Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

This project has a 2023 contingent application

City of Reno

Core Router Replacement

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

$ 144,854.24 Requested

Submitted: 8/31/2023 3:09:20 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

- [x] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

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.

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

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

Our Senior Network Analyst will rack, install and configure the new core routers.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

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.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes

- [x] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [ ] Yes
- [x] No

12. Describe the ways in which the project can be scaled or reduced 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. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from the sub-recipient address.
89501

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

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

						Describe how

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	the purchase (s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Router - managed - rack-mountable	Router	2	$ 9,617.09	$ 19,234.18	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.	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
Foundation Care Next Business Day Exchange Service - extended service a	Maintenance	2	$ 2,557.04	$ 5,114.08	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.	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
Power supply - hot-plug - 1800 Wa	Internal Parts/Modules	8	$ 1,781.92	$ 14,255.36	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.	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
Management Module - network management device	Internal Parts/Modules	2	$ 6,407.51	$ 12,815.02	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.	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
48 Port 1G 10G 25GbE	Internal Parts/Modules	2	$ 35,610.30	$ 71,220.60	This is a complete	All pieces of equipment are	Hardware, Computer,	04HW-01-

SFP28 v2 Extended Tables Module					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.	needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	Integ	INHW
48-port 1GbE Class 4 PoE and 4-port SFP56 v2 Module - switch	Internal Parts/Modules	2	$ 7,123.84	$ 14,247.68	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.	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
50GBase direct attach cable - 10 ft	Internal Parts/Modules	2	$ 349.28	$ 698.56	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.	All pieces of equipment are needed for redundancy and a complete solution. The complete solution is what follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
64/54XX FDN SUB 7Y	License and Subscription	2	$ 3,634.38	$ 7,268.76	Warranty and Subscription for seven years.	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.	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	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			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	☑	2022 Grant Milestone
Capabilities Assessment download template	☑	Capabilities Assessment

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

Application ID: 449758

	Applicant Name	City of Reno
	Project Name:	Core Router 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	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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

This project has a 2023 contingent application

City of Reno

Network and Security Assessment

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

$ 52,237.00 Requested

Submitted: 8/31/2023 2:20:42 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

Telephone	775-334-3105
Fax	
Web	reno.gov
EIN	886000201
UEI	TH74SE96JVC7
SAM Expires	

Director of Finance
Vicki Van Buren
vanburenv@reno.gov

Pre-Application *top*

1. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

- [ ] 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.
- [x] 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. (SLCGP: Appendix A)
Projects may align with more than one element.

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and 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.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.
- [ ] 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.

- [ ] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [x] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

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. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

The City of Reno IT Manager, Senior Network Engineer and Senior Cybersecurity Analyst will work in conjunction with the consultant engineers. The scope of work calls for a Network assessment:
• 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)

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

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.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [ ] Yes
- [x] No

12. Describe the ways in which the project can be scaled or reduced 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. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from the sub-recipient address.
89501

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

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

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

TRAINING COSTS

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

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			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 and Purchasing Procurement and Purchasing
Milestones download template	☑	2022 Grant Milestone
Capabilities Assessment download template	☑	Capabilities Assessment

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

Application ID: 449743

	Applicant Name	City of Reno
	Project Name:	Network Assessment
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

This project has a 2023 contingent application

City of Reno

Switch Replacement

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

$ 205,023.39 Requested

Submitted: 8/31/2023 3:09:53 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

- [x] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [x] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

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 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.

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

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

Our Senior Network Analyst will replace unsupported switches with the new hardware and configure each device.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

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.

7. Will you be retaining funds for Management & Administration (M&A)?
M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced 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. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from the sub-recipient address.
89501

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

- [x] Build
- [ ] Sustain

15. Is this request 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

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
48FP L2 Stck Cld-Mngd 48x GigE 740W PoE Switch	Switch	27	$ 5,433.70	$ 146,709.90	These are smaller replacement purchases, we could modify the project as needed.	The switch and maintenance/warranty follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
48FP Enterprise License and Support, 7YR	License and Subscription	27	$ 1,666.26	$ 44,989.02	Warranty and Subscription for seven years.	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.	Applications, Software as	04AP-11-SAAS
24P L2 Stck Cld-Mngd 24x GigE 370W PoE Switch	Switch	3	$ 3,403.87	$ 10,211.61	These are smaller replacement purchases, we could modify the project as needed.	The switch and maintenance/warranty follows NIST framework.	Hardware, Computer, Integ	04HW-01-INHW
24P Enterprise License and Support, 7YR	License and Subscription	3	$ 1,037.62	$ 3,112.86	Warranty and Subscription for seven years.	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.	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	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			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	☑	2022 Grant Milestone
Capabilities Assessment download template	☑	Capabilities Assessment

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

Application ID: 449759

	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

This project has a 2023 contingent application

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Clark County School District

Incident Response Planning and Tabletop Exercise

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

$ 68,750.00 Requested

Submitted: 8/29/2023 12:33:31 PM (Pacific)

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

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

Clark County School District

5100 W Sahara Ave
Las Vegas,
NV 89146
United States

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

Telephone 702-799-2273
Fax
Web
EIN 88 6000030
UEI SRBYQ7XFBYA6
SAM
Expires

Pre-Application *top*

1. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?
- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
- [x] Yes
- [ ] No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.
- [x] I understand and agree.

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

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.
- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and 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.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.
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. Project Implementation - 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.
See SLCGP: Appendix A for sample evidence of implementation.
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.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.
See SLCGP: Appendix A for examples of project outcome formats.

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

7. Will you be retaining funds for Management & Administration (M&A)?
M&A may be retained at up to 5% of the total cost of the project.
- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.
- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.
- [ ] Our agency has signed up for these services already
- [x] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?
- [ ] Yes
- [x] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
Can not be scaled due to the vendor package of an incident response plan and single tabletop exercise.

13. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.
- [x] Build
- [ ] Sustain

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

Line Item Detail Budget *top*

PLANNING COSTS

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

EQUIPMENT COSTS

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

TRAINING COSTS

	How would your organization	Describe how the purchase(s)	Do you plan to

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

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

Application ID: 449631

	Applicant Name	Clark County School District
	Project Name:	Incident response tabletop
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

This project has a 2023 contingent application

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Clark County School District

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: 8/29/2023 10:44:56 AM (Pacific)

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

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

Clark County School District

5100 W Sahara Ave
Las Vegas,
NV 89146
United States

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

Telephone 702-799-2273
Fax
Web
EIN 88 6000030
UEI SRBYQ7XFBYA6
SAM
Expires

Pre-Application *top*

1. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?
- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
- [x] Yes
- [ ] No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.
- [x] I understand and agree.

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

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.
- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and 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.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.
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. Project Implementation - 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.
See SLCGP: Appendix A for sample evidence of implementation.
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 waves the rest of the 500 critical accounts identified.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.
See SLCGP: Appendix A for examples of project outcome formats.

500 critical district employees will have multi factor authentication protected accounts.

7. Will you be retaining funds for Management & Administration (M&A)?
M&A may be retained at up to 5% of the total cost of the project.
- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.
- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.
- [ ] Our agency has signed up for these services already
- [x] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?
- [ ] Yes
- [x] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
Currently scaled down to most critical accounts totaling 500. Clark County School District has approx. 40,000 employees.

13. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.
- [x] Build
- [ ] Sustain

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

Line Item Detail Budget top

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.
Program Management	Contractor Cost: Program and Project management resources	150	175.00	$ 26,250.00	One time cost.	Planning, organizing and managing the completion for the project, while ensuring that it delivers the expected results on time, on budget, and within scope. 150 hours at $175 per hour.
				$		
				$		
				$		

					$		
					$		
					$		
					$		
					$		
					$		
					$		
					$		
					$		
					$		
					$		
		150		**175.00**	**$ 26,250.00**		

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
MFA	Multifactor Authentication – 500 account	1	$ 30,668.98	$ 30,668.98	Reduce funding to other district priorities.	Adopt and use best practices and methodologies to enhance cybersecurity – Multifactor Authentication	Applications, SAAS	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	**$ 30,668.98**	**$ 30,668.98**				

TRAINING COSTS

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

EXERCISE COSTS

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

Document Uploads *top*

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

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

Application ID: 449202

	Applicant Name	Clark County School District
	Project Name:	Multifactor Authentication
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

This project has a 2023 contingent application

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Ely Shoshone Tribe

Migrate to a .gov internet domain

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

$ 28,487.90 Requested

Submitted: 8/25/2023 2:47:19 PM (Pacific)

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

Additional Contacts
balaress@elyshoshonetribe.com

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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [x] Yes
- [ ] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

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

- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [x] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

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"

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. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

.

Sample Evidence of Implementation: The Ely Shoshone Trine operates only the .gov internet domain and does not use .com, .org, or any other domain.

Process

The Ely Shoshone Tribe will contract with a cyber security consultant to implement the Ely Shoshone Project - migrating 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

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

Migrate to a .gov internet domain.

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.

7. Will you be retaining funds for Management & Administration (M&A)?
M&A may be retained at up to 5% of the total cost of the project.

- [x] Yes
- [ ] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
$1,356.57

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [ ] Our agency has signed up for these services already
- [x] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [ ] Yes
- [x] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
This project can not be scaled down; the project is to migrate the existing elyshoshonetribe.com to .gov website and email address

13. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

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

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Windows Server	Windows Server and Licensing	1	$ 3,374.08	$ 3,374.08	This is a one-time purchase that doesn't require monthly expenses.	This will 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.	Hardware, Computer	04HW-01-INHW
O365 Licensing	G3 Licensing for 53 Users	53	$ 276.00	$ 14,628.00	This expense will be covered through normal budget planning.	This will 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.	Software as a Service	04AP-11-SAAS
Email Backup/Archiving	Email Backup/Archiving Software	53	$ 60.00	$ 3,180.00	This expense will be covered through normal budget planning.	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.	Software as a Service	04AP-11-SAAS
Email Spam Protection	Email Spam Protection Software	53	$ 60.00	$ 3,180.00	This expense will be covered through normal budget planning.	This provides protection against spam/viruses/phishing emails. Implement security protections commensurate with risk.	Software as a Service	04AP-11-SAAS
Email Migration Software	Used to migrate from Gmail to O365	53	$ 15.00	$ 795.00	This is a one-time purchase that doesn't require monthly expenses.	This will 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.	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	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this training with the State Training Officer?
O365 End User Training	Providing Training to all end users on how to use O365	13	$ 149.00	$ 1,974.25	This is a one time cost	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	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

		$	$		
		$	$		
		$	$		
		$	$		
		$	$		
		$	$		
		$	$		
		$	$		
	0	$ 0.00	$ 0.00		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 - Travel Policy
Payroll Policy	☑	General Payroll Policies
Procurement Policy	☑	Ely Shoshone - Procurement Policy
Milestones download template	☑	Ely SHoshone - Project Milestones
Capabilities Assessment download template	☑	Capabilities Assessment

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

Application ID: 448992

	Applicant Name	Ely Shoshone Tribe
	Project Name:	Migrate to a .gov internet domain
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Humboldt County Emergency Management

Firewall Threat Protection

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

$ 166,246.00 Requested

Submitted: 8/29/2023 9:57:44 AM (Pacific)

Project Contact
Carol Lynn
carol.lynn@humboldtcountynv.gov
Tel: 17753753195

Additional Contacts
mike.detullio@humboldtcountynv.gov

Humboldt County Emergency Management

50 West Fifth St
Winnemucca, NV 89445
United States

County Manager
Dave Mendiola
dave.mendiola@humboldtcountynv.gov

Telephone	17753753195
Fax	
Web	
EIN	88 6000086
UEI	LWU1E6XDTBK7
SAM Expires	

Pre-Application *top*

1. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [x] Yes
- [ ] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [x] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [x] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

- [x] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [x] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [x] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

We would like to purchase a pair of high availability firewalls. This will allow our backup datacenter and internet connection to be made available to our users at a high level of security. We will be able to monitor applications and their usage, monitor network activity, exercise industry best practices as they relate to cybersecurity. Being our disaster recovery site, these firewalls will also provide for continuity of operations at the same or better level of security at our primary datacenter.

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

Humboldt County's Technology Services Department will plan for, configure, and deploy the firewalls at our disaster recovery site. Before the firewalls arrive, we will have documented the necessary firewall policies, web content filtering policies, and routing structure. Upon their arrival, we will configure the firewalls and schedule deployment into a test environment, followed shortly by a move to the production environment.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

Our disaster recovery site will be protected by state-of-the-art cybersecurity appliances that assist in a safe continuity of operations should be experience a failure at our primary datacenter.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?

Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

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

Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.

We could implement a single firewall rather than an HA pair. However, this would reduce the resiliency of the project outcome and could affect the agency negatively should there be a failure in the primary firewall at the DR site.

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

The project location could be distinct from the sub-recipient address.

89445

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

- [x] Build
- [ ] Sustain

15. Is this request deployable to other jurisdictions?

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

				$			
				$			
				$			
				$			
				$			
				$			
		0	0.00	$ 0.00			

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Firewalls	High availability firewall	2	$ 83,123.00	$ 166,246.00	This is a one time cost, with exception of the annual licensure, which will be absorbed by the TSD budget.	These firewalls are what will allow us to achieve the desired project outcome as outlined in the Application Questions.		
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				

			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		2	$ 83,123.00	$ 166,246.00			

TRAINING COSTS

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

EXERCISE COSTS

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

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

Document Uploads *top*

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

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

Application ID: 447811

	Applicant Name	Humboldt County
	Project Name:	Firewall Threat Protection
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
1	Procurement	Product order complete 3 weeks after award
2	Installation	Installation complete 6 weeks after product receipt
3	Evaluation	Testing complete 3 weeks after installation
4	Implementation	Product put in service after successful testing
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Nevada Secretary of State

Secretary of State Project Orion-Switch Rack

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

$ 268,000.00 Requested

Submitted: 8/30/2023 11:56:39 AM (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 88-6000022
UEI
SAM
Expires

Pre-Application *top*

1. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.
- [ ] 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.

- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

The Secretary of State is modernizing legacy systems through a series of projects within Orion portfolio. One of the main objectives is to enhance security protection across all platforms that are utilized by constituents across the state and local and state governments. The Switch rack expansion with servers is required in our outsourced data center and is necessary to accommodate the new systems coming online for project Orion. To ensure the continuity of operation the switch rack expansion with servers will maintain even spacing between equipment, encouraging ventilation, and reducing the need for external cooling. In the event of a cybersecurity incident the racks allow for the equipment to be as accessible as possible. Additionally, this will organize the equipment to ensure that ongoing Maintenace is easy. This is a five-year plan that includes the racks the expansion, storage, power, and hosting of the servers.

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

The rack expiation and the servers will be set up and maintained by the switch facility.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

This will allow for the Secretary of State to move forward with other cybersecurity initiatives to support project Orion. With the new technologies coupled with the legacy systems we need to ensure their security this project will enable us to do that.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?

Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

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

Please view SCLGP: Appendix G for additional information on these services and memberships.

- [ ] Our agency has signed up for these services already
- [x] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [ ] Yes
- [x] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.

Due to the technologies being brought on and the legacy systems currently in existence we are unable to reduce or scale down this project.

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

The project location could be distinct from the sub-recipient address.

89706

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

- [x] Build
- [ ] Sustain

15. Is this request deployable to other jurisdictions?

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Switch Rack/Server Expansion	This is a five-year plan for storage and maintenance	1	$ 268,000.00	$ 268,000.00	The organization will be able to sustain this by including this as a line item in the budget moving forward.	This will ensure if a cybersecurity event happens servers are easily accessible and easy to maintain.	Hardware, Computer, Integ	04HW-01-INHW
				$				
				$				
				$				

			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		1	$ 268,000.00	$ 268,000.00			

TRAINING COSTS

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

EXERCISE COSTS

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

		$	$		
		$	$		
		$	$		
		$	$		
		$	$		
		$	$		
		$	$		
	0	$ 0.00	$ 0.00		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	☑	Purchasing Policy
Milestones download template	☑	NV SOS Milestones
Capabilities Assessment download template	☑	

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

Application ID: 449037

	Applicant Name	Nevada Secretary of State
	Project Name:	Project Orion
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase of Switch Racks and Servers	1-May
2		
3		
4		
5		
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

Will request updated Milestones if funded, to include installation and deployment of switch racks and servers - AJ 09/08/23

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Nye County

Nye County Cybersecurity Incident EOC upgrade

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

$ 2,835.00 Requested

Submitted: 8/28/2023 3:26:59 PM (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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?
- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
- [x] Yes
- [ ] No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.

You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.

See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?

A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [x] Yes
- [ ] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

3. Please select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)

Projects may align with more than one element.

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and 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.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by

NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

- [x] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [x] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

The Cyber Security Incident Response Plan for Nye County's Information Technology Department dictates that in the event of a major cyber security incident, the Emergency Operations Center (EOC) at Nye County DEM in Pahrump will become the base of operations for the response to the incident. This will enable the IT department to have immediate access to elected and appointed County leadership, Department Heads and DEM staff in a single, secure location to provide timely decision making and response activities in order to ensure continuity of government operations as well as continuity of communications. To ensure a high level of security for the electronics, radios and other communications equipment that will need to be located at the EOC, it is necessary to enhance surveillance capabilities in and around the DEM/EOC complex.

To that end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the DEM complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for constant monitoring and access control.

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

Nye County IT will obtain cost estimates for indoor and outdoor security cameras. 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 and Facilities Management will install the security cameras. Upon completion of the 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.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

Increased safety/security and access control at Nye County's EOC for elected and appointed officials, IT Staff and DEM/EOC Staff in the event of a major cybersecurity incident.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [x] Yes
- [ ] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
$135.00

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [x] Yes
- [ ] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
If necessary, we can reduce the number of camera's requested, and delete M&A request.

13. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.
5% M&A	M&A	1	$ 135.00	$ 135.00	Would not be required.	5% M&A
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		1	**$ 135.00**	**$ 135.00**		

EQUIPMENT COSTS

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

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Indoor/Outdoor Security Cameras	Security Cameras	1	$ 2,000.00	$ 2,000.00	Seek alternate grant funding	Enhanced safety for continuity of operations	Systems, Video Assessment	14SW-01-VIDA
60" Wall mounted display monitor	Monitor and wall mount	1	$ 700.00	$ 700.00	Seek alternate grant funding	Enhanced safety for continuity of operations	Display, Video	04MD-03-DISP
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		2	**$ 2,700.00**	**$ 2,700.00**				

TRAINING COSTS

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

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			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 FY22 SLCGP #2 Grant Milestones
Capabilities Assessment download template	☑	Nye County FY22 SLCGP Capabilities Assessment

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

Application ID: 449319

	Applicant Name	Nye County DEM/IT
	Project Name:	Nye County Cybersecurity Incident EOC Upgrade
	Project Funding Stream:	FY 2022 SLCGP #2
	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	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

Nevada Office of the Military, Division of Emergency Management

This project has a 2023 contingent application

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Nye County

Nye County Firewall Upgrade

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

$ 62,219.49 Requested

Submitted: 8/23/2023 8:25:41 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority

businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [x] Yes
- [ ] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

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

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats,

such as through cybersecurity hygiene training.

- [x] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [x] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.
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. Project Implementation - 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.
See SLCGP: Appendix A for sample evidence of implementation.
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.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.
See SLCGP: Appendix A for examples of project outcome formats.
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.

7. Will you be retaining funds for Management & Administration (M&A)?
M&A may be retained at up to 5% of the total cost of the project.

- [x] Yes
- [ ] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
$2,963

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [ ] Yes
- [x] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
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. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget top

PLANNING COSTS

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

					discontinued?	Application Questions section.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	**$ 0.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.
5% M&A	M&A	1	$ 2,963.00	$ 2,963.00	Would not be necessary	The firewall upgrade, consolidation, and addition of the logging server 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	How would your organization sustain this project if grant funding was reduced or	Describe how the purchase(s) within this element tie into the project as described in the Application	AEL Name	AEL Number

					discontinued?	Questions section.		
Firewall appliance	Firewall appliance	1	$ 13,176.47	$ 13,176.47	Seek alternate grant funding	Update current firewall and consolidate current web filter and add extended logging	Firewall, network	05NP-00-FWAL
Firewall advanced threat protection subscription	Firewall subscription	1	$ 46,080.02	$ 46,080.02	Seek alternate grant funding	Provide advanced threat protection, energize updates, instant replacement, malware protection, advanced remote, insights subscriptions for 36 months	Firewall, network	05NP-00-FWAL
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		2	**$ 59,256.49**	**$ 59,256.49**				

TRAINING COSTS

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

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			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 FY22 SLCGP Grant Milestones
Capabilities Assessment download template	☑	Nye County FY22 SLCGP Grant Capabilities Assessemtn

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

Application ID: 448162

	Applicant Name	Nye County DEM/IT
	Project Name:	Nye County Firewall Upgrade
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Washoe County Emergency Management & Homeland Security Program

Washoe County Second Judicial Court: Audit, Remediation, & Network Build Up

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

$ 77,000.00 Requested

Submitted: 8/31/2023 4:30:20 PM (Pacific)

Project Contact
Kelly Echeverria
KEcheverria@washoecounty.us
Tel: 7753375859

Additional Contacts
jnadams@washoecounty.gov,
chris.long@washoecourts.us

Washoe County Emergency Management & Homeland Security Program

5195 Spectrum Blvd
Reno, NV 89509

Program Coordinator
Francisco Ceballos
Fceballos@washoecounty.gov

Telephone	7753994811
Fax	
Web	www.readywashoe.com
EIN	262800962
UEI	GPR1NY74XPQ5
SAM Expires	11/10/2021

Pre-Application *top*

1. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE

and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

- [ ] 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.
- [x] 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. (SLCGP: Appendix A)
Projects may align with more than one element.

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.

- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

The Second Judicial District Court (SJDC) is seeking funding to enhance the critical judicial network and database systems. As a separate branch of government, SJDC is funded within Washoe County but must maintain completely separate networks and database systems from the Executive Branch. The SJDC plans to implement this funding to improve and continuity test and evaluate the security of its network by hiring a cyber security auditing company to take a deep dive into our network, applications, and security and improve our posture and standard to harden against Cyber-attacks and intrusions. This professional assessment will include an assessment of our current state in accordance with National Institute of Standards and Technology (NIST) standards and framework. The SJDC will also utilize this funding to hire a professional cyber security firm to evaluate our active directory and cloud security and then provide remediation to harden security standards. Additional Next Generation Firewall interfaces and firewalls will also be added to allow the Court network traffic to be segmented, filtered, and inspected against cyber-attacks and intrusions. Additional network switches would be purchased to replace out-of-date and insecure switches. If awarded, 36% of funding will benefit rural Washoe County.

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

The SJDC, Court Tech team will be responsible for acquiring necessary quotes, purchasing the equipment, and hiring the assessment teams/contractors in accordance with the milestone timeline. This project will be led by Court Tech Manager, Celina Galindo. Assessment review and follow-up will be conducted by all and reported to the Second Judicial District Court Leadership Team.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

The Second Judicial District Court strives to provide the timely, fair, and efficient administration of justice under the law, in a matter that instills and sustains the public's confidence in the judicial system. In order to provide this justice, a strong, safe, network backbone must be in place. Without the security of the justice documents, the public's confidence would be eliminated. With this funding, SJDC strives to enhance cybersecurity and continue to provide faith in the justice system for everyone.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
If necessary, the Second Judicial District Court could eliminate Firewall and Interfaces assessment, but that would keep that area of the network at a higher risk for cyber-attacks and intrusions.

13. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from the sub-recipient address.
89501

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

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget top

PLANNING COSTS

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

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.
Professional Network Assessment	Cyber security auditing company to take a deep dive into our network, applications, and security and improve our posture and standard to harden against Cyber-attacks and intrusions.	1	10,000.00	$ 10,000.00	SJDC would submit a request to the County for additional budget authority to fund this assessments. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available	This would include to assess our current state in accordance with NIST Standards and framework.
2. Active Director Security Audit and Remediations	Engage services with a professional Cyber security firm to evaluate our active directory and cloud security then provide remediation to harden security standards	1	12,000.00	$ 12,000.00	SJDC would submit a request to the County for additional budget authority to fund this assessments. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available	Harden security standards
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		2	**22,000.00**	**$ 22,000.00**		

ORGANIZATION COSTS

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

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Addition Next Generation Firewall	3. Addition Next Generation Firewall interfaces to bring all network traffic to be segmented, filtered, inspected against cyber-attacks and intrusions	1	$ 10,000.00	$ 10,000.00	SJDC would submit a request to the County for additional budget authority to carry out this project. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available.	This add-on provides additional insight into cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.	Firewall network	05NP-00-FWAL
Additional Next Generation Firewalls	4. Additional Next Generation Firewalls bring all bring all network traffic to be segmented, filtered, inspected against cyber-attacks and intrusions.	1	$ 10,000.00	$ 10,000.00	SJDC would submit a request to the County for additional budget authority to carry out this project. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available.	This add-on provides additional insight into cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.	Firewall network	05NP-00-FWAL
Internet and Network Content filtering	5. Internet and Network Content filtering to increase Cyber Security.	1	$ 15,000.00	$ 15,000.00	SJDC would submit a request to the County for additional budget authority to carry out this project. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available.	This add-on provides additional insight into cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.	Firewall network	05NP-00-FWAL
Network switches	6. Network switches to replace out of date and insecure switches	1	$ 20,000.00	$ 20,000.00	SJDC would submit a request to the County for additional budget authority to carry out this project. If denied, SJDC would also seek grant funding if	This add-on provides additional insight into cybersecurity related activities and issues to	Firewall network	05NP-00-FWAL

					available from the State of Nevada, Administrative Offices of the Court if available.	enhance cyber-security at Second Judicial District Court.	
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		4	$ 55,000.00	$ 55,000.00			

TRAINING COSTS

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

EXERCISE COSTS

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

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

Document Uploads *top*

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

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

Application ID: 449722

	Applicant Name	Second Judicial District Court
	Project Name:	SJDC's Cyber-Security Audit and Network Build Up
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
1	Acceptance of Funding by Washoe County Board of County Commissioners (BCC), Setting up of separate grant tracking of fiscal expenses within financial system	Assume award notification by 1/1/2024. Within 90 days of receipt of Award notification. By end of March 2024
2	Obtain necessary quotes from vendors for audit services and network switches	within 90 days of receipt of Award notification. By end of March 2024
3	Issue of Purchase Orders for Audits and equipment	within 45 days of acceptance of funds by BCC. By mid May 2024
4	Completion of Audits by selected contractors	within 90 days of issue of PO. By end of Aug 2024
5	Internal Review of Audit recommendation and implementation of possible updates	within 60 days of ocmpletion of audits. By end of Oct 2024
6	Install of equipment	within 45 days of receipt of equipment. may vary depending on product backlog/shipment issues
7	Final review and report of project to DEM	By end of December 2024
8		
9		
10		

*Please add additional rows as necessary for your project

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Washoe County Emergency Management & Homeland Security Program

Washoe County Second Judicial District Court: Cyber Secure Wireless and Filtering

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

$ 85,900.00 Requested

Submitted: 8/31/2023 4:23:04 PM (Pacific)

Project Contact
Kelly Echeverria
KEcheverria@washoecounty.us
Tel: 7753375859

Additional Contacts
jnadams@washoecounty.gov,
chris.long@washoecourts.us

Washoe County Emergency Management & Homeland Security Program

5195 Spectrum Blvd
Reno, NV 89509

Program Coordinator
Francisco Ceballos
Fceballos@washoecounty.gov

Telephone	7753994811
Fax	
Web	www.readywashoe.com
EIN	262800962
UEI	GPR1NY74XPQ5
SAM Expires	11/10/2021

Pre-Application *top*

1. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE

and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.
See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?
A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

- [ ] 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.
- [x] 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. (SLCGP: Appendix A)
Projects may align with more than one element.

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and 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.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] 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.

- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.
The Second Judicial District Court (SJDC) is seeking funding to be able to enhance and secure their wireless network systems. As a separate branch of government, SJDC is funded within Washoe County but must maintain completely separate networks and database systems from the Executive Branch. SJDC plans to implement this funding to improve its cyber-secure wireless and filtering systems by purchasing wireless access points since wireless points are a common target and known point for cyber intrusion and exploitation. In addition to purchasing the access points, SJDC would like to purchase an internet proxy for cyber security with zero trust access. The last added component to enhance the security would be additional security for the end users. By purchasing end-point protection for all users against malware, viruses, and anomalies with 24/7 monitoring, the SJDC Court Tech team could be notified immediately upon a potential risk or breach of security and be able to close off that user prior to the risk of infecting the whole system. If awarded, 36% of funding will benefit rural Washoe County.

5. Project Implementation - 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.
See SLCGP: Appendix A for sample evidence of implementation.
SJDC, Court Tech team will be responsible for acquiring necessary quotes, and purchasing the equipment. This project will be led by Court Tech Manager, Celina Galindo. Assessment review and follow up will be conducted by all and reported to the Second Judicial District Court Leadership Team.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.
See SLCGP: Appendix A for examples of project outcome formats.
Second Judicial District Court strives to provide the timely, fair, and efficient administration of justice under the law, in a matter that instills and sustains the public's confidence in the judicial system. In order to provide this justice, a strong, safe, network backbone must be in place. Without the security of the justice documents, the public's confidence would be eliminated. With this funding, SJDC strives to enhance the wireless cybersecurity to provide faith in the justice system for everyone.

7. Will you be retaining funds for Management & Administration (M&A)?
M&A may be retained at up to 5% of the total cost of the project.
- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?
If you are not retaining M&A, please enter "N/A"
N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
If necessary, the Second Judicial District Court could eliminate part of the equipment requests, but that would decrease the level of security for the Court and keep that area of the network at a higher risk for cyber-attacks and intrusions.

13. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from the sub-recipient address.
89501

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

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
New Wireless Access Points	Wireless systems are known point for cyber	42	$ 950.00	$ 39,900.00	SJDC would submit a request to the County for additional budget authority to	This add-on provides additional insight into	Hardware, computer	04HW-01-INHW

	intrusion and exploitation.				carry out this project. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available.	cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.		
Internet Proxy	Internet Proxy for Cyber Security (Zero trust access)	1	$ 20,000.00	$ 20,000.00	SJDC would submit a request to the County for additional budget authority to carry out this project. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available.	This add-on provides additional insight into cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.	Hardware, computer	04AP-11-SAAS
End point protection	End point protection for all users to protect against Malware, viruses, and anomalies with 24/7 monitoring.	1	$ 26,000.00	$ 26,000.00	SJDC would submit a request to the County for additional budget authority to carry out this project. If denied, SJDC would also seek grant funding if available from the State of Nevada, Administrative Offices of the Court if available.	This add-on provides additional insight into cybersecurity related activities and issues to enhance cyber-security at Second Judicial District Court.	System, Security	05NP-00-SIEM
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		44	**$ 46,950.00**	**$ 85,900.00**				

TRAINING COSTS

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

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

EXERCISE COSTS

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

Document Uploads *top*

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

download template

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

Application ID: 449721

	Applicant Name	Second Judicial District Court
	Project Name:	SJDC's Cyber-Secure Wireless and Filtering
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
1	Acceptance of Funding by Washoe County Board of County Commissioners (BCC), Setting up of separate grant tracking of fiscal expenses within financial system	Assume award notification by 1/1/2024. Within 90 days of receipt of Award notification. By end of March 2024
2	Obtain necessary quotes from vendors for all equipment	within 90 days of receipt of Award notification. By end of March 2024
3	Issue of Purchase Orders for equipment	within 45 days of acceptance of funds by BCC. By mid May 2024
4	Install of equipment	within 90 days of receipt of equipment. may vary depending on product backlog/shipment issues.
5	Final review and report of project to DEM	By end of December 2024
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

Nevada Office of the Military, Division of Emergency Management

This project has a 2023 contingent application

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Washoe County School District

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 10:31:38 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.

You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.

See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?

A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

3. Please select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)

Projects may align with more than one element.

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.

- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

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. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

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.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

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

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?

Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes

- [x] No

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

Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced 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. Project Location: Provide the 5-digit zip code where the project will be executed.

The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

15. Is this request deployable to other jurisdictions?

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Directory Auditing Software License Subscription	Software licensing for directory services auditing	1	$ 2,515.00	$ 2,515.00	WCSD will sustain this project by incorporating this cost into an	This purchase will enhance WCSD's monitoring and auditing capabilities. The native logging	Software, Risk Management	04AP-04-RISK

					ongoing operating budget.	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.		
Cloud Directory Auditing Software License	Software licensing for cloud directory services auditing	1	$ 995.00	$ 995.00	WCSD will sustain this project by incorporating this cost into our ongoing operating budget.	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.	Software, Risk Management	04AP-04-RISK
File Directory Auditing Software	Software licensing for file server auditing	1	$ 2,995.00	$ 2,995.00	WCSD will sustain this project by incorporating this cost into our ongoing operating budget.	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.	Software, Risk Management	04AP-04-RISK
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		3	**$ 6,505.00**	**$ 6,505.00**				

TRAINING COSTS

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

EXERCISE COSTS

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

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

Application ID: 448882

	Applicant Name	Washoe County School District
	Project Name:	WCSD Account and File Auditing Software License
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Washoe County School District

WCSD Cloud Assessment and Response System

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

$ 6,912.00 Requested

Submitted: 8/28/2023 10:32:24 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?
- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
- [x] Yes
- [ ] No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.

You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.

See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?

A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

- [ ] 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.
- [x] 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. (SLCGP: Appendix A)

Projects may align with more than one element.

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.

- [ ] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

This project is to purchase and implement a cloud-based assessment and response system that will supplement Washoe County School District's existing endpoint detection and response system. This system will be used to perform broad queries against endpoints for threat hunting and artifact collection. These capabilities will enable WCSD's IT security staff to identify a breach and immediately respond thereto. This will assist WCSD IT department to overcome key weaknesses in existing tooling. It will be built on a cloud infrastructure provider using open source tooling. Putting the system on a third-party's cloud infrastructure will allow the system to reach systems even if they were deployed across the District or on other public networks. This system will be supported using open-source and free tooling. From a technical perspective, this will accomplish Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments" because the tooling supports broad queries against endpoints and can support some incident response capabilities. WCSD is large, geographically-dispersed public entity. However, WCSD has a relatively small IT department. Performing these functions through any other means is technically impractical with current constraints and limitations. This software is necessary to support WCSD's daily operations, and provide a safe and secure learning environment for WCSD's 62,000 students, including those in rural areas of Washoe County.

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

This project will be implemented by internal IT department staff. The third-party cloud provider will support hosting. The tooling itself is not supported by a third-party vendor and relies on free and open source tools. The work for this project is performed in centralized consoles and does not require on-hands installation of new equipment, systems, or software.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

Implement a cloud-based threat hunting and response platform to assess the security posture of all WCSD systems on internal and external networks.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?

Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.
This project can be scaled up or down by adding or removing hosts from the cloud provider. The front-end is a load balancer that pushes traffic to a back-end system. This architecture allows WCSD's IT department to add more load-balancers and back-end resources to support threat hunting and response actions.

13. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

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

Cloud Infrastructure	Cloud infrastructure consumption costs, including computing and storage resources, cloud portal, and vendor support.	1	$ 6,912.00	$ 6,912.00	WCSD will sustain this project through multiple mechanisms. WCSD may reallocate budget priorities and ensure that the level of continued support for these products is necessary. WCSD could potentially switch to other cloud services or house these capabilities in the internal DMZ due to potential cost savings. In the current configuration, computer and networking resources are included and take unique advantage of cloud provider capabilties.	$6,912 is the total cost for the cloud-provider resources to host the system. The system relies on open source tooling to query distributed endpoints. This is very useful for threat hunting and incident response because WCSD can prioritize and collect artifacts (data, metrics, files) from distributed systems.	Applications, Software as	04AP-11-SAAS
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		1	**$ 6,912.00**	**$ 6,912.00**				

TRAINING COSTS

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

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

EXERCISE COSTS

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

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

Application ID: 448898

	Applicant Name	Washoe County School District
	Project Name:	WCSD Cloud Assessment and Response System
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
1	Purchase hosted resources	15 days after award
2	Access portal and provision resource	30 days after award
3	Perform endpoint installation components	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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

This project has a 2023 contingent application

Washoe County School District

Email Security System

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

$ 249,750.00 Requested

Submitted: 8/28/2023 10:32:04 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.

You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.

See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?

A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

3. Please select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)

Projects may align with more than one element.

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.

- [ ] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

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. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

This project will be implemented by internal IT department staff. Because WCSD's enterprise email system is hosted, the project 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 the organization's email system. This work will be performed in a centralized console and does not require on-hands installation of new equipment, systems, or software.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

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

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?

Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes

- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced 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. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
Email Security Software License	Software licensing for email security	75,000	$ 3.33	$ 249,750.00	WCSD will sustain this project through multiple	$250,000 is the total cost for this licensing based on current estimates. This item	Applications, Software as	04AP-11-SAAS

	product, including cloud portal and vendor support				mechanisms. This may include reallocated budget priorities to ensure that the level of continued supports for these products are necessary.	will allow WCSD to implement an integrated email security suite for all accounts and mailboxes. Email compromise is a common vector for bad actors and often results in financial loss for victims, as well as serving as a springboard to compromise other organizations. If one entity in the State of Nevada gets compromised and they regularly work with others, they can serve as an avenue to compromise other organizations.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		75,000	**$ 3.33**	$ 249,750.00		

TRAINING COSTS

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

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

EXERCISE COSTS

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

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

Application ID: 448887

	Applicant Name	Washoe County School District
	Project Name:	WCSD Email Security System
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Washoe County School District

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 10:30:32 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?

- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.

You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.

See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?

A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

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

3. Please select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)

Projects may align with more than one element.

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.

- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

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. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

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.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

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

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?
Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by 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).
Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced 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. Project Location: Provide the 5-digit zip code where the project will be executed.
The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

Line Item Detail Budget top

PLANNING COSTS

	How would your organization	Describe how the purchase(s)

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	sustain this project if grant funding was reduced or discontinued?	within this element tie into the project as described in the Application Questions section.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	0.00	$ 0.00		

ORGANIZATION COSTS

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

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	AEL Name	AEL Number
MFA software	Software licensing for	700	$ 26.96	$ 18,872.00	WCSD will sustain this project through	$18,872 is the total cost for this licensing project.	Device, Biometric	05AU-00-BIOM

license	MFA product, including cloud portal and vendor support.				multiple mechanisms. The project will reduce the number of administrators in the network to reduce licensing costs. WCSD can also remove legacy software that requires elevated permissions to reduce the overall license count used. This will decrease long-term costs. After exhausting both avenues, WCSD will allocate funding for this project to support ongoing licensing costs.	This resource 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), IT staff can prevent the accounts from being used by a hacker who could have compromised or stolen a user's passwords from other means (malware, phishing, third-party breach, etc.). This will make the network significantly more resilient to cyber attacks and adds an additional layer of security across the entire network.	Authent
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		700	**$ 26.96**	$ 18,872.00			

TRAINING COSTS

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

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

EXERCISE COSTS

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

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

Application ID: 448671

	Applicant Name	Washoe County School District
	Project Name:	Multi-Factor Authentication (MFA) License
	Project Funding Stream:	FY 2022 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

Nevada Office of the Military, Division of Emergency Management

FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 8/31/2023

Washoe County School District
WCSD Penetration Test

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

$ 16,081.00 Requested

Submitted: 8/28/2023 10:31:10 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. To qualify for this grant you must be a state, territory, local, or tribal government (SLCGP: C.1). Are you a state, territory, local, or tribal government?
- [x] Yes
- [ ] No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk (SCLGP: A.10.b). Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).
- [x] Yes
- [ ] No

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

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 200.322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of Emergency Management (DEM) in advance of the procurement.

You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

- [x] I understand and agree.

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

- [x] I understand and agree.

6. Entities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please acknowledge your understanding and agreement of this requirement.

See SLCGP: C.4 for more information.

- [x] I understand and agree.

Application Questions *top*

1. Is this agency within a rural area?

A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)

- [ ] Yes
- [x] No

2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)

- [ ] 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.
- [x] 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. (SLCGP: Appendix A)

Projects may align with more than one element.

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and 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.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.
- [ ] 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.

- [ ] 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.
- [ ] 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.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity 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. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.

This project is to perform a "known compromise" penetration test on the Washoe County School District (WCSD) network. A penetration test is an active test of a network where a tester attempts to exploit weaknesses and vulnerabilities in a network based on what they discover is actively in use. In a "known compromise" test, the penetration tester starts with a foothold established in the network and more closely mirrors what an actual bad actor would discover when compromising an internal computer. The proposed test will involve testing at WCSD's central IT office, as well as at an individual school. This test will help IT internal staff understand and prioritize remediations that will help understand the current cybersecurity posture and areas for improvement, while also enhancing network preparation, response, and resilience in the event of a legitimate cyber breach.

5. Project Implementation - 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.

See SLCGP: Appendix A for sample evidence of implementation.

WCSD will coordinate this penetration test internally and work with a third-party vendor to perform the test. The test will be specifically scoped to encompass two separate sites within the WCSD's enterprise network. This will ensure that the project and test is realistic and based on "real world" scenarios. The third-party contractor will perform the actual work. While we have an internal IT security staff, the intent is to make sure that the test most directly mirrors a legitimate adversary, their perspective, and capabilities. Performing the test internally would prevent IT staff from understanding how the adversary perceives our environment.

6. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.

See SLCGP: Appendix A for examples of project outcome formats.

WCSD will improve preparation, response, and resilience of information systems, applications, and user accounts owned or operated by WCSD against cybersecurity risks and cybersecurity threats by understanding an adversary's perspective.

7. Will you be retaining funds for Management & Administration (M&A)?

M&A may be retained at up to 5% of the total cost of the project.

- [ ] Yes
- [x] No

8. If retaining M&A, what is the amount you will retain?

If you are not retaining M&A, please enter "N/A"

N/A

9. 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?

Please see the EHP Guidance attachment for more information on EHP reviews.

- [ ] Yes
- [x] No

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

Please view SCLGP: Appendix G for additional information on these services and memberships.

- [x] Our agency has signed up for these services already
- [ ] Our agency has not yet signed up for these services, but understand we will be required to sign up for them if our project is awarded

11. Is this project scaleable? Can any part of it be reduced?

- [x] Yes
- [ ] No

12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.

This project is currently scoped to two WCSD sites - the administration facility and an individual school. This will inform follow-up efforts for making WCSD more resilient to cyber threats. The project could be scaled up by adding additional sites and including more advanced attacker techniques like dropping removable drives, physical penetration tests, cloud assessment, wi-fi based attacks, or adding an external assessment. The project could includes a re-look to ensure that vulnerabilities have been fixed and could be reduced to eliminate the re-look if that was necessary.

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

The project location could be distinct from 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.

- [x] Build
- [ ] Sustain

15. Is this request deployable to other jurisdictions?

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

- [ ] Yes
- [x] No

Line Item Detail Budget *top*

PLANNING COSTS

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

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

ORGANIZATION COSTS

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

EQUIPMENT COSTS

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

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

TRAINING COSTS

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

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	How would your organization sustain this project if grant funding was reduced or discontinued?	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	Do you plan to coordinate this exercise with the State Exercise Officer?
Penetration Test	Assumed compromise penetration test and follow-up evaluation.	1	$ 16,081.00	$ 16,081.00	Penetration tests are meant to be temporal and integrated into overall vulnerability management efforts. This project will support a current state assessment	This project will support the all-inclusive penetration test. This test will provide a better understanding of how the network is	no

				that will allow WCSD to prioritize and remediate risks. This is not an ongoing project and will be evaluated again based on future needs.	vulnerable to attackers using actual attacker tradecraft. It is the best representation of our true cyber risk that can be performed.	
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
			$ $			
		1	**$ 16,081.00** $ 16,081.00			**0**
Total		**1**	**$ 16,081.00** $16,081.00			**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	☑	Penetration Test milestones
Capabilities Assessment download template	☑	WCSD capabilities assessment

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

Application ID: 448865

	Applicant Name	Washoe County School District
	Project Name:	Penetration Test
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
1	Perform initial coordination with contractor	30 days after award
2	Plan and scope the assessment	45 days after award
3	Receive assessment-specific equipment from	60 days after award
4	Perform assessment	70 days after award
5	Review initial findings	90 days after award
6	Implement changes	120 days after award
7	Perform secondary evaluation	130 days after award
8	Perform final review	150 days after award
9		
10		

*Please add additional rows as necessary for your project