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

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 449130

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

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

*Please add additional rows as necessary for your project

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

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

$ 24,401.60 Requested

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

Project Contact
Jessica Greener
jgreener@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

Telephone	775-283-2100
Fax	775-283-2093
Web	https://www.carsoncityschools.com/
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 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 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.
□ 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?
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.

5. How does your project align with the objective selected in Question 2?
Our risk assessments indicate a need for improvements around physical security. The objective of this project is to mitigate the risks associated with unauthorized access.

6. How does your project align with the program element(s) selected in Question 3?
Addressing 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 resources from unauthorized access.

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.
Upon 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 conducted by district employees and will be scheduled to take place over school breaks to avoid negative impacts to operations.

8. Describe, in a few sentences, the desired outcome(s) of your project.
Our desired outcome is to secure access to ICT equipment for the purpose of mitigating cyber risk associated with unauthorized access.

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
☑ No

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
□ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

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

The project can't be expanded. We need a specific number of secure equipment racks to replace our existing unsecure equipment racks. Purchasing more than what is being requested is not necessary.

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, 89703, and 89706

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

☑ Build
□ Sustain

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

□ Yes
☑ No

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application	How would your organization sustain this project if grant funding was reduced	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

					Questions section.	or discontinued?		
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	$ 748.00	$ 20,196.00	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.	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	$ 600.80	$ 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.	If funding was 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	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

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

EXERCISE COSTS

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

Document Uploads *top*

Documents Requested *	Required?	**Attached Documents** *
A-133 Audit (Most Current)	☑	2022 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

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

Application ID: 449453

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 Program
	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		

*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 Core Router Replacement

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

$ 144,854.24 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
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.

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?
The City of Reno has one functioning core router with our backup in a non-working condition. The current routers went end of sale in 2015 and no new software releases since 2020. This device is the central routing hub for all East/West traffic in the entire network and is critical to have continuous security patching along with redundancy. The City of Reno also supports/hosts the regional 911 CAD systems for public safety response and dispatching for all citizens of Reno, Washoe, Sparks, UNR PD, RSIC PD, Reno Airport and Pyramid Lake PD. 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 assessment 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 install 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 future.

5. How does your project align with the objective selected in Question 2?
Leveraging 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. This 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 experience hardware failures in the near future.

6. How does your project align with the program element(s) selected in Question 3?
The new routers follow the NIST framework - Identify, Protect, Detect, Respond and Recover:
PR.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.DS-2: Data-in-transit is protected -NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity NIST SP 800-53 Rev. 4 SC-16, SI-7

PR.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-32, 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

7. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Our Senior Network Analyst will rack, install and configure the new core routers.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The 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 routers provide for resilience in an attack, equipment failure, or disaster.

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

☑ No

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

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

The project is a complete replacement of our core routers. It would not be best practice to do a partial replacement, nor would it get you any of the security features/functionality that we aim to accomplish with this replacement.

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

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

89501

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

☑ Build

☐ Sustain

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

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

☐ Yes

☑ No

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

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Router - managed - rack-mountable	Router	2	$ 9,617.09	$ 19,234.18	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	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	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	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	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	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	Internal Parts/Modules	2	$ 6,407.51	$ 12,815.02	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	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	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what 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	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	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	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
50GBase direct attach cable - 10 ft	Internal Parts/Modules	2	$ 349.28	$ 698.56	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	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	$ 7,268.76	The City has 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.	Warranty and 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	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			

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

Document Uploads *top*

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

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

Application ID: 449760

	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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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.

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?
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
• 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
• 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.

The 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 give access for the assessment to be completed.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The City will receive a deliverable report with prioritized action items. Action items will be assessed and planned based on funding needed, if hardware replacements are required, staff time balance with day to day operations and when changes can be implemented while minimizing down time/user impact. Recommendations with no financial impact will be assessed and scheduled. Recommendations with a financial impact will be assessed and prioritized for budgeting.

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

☑ No

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

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

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

☑ Build

☐ Sustain

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

☐ Yes

☑ No

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Fixed Fee Cost	Total cost for complete assessment.	1	52,237.00	$ 52,237.00	This is a fixed price for the complete network and security assessment.	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	52,237.00	$ 52,237.00

ORGANIZATION COSTS

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

EQUIPMENT COSTS

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

TRAINING COSTS

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

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 449751

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

Logout | 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		

*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/SUSTAIN Switch Replacement

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

$ 205,023.39 Requested

Submitted: 8/31/2023 3:11:22 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	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
☐ 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?
The 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 interface 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 target 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 pane 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 project would assist the City in getting back inline with consistent replacement.

5. How does your project align with the objective selected in Question 2?
This 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 easier 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 segmentation 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 Plant 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.

6. How does your project align with the program element(s) selected in Question 3?
The new switches follow the NIST framework - Identify, Protect, Detect, Respond and Recover:
PR.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.DS-2: Data-in-transit is protected NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity NIST SP 800-53 Rev. 4 SC-16, SI-7

PR.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-32, 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

7. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
Our Senior Network Analyst will replace unsupported switches with the new hardware and configure each device.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The 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. 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
☑ No

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

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

We have asked for the replacement of 30 of our oldest switches. We currently have 64 unsupported switches. Getting approved for even one switch helps us get through the required amount of switches that need to be replaced. The total of each switch with support is $6,454.51 and thus the number can be scaled up or down. We would benefit from 30 from the 2022 funding round and another 30 from the 2023 funding round but this can definitely be scaled up or down.

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

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

89501

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

☑ Build

□ Sustain

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

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

□ Yes

☑ No

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

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

0	$ 0.00	$ 0.00

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
48FP L2 Stck Cld-Mngd 48x GigE 740W PoE Switch	Switch	27	$ 5,433.70	$ 146,709.90	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
48FP Enterprise License and Support, 7YR	License and Subscription	27	$ 1,666.26	$ 44,989.02	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	$ 10,211.61	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
24P Enterprise License and Support, 7YR	License and Subscription	3	$ 1,037.62	$ 3,112.86	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
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		60	**$ 11,541.45**	$ 205,023.39				

TRAINING COSTS

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

EXERCISE COSTS

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

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

Document Uploads *top*

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

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

Application ID: 449761

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

Logout | Browser

	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		

*Please add additional rows as necessary for your project

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

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

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

$ 68,750.00 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
UEI	SRBYQ7XFBYA6
SAM Expires	

Pre-Application top

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

☑ 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?
Security Vendor will work with Clark County School District staff to update incident response plans, create additional departmental work aids, and create a tailored tabletop focused on transportation and food services disruptions due to cyberattack. CCSD is focused on these critical services to ensure continuity of operations. Benefits the 7.24% of rural communities that 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?
The project ensures that the proper protocols are in place to respond effectively to cybersecurity incidents and ensure continuity of operations.

6. How does your project align with the program element(s) selected in Question 3?
The project ensures that there has been proper preparation by examining the response and resilience of the information systems in place. Further, the project will ensure that there 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)
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

☑ No

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

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

Can not be scaled due to the vendor package of an incident response plan and single tabletop exercise.

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

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

☑ Build

☐ Sustain

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

☐ Yes

☑ No

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Professional Services	Professional Services for Incident response plan	1	35,000.00	$ 35,000.00	One time cost.	Preparation and planning for the setup of the incident response plan and the tabletop exercise.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		

				$
				$
		1	35,000.00	$ 35,000.00

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Program Management	Contractor Cost: Program and Project management resources	50	$ 175.00	$ 8,750.00	Organizing and managing the completion of the project, 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

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

TRAINING COSTS

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

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

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
Professional Services	Services for tabletop exercise	1	$ 25,000.00	$ 25,000.00	Enhance the response and resilience of critical systems. Ensure the continuity of operations.	One time cost.	Yes
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		1	$ 25,000.00	$ 25,000.00			0
Total		**1**	**$ 25,000.00**	**$25,000.00**			**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

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

Application ID: 449733

	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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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: Pre-Application Application Questions Line Item Detail Budget Document Uploads

$ 76,918.98 Requested

Submitted: 8/30/2023 1:58:39 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
UEI	SRBYQ7XFBYA6
SAM Expires	

Pre-Application *top*

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

☑ 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?
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 that 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 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.
500 critical 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, 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

☑ No

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

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

- □ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- ☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

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

No.

Currently scaled down to most critical accounts totaling 500. Clark County School District has approx. 40,000 employees.

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

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

- ☑ Build
- □ Sustain

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

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

- □ Yes
- ☑ No

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Program Management	Contractor Cost: Program and Project management resources	150	175.00	$ 26,250.00	Planning, oversight and project management to attain milestone delivery associated with: Adopt and use best practices and methodologies to enhance cybersecurity – Multi Factor Authentication. 150 hours at $175 per hour.	One time cost.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		150	**175.00**	**$ 26,250.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Professional Services	Professional Services to implement MFA	1	$ 20,000.00	$ 20,000.00	Integration expertise to enhance cybersecurity - Multi Factor Authentication	One time cost.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
		1	$ 20,000.00	$ 20,000.00

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
MFA	Multifactor Authentication – 500 accounts	1	$ 30,668.98	$ 30,668.98	Adopt and use best practices and methodologies to enhance cybersecurity – Multi Factor Authentication	Reduce funding to other district priorities.	Applications, SAAS	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	$ 30,668.98	$ 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	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)	☑	CCSD Comprehensive Annual 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

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

Application ID: 449732

	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		

*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 Requested

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.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
UEI	SRBYQ7XFBYA6
SAM Expires	

Pre-Application top

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

☑ 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?

Increase security posture by installing new next-generation firewalls in front of all datacenter resources. Currently, only certain data center resources are protected by firewalls. Unprotected 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 traffic 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.

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?

Protect datacenter applications, critical services and student data that are currently susceptible to cyber security attacks and are at risk.

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

Increase security posture by installing new next-generation firewalls in front of all datacenter resources. Currently, only certain data center resources are protected by firewalls. Unprotected 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 traffic 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.

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.

Purchase hardware and software firewalls. CCSD network personnel and consultants will install the firewalls in the datacenter. Staff will test functionality and once validated will cut over traffic to the new firewalls.

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

Ability 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 of communications and data network within the data center and out to schools. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers.

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

☑ No

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

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

The firewall sizing is based on the amount of traffic flowing through the datacenter and out to schools currently. Scaling down or reducing the firewall capacity would block access to critical resources for students and teachers.

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

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

☑ Build

☐ Sustain

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

☐ Yes

☑ No

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Program Management	Contractor Cost: Program and Project management resources	1,200	175.00	$ 210,000.00	Planning, oversight and project management to attain milestone delivery associated with: Deploy new capability to monitor, audit, track network traffic and ensure continuity of communications to these key resources. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers. 1,200 hours at $175 per hour.	Reduce funding to other district priorities.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		1,200	**175.00**	**$ 210,000.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Consulting Services	Professional Services to implement.	1	$ 70,999.00	$ 70,999.00	Installation and configuration of firewalls that will block malicious traffic. Mitigate risks and cybersecurity threats relating to critical resources for students and teachers.	N/A - One time cost.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$
			$	$
			$	$
			$	$
		1	$ 70,999.00	$ 70,999.00

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Firewall	Virtual Firewalls and Licensing	6	$ 5,513.51	$ 33,081.06	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.	Firewall, Network	05NP-00-FWAL
Firewall	Hardware Firewalls and Licensing	2	$ 488,850.60	$ 977,701.20	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.	Firewall, Network	05NP-00-FWAL
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		8	$ 494,364.11	$ 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.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

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

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 449664

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

Will request title be corrected if project is funded - AJ 09/11/23

	Milestone Description*	Date of Expected Completion
1	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
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

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

Clark County School District

Security Awareness Training SAAS

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

$ 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
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
UEI	SRBYQ7XFBYA6
SAM Expires	

Pre-Application top

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

☑ 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?
Purchase SaaS security awareness platform and 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.

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?
Ensure staff are appropriately trained in cybersecurity through the use of a security awareness training platform.

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.

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.
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.

8. 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.

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

☑ No

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

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

- □ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- ☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

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

The SaaS platform is provisioned based on the number of employees in the district.

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

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

- □ Build
- ☑ Sustain

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

- □ Yes
- ☑ No

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Program Management	Contractor Cost: Program and Project management resources	150	175.00	$ 26,250.00	Planning, oversight and project management to enhance security awareness of staff. 150 hours at $175 per hour.	Reduce funding to other district priorities.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		150	**175.00**	**$ 26,250.00**		

ORGANIZATION COSTS

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

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Security Awareness Platform	Security as a service - Security Awareness Platform – 24 month term	1	$ 400,000.00	$ 400,000.00	Enhance security awareness of staff.	Reduce funding to other district priorities.	Applications, SAAS	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	$ 400,000.00	$ 400,000.00				

TRAINING COSTS

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

EXERCISE COSTS

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

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

Document Uploads *top*

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

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

Application ID: 449665

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

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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

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

Clark County School District

SUSTAIN - Multi Factor Authentication for ALL Employees

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

$ 782,800.00 Requested

Submitted: 8/29/2023 2:26:01 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	886000030
UEI	SRBYQ7XFBYA6
SAM Expires	

Pre-Application *top*

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

☑ 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?
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 that 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 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 "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

☑ No

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

the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

Clark County School District has approx. 40,000 employees. The MFA software is purchased based on the capacity of users. The protection of MFA could be applied to Principals, Vice Principals, Office Administrators and District administrative accounts, reducing the software capacity to support 20,500 critical accounts. This would leave teachers and other staff accounts susceptible to attack.

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

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

☐ Build

☑ Sustain

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

☐ Yes

☑ No

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Program Management	Contractor Cost: Program and Project management resources	250	175.00	$ 43,750.00	Planning, oversight and project management to attain milestone delivery associated with: Adopt and use best practices and methodologies to enhance cybersecurity – Multifactor Authentication. 250 hours at $175 per hour.	One time cost.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		250	**175.00**	**$ 43,750.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Professional Services	Professional Services to implement MFA	1	$ 20,000.00	$ 20,000.00	Integration expertise to enhance cybersecurity - Multi Factor Authentication	One time cost.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
		1	$ 20,000.00	$ 20,000.00

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
MFA	Multifactor Authentication – 40,000 accounts	1	$ 719,050.00	$ 719,050.00	Adopt and use best practices and methodologies to enhance cybersecurity – Multi Factor Authentication	Reduce funding to other district priorities.	Applications, SAAS	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	$ 719,050.00	$ 719,050.00				

TRAINING COSTS

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

EXERCISE COSTS

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

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

Document Uploads *top*

Documents Requested *	Required?	**Attached Documents** *
A-133 Audit (Most Current)	☑	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 Update CCSD Capabilities Assessment

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

Application ID: 449654

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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

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

Ely Shoshone Tribe

"CONTINGENT" Migrate to a .gov internet domain

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

$ 28,487.90 Requested

Submitted: 8/28/2023 2:24:02 PM (Pacific)

Project Contact
Michael Dalton
daltonm@elyshoshonetribe.com
Tel: (775) 289-7989

Additional Contacts
none entered

Ely Shoshone Tribe

505 S Pioche Hwy
Ely, NV 89301
United States

Finance Director
Sarah Balares
balaress@elyshoshonetribe.com

Telephone	(775) 289-3013
Fax	
Web	
EIN	94 2398696
UEI	PHLGX6MG6UK1
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?
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.

5. How does your project align with the objective selected in Question 2?
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 methodologies 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 use 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 a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

□ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
This project can not be scaled down; the project is to migrate the existing elyshoshonetribe.com to the .gov website and email address.

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

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

☑ Build

□ Sustain

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

□ Yes

☑ No

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
M&A Costs	Grant Administration	1	$ 1,356.57	$ 1,356.57	This expense will be covered through everyday budget planning.	Grant administration will involve quarterly progress reporting, quarterly financial reporting, and maintaining the cyber hygiene services.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		1	**$ 1,356.57**	**$ 1,356.57**		

EQUIPMENT COSTS

	Describe how the purchase(s) within	How would your organization

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	this element tie into the project as described in the Application Questions section.	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
Windows Server	Windows Server and Licensing	1	$ 3,374.08	$ 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	This is a one-time purchase that does not require monthly expenses	Hardware, Computer	04HW-01-INHW
O365 Licensing	G3 Licensing for 53 Users	53	$ 276.00	$ 14,628.00	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	53	$ 60.00	$ 3,180.00	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	This expense will be covered through normal budget planning	Software as a service	04AP-11-SAAS
Email Spam Protection	Email Spam Protection Software	53	$ 60.00	$ 3,180.00	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	This is a one-time purchase that doesn't require monthly expenses	Software as a service	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		213	**$ 3,785.08**	**$ 25,157.08**				

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?
O365 End USer Training	Provide Training to all end users on how to use O365	13	$ 149.00	$ 1,974.25	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**

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)	☑	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

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

Application ID: 449563

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

Logout | 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

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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

Submitted: 8/31/2023 4:03:22 PM (Pacific)

Project Contact
Lisa Lucas
llucas@doc.nv.gov
Tel: 7759775608

Additional Contacts
cfranklin@doc.nv.gov

Nevada Department of Corrections

5500 Snyder Avenue, Building 89
89701, NV 89706
United States

Director
James Dzurenda
jdzurenda@doc.nv.gov

Telephone	17759775608
Fax	
Web	www.doc.nv.gov
EIN	886000022
UEI	F66UTU4ATHJ1
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?
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 includes real-time analysis of traffic and the ability to identify and block advanced threats such as zero-day exploits and malware.

6. How does your project align with the program element(s) selected in Question 3?
A newer, upgraded firewall hardware and management software offer several features and capabilities that enhance an organization's preparation against cyber risks and threats, facilitate continuous vulnerability assessment and threat mitigation, and promote the adoption of best practices to enhance cybersecurity. Here's how the firewalls could achieve these goals; enhancing preparation against cyber risks and threats, implementing continuous vulnerability assessment and threat mitigation, adopting best practices to enhance cybersecurity.

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.
Implementation and deployment will be completed by a combination of NDOC IT personnel as well as vendor professional service. NDOC personnel will travel to each location to install the hardware. The chosen vendor would assist NDOC with each device configuration and testing. The NDOC Project Manager would oversee the project build, and provide planning and implementation support to IT personnel and vendor.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcomes of this project include: improved security, advanced threat detection, reduced attack surface, enhanced visibility, improved performance, efficient management, compliance and reporting, secure remote access, integration with security ecosystem, resilience and high availability, future-readiness, and cost-efficiency. Ultimately, the desired outcome of this firewall refresh project will center around strengthening the organization's cybersecurity defenses, enhancing network performance, and ensuring alignment with current and future security challenges. These outcomes collectively contribute to a more resilient and secure digital environment.

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
☑ No

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA’s Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --Nationwide Cybersecurity Review (NCSR)-- The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
□ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
Yes, it can be reduced. It can be reduced removing the hardware, licenses, and support for the devices that do not reach end-of-life in 14 months. Can also be reduced by shortening the license and support years down from 5 to1.

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
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	$ 4,000.00	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

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
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	$ 52,813.86	Required software for firewall, provides additional security features.	Reduce from 5 years to 1 years. Add to NDOC base budget.	SOFTWARE, NETWORK	04SW-04-NETW
Firewall URL Filtering	ADVANCED URL FILTERING SUBSCRIPTION,	8	$ 9,364.16	$ 74,913.28	Required software for firewall,	Reduce from 5 years to 1 years. Add to	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	$ 113,330.00	Required to maintain firewall uptime.	Reduce from 5 years to 1 years. Add to NDOC base budget.	SOFTWARE, NETWORK	04SW-04-NETW
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.	Reduce from 5 years to 1 years. Add to NDOC base budget.	SOFTWARE, NETWORK	04SW-04-NETW
Camp FIrewalls	FIREWALL DEVICES	5	$ 1,295.00	$ 6,475.00	Firewall provides network security.	One time purchase.	FIREWALL, NETWORK	05NP-00-FWAL
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.	Reduce from 5 years to 1 years. Add to NDOC base budget.	SOFTWARE, NETWORK	04SW-04-NETW
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.	Reduce from 5 years to 1 years. Add to NDOC base budget.	SOFTWARE, NETWORK	04SW-04-NETW
Camp equipment rack	RACK MOUNTABLE TRAY FOR UP TO TWO DEVICESAND 4 PO WER ADAPTERS FOR A 2 POST RACK MOUNT	5	$ 89.83	$ 449.15	Hardware for camp mounting firewalls.	One time purchase.	HARDWARE, COMPUTER, INTEG	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
		73	**$ 46,934.85**	**$ 436,897.05**				

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?
IT Staff Training		150	$ 109.83	$ 16,474.50	Provide NDOC IT training for hardware configurations and to implement 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	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

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

Document Uploads *top*

Documents Requested *	Required?	**Attached Documents** *
A-133 Audit (Most Current)	☑	Single Audit Report
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

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

Application ID: 448611

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

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 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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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: Pre-Application Application Questions Line Item Detail Budget Document Uploads

$ 1,000,000.00 Requested

Submitted: 8/30/2023 3:49:36 PM (Pacific)

Project Contact
Shauna Bakkedahl
shauna.b@sos.nv.gov
Tel: 775-230-8686

Additional Contacts
none entered

Nevada Secretary of State

101 N Carson St
Carson City, NV 89701
United States

ASO 3
Ashley Griffitts
dalea@sos.nv.gov

Telephone	775-684-5709
Fax	
Web	https://www.nvsos.gov/sos
EIN	886000022
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.

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?
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 business licensing portal and processing systems. Quickly identify clean copies of data for the purpose of recovery. Isolation, immutable backups, comprehensive scanning, and detailed reporting allows the Cyber Recovery Secretary of State's Office, Nevada to recover critical systems with confidence.

5. How does your project align with the objective selected in Question 2?
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 gap of not having an immutable, offline backup of our most precious data.

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 intervention. This operational air gap delivers network isolation, inaccessible from production and from unsecured networks. It will eliminate production-accessible management interfaces that can be compromised. The cyber-Vault deployed within the secured vault environment (Switch Facility), which automates data synchronization between the vault and production systems, creating immutable copies with locked retention policies. Additionally, the Vault will run analytics designed to detect potential issues early.

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 data and a path to recovery from a cyber event.

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

☑ No

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

□ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

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

☑ Build

□ Sustain

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

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

□ Yes

☑ No

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

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Dell Cyber Vault	Data Protection Software	1	$ 1,000,000.00	$ 1,000,000.00	Protects mission critical data within the Secretary of State in a separate highly secured area.	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**	$ 1,000,000.00				

TRAINING COSTS

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

EXERCISE COSTS

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

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

Document Uploads *top*

Documents Requested *	Required?	**Attached Documents** *
A-133 Audit (Most Current)	☑	A133 Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestones
Capabilities Assessment download template	☑	

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

Application ID: 449040

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

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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

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

Nye County

CONTINGENCY Nye County Firewall Upgrade

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

$ 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
bjjabbour@nyecountynv.gov

Telephone	(775) 482-8192 or (775) 751-7075
Fax	(775) 482-8198 or (775) 751-7093
Web	www.nyecountynv.gov
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

□ 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 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

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

No. The firewall upgrade, consolidation, and addition of the logging server cannot be scaled down as removing any one component would render the intent ineffective.

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

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

89060

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

☑ Build

☐ Sustain

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

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

☐ Yes

☑ No

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

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
5% M&A	M&A	1	$	$	The firewall upgrade, consolidation, and addition of the logging server	Would not be necessary

			2,963.00	2,963.00	cannot be scaled down as removing any one component would render the intent ineffective.
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
		1	**$ 2,963.00**	**$ 2,963.00**	

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Firewall appliance	Firewall appliance	1	$ 13,176.47	$ 13,176.47	Update current firewall	Seek alternate grant funding	Firewall, network	05NP-00-FWAL
Firewall advanced threat protection subscription	Firewall subscription	1	$ 46,080.02	$ 46,080.02	Provide advanced threat protection, energize updates, instant replacement, malware protection, advanced remote, insights subscriptions for 36 months	Seek alternate grant funding	Firewall, network	05NP-00-FWAL
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		2	**$ 59,256.49**	**$ 59,256.49**				

TRAINING COSTS

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

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

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 448079

	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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

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

State of Nevada - Office of Cyber Defense Coordination

OCDC SLTT Resources Program

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

$ 228,800.00 Requested

Submitted: 8/31/2023 2:11:25 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	
EIN	866000022
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, 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?

Create 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 areas. It allows 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 communication 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. We are focusing our efforts on rural areas, with a minimum 80% of the funds awarded to be invested solely in those rural areas, however, our work is open to non-rural entities as well should they choose to use it. We anticipate rural funding allocation to exceed 80%. The needs of the rural areas will drive our products direction.

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

This project 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 and help them develop a roadmap of what is needed, and how to proceed in addressing that roadmap.

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

By allowing entities in our area of responsibility 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. 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 our area of responsibility, including those in the rural areas, to work together in sharing information in order to 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, education, outreach and technical threat analysis.

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

☑ No

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

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

- ☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- ☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

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

We can scale in multiple ways: If we expanded the project, we would be able to do more training and outreach programs. If we reduced the project, we would cut back on training and outreach.

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

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

89711

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

- ☑ Build
- ☐ Sustain

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

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

- ☑ Yes
- ☐ No

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Cybersecurity Policy Resource Repository	Create and maintain a repository of policy templates that partner agencies can use to build out their cybersecurity policies relevant to their organization.	1	20,000.00	$ 20,000.00	This will allow us to directly support entities throughout the state of Nevada become better cyber aware by sharing policy templates to help build their cybersecurity policies, thus ensuring they are better protected from cyber threats and/or attacks.	Work at finding alternate funding within our budget or via other grants.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		1	**20,000.00**	**$ 20,000.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Community Outreach	Community Outreach	1	$ 10,000.00	$ 10,000.00	This will allow us to reach out to the communities within our area of responsibility and educate the public to be cyber safe.	Work at finding alternate funding within our budget or via other grants.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

		$	$
		$	$
		$	$
		$	$
		$	$
		$	$
		$	$
		$	$
	1	**$ 10,000.00**	**$ 10,000.00**

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Cybersecurity Lab	Hardware and software for performing malware testing, security assessments, and security evaluations of various tools in use by partner entities	1	$ 84,000.00	$ 84,000.00	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.	Working with rural and other entities to ensure smoother deployment of support projects.	Hardware, Computer, Integ	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	**$ 84,000.00**	**$ 84,000.00**				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
Training for Incident Responders	Training Vouchers	4	$ 8,700.00	$ 34,800.00	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	**$ 8,700.00**	$ 34,800.00	**0**

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
Conference	Create a cyber conference for our partner entities throughout Nevada.	1	$ 50,000.00	$ 50,000.00	This will provide much needed networking and collaboration between the states partners with the ultimate goal of cyber entities within the state working together to create solutions and share expertise with on another.	Work at finding alternate funding within our budget or via other grants. This funding could include charging attendees and vendors for attending the conference.	No
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		1	**$ 50,000.00**	$ 50,000.00			**0**
Total		**1**	**$ 50,000.00**	**$50,000.00**			**0**

Document Uploads *top*

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

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

Application ID: 449707

	Applicant Name	Office of Cyber Defense Coordination
	Project Name:	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 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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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

$ 163,700.00 Requested

Submitted: 8/31/2023 2:10:52 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	
EIN	866000022
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, 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?
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.

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

☑ No

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

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

We can scale in multiple ways: Make additional use of contractors to speed development of the necessary tools. Subsidize or completely cover hardware/software licensing costs for rural/partner entities as well as increase initial deployment scopes.

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

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

89711

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

☐ Build

☑ Sustain

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

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

☑ Yes

☐ No

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

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Direct Support for Partner Entities	Working with all state entities, including rural, to ensure smoother	1	$ 20,000.00	$ 20,000.00	Would be used to directly support the deployment of the project with partner entities and provide hands on support for the technical needs required to get the	Work at finding alternative funding within our budget and request partner entities to assist in financially.

	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	$ 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	$ 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

Equipment Cost Name	**Line Item Description**	**Quantity**	**Unit Cost**	**Total**	**Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.**	**How would your organization sustain this project if grant funding was reduced or discontinued?**	**AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info**	**AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info**
Hardware Servers	Servers to run log analysis and collection tools.	1	$ 18,000.00	$ 18,000.00	Servers would be used to run software and services to support all elements of the project.	Look for legislative appropriations in the next legislative cycle.	Hardware, Computer, Integ	04HW01-1NHW
Software Licensing	Software Licenses	6	$ 6,000.00	$ 36,000.00	This 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**	**$ 54,000.00**				

TRAINING COSTS

Training Cost Name	**Line Item Description**	**Quantity**	**Unit Cost**	**Total**	**Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.**	**How would your organization sustain this project if grant funding was reduced or discontinued?**	**Do you plan to coordinate this training with the State Training Officer?**
Training for SOC / SEIM	Training Vouchers	4	$ 8,700.00	$ 34,800.00	Would allow us to create useful 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	$ 8,700.00	$ 34,800.00			0

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 449706

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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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

$ 510,000.00 Requested

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	
EIN	866000022
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, 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?
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 threat and/or an attack. This team will implement security 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.

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
☑ No

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

□ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
We can scale by expanding or reducing the number of staffing hired and the positions needed based on the needs of our partner entities.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89711

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

☑ Build
□ Sustain

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

☑ Yes
□ No

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

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

ORGANIZATION COSTS

Organizational Cost Name	**Line Item Description**	**Quantity**	**Unit Cost**	**Total**	**Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.**	**How would your organization sustain this project if grant funding was reduced or discontinued?**
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	$ 510,000.00	By creating an Incident Response Team we can support our SLTT partners within the state of Nevada, to include the rural entities. We can provide immediate assistance when any entity is experiencing a cyber threat or attack.	We would either seek alternate sources of funding or wait until the next legislative appropriations cycle and in the meantime, we would work within the means we have available.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		3	**$ 170,000.00**	**$ 510,000.00**		

EQUIPMENT COSTS

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

TRAINING COSTS

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

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

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 446168

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 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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

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

Truckee Meadows Water Authority

Field Site Network Resiliency & Monitoring

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

$ 112,353.62 Requested

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

Project Contact
Chris Briscoe
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
□ 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?
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"

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
☑ No

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

☐ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
☑ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
The current scope of this project is all of our field sites that currently have physical security cameras. More of our remote sites may eventually have physical security cameras. The project could be reduced by decreasing the number of sites but would leave those sites without reliable connectivity.

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

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

☑ Build
☐ Sustain

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

☐ Yes
☑ No

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
WAN Switches and components	Network switches with transceivers, power supplies, and cords	2	$ 20,987.85	$ 41,975.70	To facilitate room for a new DIA circuit connection, as well as redundancy and fault tolerance across existing circuits, supporting a re-designed WAN architecture that is more robust and reliable.	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	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.	Would need to 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	$ 12,332.96	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	$ 5,790.96	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
SD-WAN subscription	Subscription for firewall feature	8	$ 419.01	$ 3,352.08	Allows for software defined WAN connectivity	Would need to attempt to add to next FY capital budget cycle, if funds were available.	Software, Network	04SW-04-NETW
NGFW Premium	Subscription for support	8	$ 559.21	$ 4,473.68	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	$ 3,352.08	Malware 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 Management Software	Central Management software	1	$ 5,499.51	$ 5,499.51	Allows for field firewalls to be centrally managed	Would need to attempt to add to next FY capital budget cycle, if funds were available.	System,Patch/Configuratio	005PM-00-PTCH
NGFW Central Management Support	Support for central management software	1	$ 1,810.77	$ 1,810.77	Support for central management of firewalls	Would need to attempt to add to next FY capital budget cycle, if funds were available.	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	$ 15,493.66	Existing firewall does not have SD-WAN feature.	Would need to attempt to add to next FY capital budget cycle, if funds were available.	Software,Network	04SW-00-PTCH
NGFW Advanced Threat Prevention	Subscription for firewall feature	8	$ 754.27	$ 6,034.16	Allows for 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	$ 0.00	0
Total	**0**	**$ 0.00**	**$0.00**	**0**

Document Uploads *top*

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

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

Application ID: 449672

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 Installation of WAN Switches at Headquarter location	4 weeks after receiving equipment
2	Configuration 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	Deployment of the NGFW Managment VM and initial configuration	2 months after receiving License for VM
5	Initial configuration of feild site firewalls - prepped centrally at main office	4 months after receiving Licensing and firewalls
6	Deployment and integration of new firewalls at 2 out of the 8 remote sites	6 months after receiving Licensing and firewalls
7	Deployment and integration of new firewalls at 4 out of the 8 remote sites	8 months after receiving Licensing and firewalls
8	Deployment and integration of new firewalls at 6 out of the 8 remote sites	10 months after receiving Licensing and firewalls
9	Deployment and integration of new firewalls at 8 out of the 8 remote sites	12 months after receiving LIcensing and firewalls

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

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)?
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 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 bad actor.
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)
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

☑ No

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP

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

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

This project could be scaled up to support additional information systems, but licensing typically covers a set amount of systems. The project allows IT staff to monitor and audit accounts and shared resources. The scope could expand or contract if we drastically increase or decrease our resource usage.

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

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

89512

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

☑ Build

□ Sustain

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

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

□ Yes

☑ No

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

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

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

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

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Directory Auditing Software License subscription	Software licensing for directory services auditing	1	$ 2,860.00	$ 2,860.00	This purchase will enhance WCSD's monitoring and auditing capabilities. The native 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 cyber attacks.	WCSD will sustain this project by incorporating this cost into the ongoing operating budget.	Software, Risk Management	04AP-04-RISK
Cloud Directory Auditing Software License	Software licensing for cloud directory services auditing	1	$ 995.00	$ 995.00	This purchase will enhance WCSD's monitoring and auditing capabilities. The native logging capabilities of windows operating systems are very limited and this software will allow for significantly improved visibility and log	WCSD will sustain this project by incorporating this cost into the ongoing operating budget.	Software, Risk Management	04AP-04-RISK

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

TRAINING COSTS

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

EXERCISE COSTS

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

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

Document Uploads *top*

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

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

Application ID: 448914

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

Logout | Browser

	Applicant Name	Washoe County School District
	Project Name:	WCSD Account and File Auditing Software 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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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
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)?
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.

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

Implement an email security solution to protect all users from internal and external email threats including malware, phishing, and business email compromise.

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
☑ No

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
□ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
This project will support ingress/egress, as well as intra-organization email security. This is critical because most email threats come from outside the organization, but internal threats, such as business email compromise, come from inside the organization (intra-org). This project will cover all staff and student accounts. Limiting implementation to just staff members, rather than including student accounts, would drastically degrade WCSD's capabilities in the event of a compromise of student accounts.

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

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

☑ Build
□ Sustain

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

□ Yes
☑ No

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

				$
				$
		0	0.00	$ 0.00

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Email Security Software License	Software licensing for email security product, including cloud portal and vendor support	75,000	$ 3.33	$ 249,750.00	$250,000 is the total cost for this licensing based on current estimates. This item will allow WCSD to implement an integrated email security suite for all accounts and mailboxes. Email compromise is a common vector for bad actors and often results in financial loss for victims, as well as serving as a springboard to compromise other organizations. If one entity in the State of Nevada gets compromised and they regularly work with others, they can serve as an avenue to compromise	WCSD will sustain this project through multiple mechanisms. This project will result in reallocated budget priorities and ensure that the level of continued support for these products are necessary. WCSD will potentially switch to other products due to cost savings.	Applications, Software AS	04AP-11-SAAS

					other organizations.
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
		75,000	$ 3.33	$ 249,750.00	

TRAINING COSTS

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

EXERCISE COSTS

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

Document Uploads top

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	FY22 Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy Payroll Regulation

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

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

Application ID: 448906

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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 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
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)?
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 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"

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
☑ No

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
□ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
This project could be scaled up to support MFA for the entire District staff or staff and students. The current system configuration and license uses minimal additional "signal intelligence factors" to make decisions on whether access should or should not be granted. Improvements will include higher tiers of licensing or integrations with existing tooling to register specific endpoints and applications in a much more firm "zero trust" methodology.

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

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

☑ Build
□ Sustain

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

□ Yes
☑ No

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

0.00

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
MFA Software License	Software licensing for MFA product including cloud portal and vendor support	700	$ 26.96	$ 18,872.00	$18,872 is the total cost for this licensing based on current estimates. This item will allow WCSD to implement MFA for all administrator accounts. Administrators can make changes to a computer, enable/disable security features, and install new software. Accounts with these permissions are a target for hackers/bad actors because of these elevated permissions. By securing these accounts with multiple factors (i.e. supplemental one-time codes), WCSD can prevent them from being used by a hacker who could have compromised or stolen a	WCSD will sustain this project through multiple mechanisms. It would reduce the number of administrators in the network to reduce licensing costs. WCSD can also remove legacy software that requires elevated permissions to run to reduce the overall license count used which would decrease costs. After exhausting both avenues, WCSD will allocate funding for this project to support ongoing licensing costs.	Device, Biometric Authent	05AU-00-BIOM

					user's passwords from any other 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	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

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

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

Document Uploads *top*

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

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

Application ID: 448910

Applicant Name	Washoe County School District
Project Name:	Multi-Factor Authentication (MFA) License
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		

*Please add additional rows as necessary for your project

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

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

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

Washoe County School District

WCSD Threat Intelligence System

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

$ 37,534.00 Requested

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
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)?
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 and infrastructure for a Cyber Threat Intelligence sharing platform. The intent will be to purchase a license for sandboxing services, an intelligence feed 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 sources. 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 organization is large and geographically-dispersed. However, WCSD has a relatively small IT department with technicians serving many schools at once. This project will allow WCSD 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 improvement based on continuous testing, evaluation, and structured assessments" by creating the infrastructure for continuous testing and assessment of systems in WCSD's environment.

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

This project aligns with 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 environment.

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

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." This system will actively assess WCSD's environment against threat intelligence platforms to ensure that WCSD has an accurate picture of the environment.
5. "Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity." This project will allow WCSD to adopt and use best practices because we will have enhanced visibility into the environment.

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. WCSD will acquire subscriptions to a hosted analysis platform and integrate workflows to analyze WCSD's environment against this feed of threat intelligence. This will help WCSD analyze the environment against threat intel sources. Next, WCSD will coordinate technology resources to feed other entities cyber threat intel platforms using information from the internal environment. This process is largely automated once established, but requires coordination across technology departments and distributed staff.

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

Implement a cyber threat intelligence platform to improve security posture, awareness, and community participation.

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

☑ No

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission

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

- ☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- ☐ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

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

This project could be scaled up or down depending on the integrations with third-party cyber threat intelligence platforms. It could integrate other sources or remove them and their associated limits to reduce scope and cost.

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

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

89512

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

- ☑ Build
- ☐ Sustain

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

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

- ☐ Yes
- ☑ No

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

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

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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

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

EQUIPMENT COSTS

Equipment Cost Name	**Line Item Description**	**Quantity**	**Unit Cost**	**Total**	**Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.**	**How would your organization sustain this project if grant funding was reduced or discontinued?**	**AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info**	**AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info**
Threat Intelligence License	Software licensing for MFA product including cloud portal and vendor support	1	$ 34,000.00	$ 34,000.00	$34,000 is the total cost for this licensing for cyber threat intelligence based on current estimates. This item would allow WCSD to implement broad-base scanning of internal infrastructure in a methodical feed. It would also allow WCSD to share this with other agencies when IT staff identifies sources of attack.	WCSD will sustain this project by identifying needs and determining if the level of support is necessary going forward. WCSD will maintain infrastructure costs going forward.	Data Acquisition	13IT-00-DACQ
Hosted Infrastructure	Hosted infrastructure	2	$ 1,767.00	$ 3,534.00	This provides the hosted infrastructure to support the system. It is where the actual software and connections to third-party intel sources would take place.	WCSD will review whether staff is needed to maintain redundant systems and maintain the infrastructure costs going forward.	Applications, Software AS	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		3	**$ 35,767.00**	**$ 37,534.00**				

TRAINING COSTS

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

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 449039

	Applicant Name	Washoe County School District
	Project Name:	WCSD Threat Intelligence Platform
	Project Funding Stream:	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		

*Please add additional rows as necessary for your project