

Email This Preview Save as PDF Print Close Window A A V

Powered by ZoomGrants™ and

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 t	tribal government (S	LCGP: C.1). Are y	ou a state,
territory, local, or tribal government?				

✓ 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).

Yes

□ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. ✓ 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 als 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.
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 eplacement 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 emprove 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 0, 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 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
is. 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 lisaster.
 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

	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 No
	In 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 requirementCyber Hygiene Services Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can 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 reports and ad-hoc alerts. To register for these services, email vulnerability info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services - SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org). Our agency has not yet signed up for these services, but u
•	11. Is this project scaleable? Can any part of it be reduced? ☐ Yes ☑ 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
1	14. Build or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current level. ☑ Build ☐ Sustain
,	15. Is this 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
ine It	em Detail Budget <u>top</u>

✓ No

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	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 T	otal	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?	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 reprioritize what we will accomplish this year with regards to infrastructure and security.	and a complete solution. The complete	Hardware, Computer, Integ	04HW- 01- INHW
Foundation Care Next Business Day Exchange Service - extended service a	Maintenance	2	\$ 2,557.04	т.	This is a complete replacement of the core router, if the funds are not available we would have to reprioritize what we will accomplish this year with regards to infrastructure and security.	and a complete solution. The complete	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	and a complete solution. The complete	Hardware, Computer, Integ	04HW- 01- INHW
Management Module - network management device	Internal Parts/Modules	2	\$ 6,407.51	\$ 12,815.02	replacement of the core router, if the funds are not available we would have to re- prioritize what we	and a complete solution. The complete	Hardware, Computer, Integ	04HW- 01- INHW
48 Port 1G 10G 25GbE	Internal Parts/Modules	2	\$ 35,610.30		This is a complete	All pieces of equipment are	Hardware, Computer,	04HW- 01-

SFP28 v2 Extended Tables Module						the core router, if the funds are not available we would have to re- prioritize what we will accomplish	and a complete solution. The complete	Integ	INHW
48-port 1GbE Class 4 PoE and 4-port SFP56 v2 Module - switch	Internal Parts/Modules	2	\$ 7,123.84		68	complete replacement of the core router, if the funds are not available we would have to re- prioritize what we will accomplish	and a complete solution. The complete	Hardware, Computer, Integ	04HW- 01- INHW
50GBase direct attach cable - 10 ft	Internal Parts/Modules	2	\$ 349.28	\$ 698.4		complete replacement of the core router, if the funds are not available we would have to re- prioritize what we will accomplish	and a complete solution. The complete	Hardware, Computer, Integ	04HW- 01- INHW
64/54XX FDN SUB 7Y	License and Subscription	2	\$ 3,634.38		76	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	
			\$		\$				
			\$		\$				
			\$		\$				
			\$ \$		\$				
			\$ \$		\$				
		22	\$		\$				
			67,081.36 1	44,854.	24				

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 *
A-133 Audit (Most Current)

Required? Attached Documents *



Travel Policy	~	<u>Travel Policy</u>
Payroll Policy	~	Payroll Policy
Procurement Policy	✓	Procurement Policy
		Purchasing Policy
Milestones	✓	2022 Grant Milestone
download template		
Capabilities Assessment download template	✓	<u>Capabilities Assessment</u>

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

Application ID: 449758

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

	Applicant Name	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



Powered by ZoomGrants™ and

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

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 t	tribal government (SLCGP: C.1). Are you a state,
territory, local, or tribal government?	

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).

Yes

□ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. ✓ 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.
	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any ents identified in Question 3.
The oract and the analware if	City of Reno would like to engage a consultant to assess the network for network segmentation and security best ice recommendations and changes. The network and security assessment is the first step in identifying vulnerabilities he best practice steps to remedy those vulnerabilities. Currently the network is very flat with a wide "blast radius" should are get through. It is also lacking a detailed network diagram of how traffic is flowing and where the critical choke points containment is needed. By adopting cybersecurity best practices for a network design it can limit the damage of an sion and the ability of an attacker to move laterally. The deliverables for this project include:
Red	ecutive Summary commendations in a series of deliverable documents
Lay Lay	pical Network Map Ter 2 Topology and Layer 3 Topology for 5 sites/buildings Ter 2 assessment information Ter 3 assessment Information, including routing design
•	oiect Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented.
, i i	o cot implementation - peacipe, in actail now, and by Wilvill the Divboacd biviet will be illibicilied.

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

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

N/A	M&A, what is the amount you will retain? retaining M&A, please enter "N/A"
9. Does this which would	project require new construction, renovation, retrofitting, or modifications of an existing structure necessitate an Environmental Planning and Historic Preservation (EHP) review?
Please see th	e EHP Guidance attachment for more information on EHP reviews.
✓ No	
in a limited in participation Hygiene Servi "health" of y configuration government executing coweekly vulnerability started. Indicinformation, advisories/cy annual self-a on the Nation MS-ISAC. En year of the a Cybersecurit	D SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participal umber of free services by CISA. For these required services and memberships, please note that is not required for submission and approval of a grant but is a post-award requirementCyber rices Web Application Scanning is an "internet scanning-as-a-service." This service assesses the our publicly accessible web applications by checking for known vulnerabilities and weak as. Additionally, CISA can recommend ways to enhance security in accordance with industry and dest practices and standards. Vulnerability Scanning evaluates external network presence by intinuous scans of public, static IPs for accessible services and vulnerabilities. This service provide rability reports and ad-hoc alerts. To register for these services, email info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services - SLCGP" to get ate in the body of your email that you are requesting this service as part of the SLGCP. For more visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-ber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous seessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is base all Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and cities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the ward/subaward period of performance and annually. For more information, visit Nationwide of Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
Our age	ncy has signed up for these services already
_	ncy has not yet signed up for these services, but understand we will be required to sign up for them if our pro
Our age	ncy has not yet signed up for these services, but understand we will be required to sign up for them if our pro
Our ager is award 11. Is this pro Yes No 12. Describe	the ways in which the project can be scaled or reduced or the reasons why it cannot. In the ways in which the project can be scaled or reduced or the reasons why it cannot. In the ways in which the need for a complete assessment. There really is no way to break up the profession.
Our ager is award 11. Is this pro Yes No 12. Describe This project caservices or the	the ways in which the project can be scaled or reduced or the reasons why it cannot. In the ways in which the project can be scaled or reduced or the reasons why it cannot. In the ways in which the need for a complete assessment. There really is no way to break up the profession.
Our ager is award 11. Is this product of the project Law and the	the ways in which the project can be scaled or reduced or the reasons why it cannot. Innot be scaled due to the need for a complete assessment. There really is no way to break up the profession deliverables.
Our ager is award 11. Is this properties or the Project Land Project	the ways in which the project can be scaled or reduced or the reasons why it cannot. annot be scaled due to the need for a complete assessment. There really is no way to break up the professive deliverables. Cation: Provide the 5-digit zip code where the project will be executed. Cation could be distinct from the sub-recipient address.
Our ager is award 11. Is this properties of the Project Land Project	the ways in which the project can be scaled or reduced or the reasons why it cannot. annot be scaled due to the need for a complete assessment. There really is no way to break up the professive deliverables. Cation: Provide the 5-digit zip code where the project will be executed. Cation could be distinct from the sub-recipient address.
Our ager is award 11. Is this properties Yes No 12. Describe This project conservices or the project local services as callevel. Build Sustain 15. Is this reconservices of the select "Yes" in select "Yes" in select "Yes" in select sel	the ways in which the project can be scaled or reduced or the reasons why it cannot. annot be scaled due to the need for a complete assessment. There really is no way to break up the professive deliverables. Cation: Provide the 5-digit zip code where the project will be executed. Cation could be distinct from the sub-recipient address.
Our ager is award 11. Is this product of the project of the proje	the ways in which the project can be scaled or reduced or the reasons why it cannot. Innot be scaled due to the need for a complete assessment. There really is no way to break up the profession deliverables. Pocation: Provide the 5-digit zip code where the project will be executed. Cation could be distinct from the sub-recipient address. Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project pability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current quest deployable to other jurisdictions?

PLANN	ING COST	S			
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		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	\$ 2,237.00		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	「otal	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		

EQUIPM	ENT COS	STS						
Equipment Cost Name	Line Item Description	Quantity	Unit . Cost	Γotal	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	
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
		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
				0.00			
Total		0	\$ 0.00	\$0.00			0

Document Uploads top

Required?	Attached Documents *
~	A-133 Audit
~	Travel
~	Payroll Policy
~	Procurement and Purchasing
	Procurement and Purchasing
✓	2022 Grant Milestone
✓	<u>Capabilities Assessment</u>
	V V V

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

Application ID: 449743

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

	Applicant Name	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



Powered by ZoomGrants™ and

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 y	ou a state,
territory, local, or tribal government?	

✓ 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).

Yes

□ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. ✓ 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 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	
✓ 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 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 requirementCyber Hygiene Services Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services − SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org). Please view SCLGP: Appendix G for additional information on these services and memberships.	
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	
□ 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. 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	

Line Item Detail Budget top

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit 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	Γotal	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		

EQU	IPMEN	T 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		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	
24P L2 Stck Cld- Mngd 24x GigE 370W PoE Switch	Switch	3	\$ 3,403.87	\$ 10,211.61	replacement	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		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.	Software as	
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
			\$	\$				
		60	\$	\$				
			11,541.45	205,023.39				

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 *
A-133 Audit (Most Current)

Required? Attached Documents *



Travel Policy	▼ Travel Policy
Payroll Policy	Payroll Policy
Procurement Policy	Procurement Policy Purchasing Policy
Milestones download template	<u>2022 Grant Milestone</u>
Capabilities Assessment download template	Capabilities Assessment

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

Application ID: 449759

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

	Applicant Name	City of Reno
	Project Name:	•
	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 Telephone702-799-2273

Fax Web FIN

88 6000030 SRBYQ7XFBYA6

UEI SAM Expires

Pre-Application top

1. To qualify for this	grant you must be	a state, territory, loc	al, or tribal gove	rnment (SLCGP: C	2.1). Are you a state,	territory, local,	or tribal
government?							

✓ 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).

Yes

□ No

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

I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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.

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.
- 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.

I understand and agree.

1 10	this agency within a rural area?
A ru	this agency within a rural area? ral 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 on "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)
	Yes
4	No
2 TI	nere are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP
A.10	b.b and Appendix A) Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to implementing the control of the contro
	capabilities to respond to cybersecurity incidents and ensure continuity of operations.
	Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
	Objective 3: Implement security protections commensurate with risk.
	Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	lease select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)
Proje	ects 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 govern 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 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 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 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 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 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 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 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 resorted degradation of which may impact the performance of information systems within the jurisdiction of the state.
1	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 a 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.
Secu tailo	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Questicurity Vendor will work with Clark County School District staff to update incident response plans, create additional departmental work aids, and created tabletop focused on transportation and food services disruptions due to cyberattack. CCSD is focused on these critical services to ensure concertaions. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.
In re	sponse to question 1: There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.
5. P	roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Describe the process by w
the See	project will be accomplished. Identify who (i.e., staff, contractor) will perform the work. SLCGP: Appendix A for sample evidence of implementation.
	urity vendor will conduct interviews to collect critical processes, information systems and single points of failure information from CCSD staff. Vend ate incident response plans, playbooks and create specific departmental work aids to be used in the event of a cybersecurity event. Vendor will fac

	•	ractical incident resp n and Food Services	•	sted to ensure resilience of information syste	ms and applications associated with CCSD
	-	_	or Management & Admini of the total cost of the pro		
	Yes	retained at up to 5%	or the total cost of the proj	c ot.	
	✓ No				
	140				
	•	g M&A, what is the retaining M&A, pleas	amount you will retain? se enter "N/A"		
			construction, renovation	· · · · · · · · · · · · · · · · · · ·	ting structure which would necessitate an
	Please see th	ne EHP Guidance atta	achment for more information	on on EHP reviews.	
	Yes				
	✓ No				
	services by 0 grant but is a service asses Additionally, Vulnerability vulnerability email that you https://www.free, anonym National Inst subrecipient annually. For Please view 5 Our age	CISA. For these requiresses the "health" or CISA can recommed Scanning evaluate es. This service projude requesting the cisa.gov/topics/cybnous, annual self-actitute of Standards as should complete representation, SCLGP: Appendix Gency has not yet signed.	uired services and member and received services and member for publicly accessible and ways to enhance sees external network preservices weekly vulnerability with the subject line "Ris service as part of the er-threats-and-advisories seessment designed to mand Technology Cybersethe NCSR, administered visit Nationwide Cybersefor additional information of these services already	perships, please note that participation is services—Web Application Scanning is a web applications by checking for know urity in accordance with industry and gonce by executing continuous scans of progressing Cyber Hygiene Services—SLGCP. For more information, visit CISA (cyber-hygiene-services.—Nationwide Cybeasure gaps and capabilities of a SLT's curity Framework and is sponsored by Doy the MS-ISAC, during the first year of the ecurity Review (NCSR) https://www.ciseconthese services and memberships.	ublic, static IPs for accessible services and for these services, email (GP" to get started. Indicate in the body of your (SP") so Cyber Hygiene Information Page: bersecurity Review (NCSR)—The NCSR is a cybersecurity programs. It is based on the HS and the MS-ISAC. Entities and their he award/subaward period of performance and urity.org/ms-isac/services/ncsr (cisecurity.org).
	12. Describe			I or reduced or the reasons why it cannot esponse plan and single tabletop exercise.	ıt.
	•		e 5-digit zip code where nct from the sub-recipient a	the project will be executed. address.	
	Select "susta			s on starting a new capability, or the inte apability at its existing/current level.	nt of the project is to close a capability gap.
	Sustain				
			other jurisdictions? s multiple jurisdictions (e.g.	, multiple cities). Select "No" if the project p	rimarily supports a single entity.
Line I	tem Detail Bu	udget <u>top</u>			
	PLANNIN	IG COSTS			
	Planning	Line Item	Quantity Unit Cost	How would your organization Total sustain this project if grant	Describe how the purchase(s) within this element tie into the project as

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.
				\$		
				\$		
				\$		
				\$		

\$	
Ψ	
\$	
\$	
\$	
\$	
\$	
\$	
\$	
\$	
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	「otal	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 Line Item Cost Name Description	Quantity	Unit Cost	al 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 0.0	\$ 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 \$ 2	5,000.00	One time cost.	Enhance the response and resilience of critical systems. Ensure the continuity of operations.	Yes
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		1 \$	\$ 25,000.00 \$ 2	5,000.00			0
Total		1 \$	25,000.00 \$25	,000.00			0

Document Uploads \underline{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	✓	CCSD Capabilities Assessment
download template		CCSD Capabilities

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

	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



Powered by ZoomGrants™ and

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 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

nates

Chief Information Officer

Marilyn Delmont delmom@nv.ccsd.net

Telephone702-799-2273

Fax Web

EIN 88 6000030 UEI SRBYQ7XFBYA6

SAM Expires

Pre-Application top

1. To qualify for this	s grant you must b	e a state, territory,	local, or tribal	l government (S	SLCGP: C.1). A	kre you a state, t	territory, local,	or tribal
government?								

✓ 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).

✓ Yes

□ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

✓ I understand and agree.

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

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.
- 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.

I understand and agree.

	Questions top
A rui as ai	this agency within a rural area? Fal 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 con "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b) Yes No
	nere 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 impro
	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
4	assessments. Objective 3: Implement security protections commensurate with risk.
	Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	ease select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A) ects 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 govern 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 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 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 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, discusse 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 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 gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforce 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 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 reso the degradation of which may impact the performance of information systems within the jurisdiction of the state.
17	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 are membership).
	Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
7.7	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.
Purc likelil and	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question hase and implement Multi Factor Authentication for Clark County School District Employees protecting student, employee, and district data. Redunce of account compromise resulting in ransomware attack. Multifactor Authentication enhances the resilience of information systems, application user accounts within CCSD. Deploying Multifactor Authentication is a best practice according to CISA guidance and will reduce the risk of ransommaccount compromise. Benefits the 7.24% of rural communities that Clark County School District provides critical services to.
In re	sponse to question 1: There are 373 school programs in SY 2023-24. 27 (7.24%) of which are considered rural schools.
the p See	oject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Describe the process by woroject will be accomplished. Identify who (i.e., staff, contractor) will perform the work. SLCGP: Appendix A for sample evidence of implementation. vare as a Service will be purchased. Software vendor will work with CCSD Enterprise Information Systems employees to configure. CCSD staff will all 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

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.

_ Y	
<u> </u>	.0
8. If re	etaining M&A, what is the amount you will retain?
If you	are not retaining M&A, please enter "N/A"
N/A	
9. Doe	es this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate
	onmental Planning and Historic Preservation (EHP) review?
	e see the EHP Guidance attachment for more information on EHP reviews.
□ Y	
✓ N	10
servic	EQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of es by CISA. For these required services and memberships, please note that participation is not required for submission and approbut is a post-award requirementCyber Hygiene Services Web Application Scanning is an "internet scanning-as-a-service." This
servic Additi	e assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configuration onally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards rability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services a
vulne	rabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for these services, email rability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body
https:	that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page: //www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR
Nation	nonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on t nal Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their
	cipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performa
	Illy. For more information, visit Nationwide Cybersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecuri
	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
	this project scaleable? Can any part of it be reduced?
Y	
✓ N	10
	escribe the ways in which the project can be scaled or reduced or the reasons why it cannot. Itly scaled down to most critical accounts totaling 500. Clark County School District has approx. 40,000 employees.
13. Pr	oject Location: Provide the 5-digit zip code where the project will be executed.
	roject location could be distinct from the sub-recipient address.
89146	
Select	ild or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project is to close a capability "sustain" if the project strictly maintains a core capability at its existing/current level.
✓	uild
	Sustain
15 ls	this request deployable to other jurisdictions?
	"Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.
✓ N	

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

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,		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		One time cost.	Integration expertise to enhance cybersecurity - Multifactor Authentication
			\$	\$	One time cost.	
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		1	\$ 20,000.00 20	\$ 0,000.00		

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		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				

TRAININ	IG COST	S					
Training Cost Name	Line Item Description	Quantity	Unit T	otal	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

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	✓	Capabilities Assessment updated
download template		CCSD Capabilities Assessment

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

	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



Powered by ZoomGrants™ and

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@elvshoshonetribe.com

Tel: (775) 289-7989

Additional Contacts

balaress@elyshoshonetribe.com

Ely Shoshone Tribe

505 S Pioche Hwy Telephone (775) 289-3013

Ely, NV 89301 Fax **United States** Web

EIN 94 2398696 **Finance Director** UEI PHLGX6MG6UK1

Sarah Balares SAM Expires

balaress@elyshoshonetribe.com

Pre-Application top

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

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).

Yes □ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

 	mino ede ouro 200. Eme You prov	and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and prity businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-tral entities should also, to the greatest extent practicable under a federal award, provide a preference for the chase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of ergency Management (DEM) in advance of the procurement. I may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract inisions guide, in the "Resource Document" tab. I understand and agree.
•	of fu	ach jurisdiction must complete its own application. The submitter of the grant application will be the recipient unds. Without an application, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant is to other agencies/organizations. I understand and agree.
;	ackı See	ntities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please nowledge your understanding and agreement of this requirement. SLCGP: C.4 for more information. I understand and agree.
Applic	atio	on Questions <u>top</u>
	A ru mos	this agency within a rural area? ral area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the t recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b) Yes
		No
		here are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most ely 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.
	4	Objective 3: Implement security protections commensurate with risk.
		Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
		lease select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A) ects 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.
	4	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,

	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 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. ✓ 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 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 not yet signed up for these servi
11. Is this project scaleable? Can any part of it be reduced? ☐ Yes ✓ 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. ☑ 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

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit 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 \$		

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		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	\$	\$		

EQUIPMENT COSTS

Equipment Cost Line Item Name Cost Cost	EQUII MEN	1 60313							
and Licensing and Licensing should be considered as the content of			Quantity		Total	your organization sustain this project if grant funding was reduced or	purchase(s) within this element tie into the project as described in the Application Questions section.		
Salusers	Windows Server		1			time purchase that doesn't require monthly	delivery of safe, recognizable and trustworthy online services by the state or local governments within the state, including through the use of the .gov		01-
Backup/Archiving Software	O365 Licensing		53			will be covered through normal budget	delivery of safe, recognizable and trustworthy online services by the state or local governments within the state, including through the use of the .gov	as a	11-
Protection Software \$\begin{array}{cccccccccccccccccccccccccccccccccccc		Backup/Archiving		\$ 60.00		will be covered through normal budget	event of a disaster, emails are backed up and archived with unlimited cloud storage. Implement security protections commensurate with	as a	11-
Software from Gmail to O365 time purchase delivery of safe, as a 11- that doesn't recognizable and Service SAAS require monthly trustworthy online expenses. services by the state or local governments within the state, including through the use of the .gov internet domain.		Protection	53	\$ 60.00		will be covered through normal budget	protection against spam/viruses/phishing emails. Implement security protections commensurate with	as a	11-
\$ \$	-	from Gmail to	53	\$ 15.00	\$ 795.00	time purchase that doesn't require monthly	delivery of safe, recognizable and trustworthy online services by the state or local governments within the state, including through the use of the .gov	as a	11-
				\$	\$				
\$ \$				\$	\$				
				\$	\$				

	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
	\$	\$		
213	\$	\$		
	3,785.08 25,1	157.08		

TRAINING COSTS

111/41141	110 0001						
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	т.	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	\$	\$			0
			149.00 1	,974.25			

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
		0.00	
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	✓	<u>Capabilities Assessment</u>

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

Application ID: 448992

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

	Applicant Name	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.lvnn@humboldtcountvnv.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, lo	cal, or tribal government (SLCGP: C.1). Are you a state,
territory, local, or tribal government?	

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).

Yes

□ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

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.
- ✓ 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.

I understand and agree.

Application Questions top

1	le	thic	agency	within	2	rural	arna	2
Ί.	. IS	tnis	agency	within	а	rurai	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

□ 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.
- 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.
 - 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,

	personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
4	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.
4	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.
4	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.
	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any nents identified in Question 3.
netwirew	would like to purchase a pair of high availability firewalls. This will allow our backup datacenter and internet connection to hade available to our users at a high level of security. We will be able to monitor applications and their usage, monitor work activity, exercise industry best practices as they relate to cybersecurity. Being our disaster recovery site, these will also provide for continuity of operations at the same or better level of security at our primary datacenter. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform
he	work.
Hum site. outi	SLCGP: Appendix A for sample evidence of implementation. boldt County's Technology Services Department will plan for, configure, and deploy the firewalls at our disaster recovery Before the firewalls arrive, we will have documented the necessary firewall policies, web content filtering policies, and ng structure. Upon their arrival, we will configure the firewalls and schedule deployment into a test environment, followed the by a move to the production environment.
	roject Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. 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 ations should be experience a failure at our primary datacenter.
M& <i>F</i> □	ill you be retaining funds for Management & Administration (M&A)? A may be retained at up to 5% of the total cost of the project. Yes No
	retaining M&A, what is the amount you will retain? u are not retaining M&A, please enter "N/A"
whice Plea	ces this project require new construction, renovation, retrofitting, or modifications of an existing structure ch would necessitate an Environmental Planning and Historic Preservation (EHP) review? se see the EHP Guidance attachment for more information on EHP reviews. Yes No
10. F	REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate
-	limited number of free services by CISA. For these required services and memberships, please note that

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

							in accordance with industry and	
						Inerability Scanning evaluates	external network presence by /ulnerabilities. This service provid	00
						. To register for these services		62
							giene Services – SLCGP" to get	
	started. Ind	licate in the b	ody of you	r email	that	you are requesting this service	e as part of the SLGCP. For more	
						nation Page: https://www.cisa.g		
						•	R) The NCSR is a free, anonymou is cybersecurity programs. It is bas	-
							ork and is sponsored by DHS and	
						0, ,	stered by the MS-ISAC, during the	
						nance and annually. For more i		
	-	-				ecurity.org/ms-isac/services/ncs		
		r SCLGP: Appe Jency has signe				formation on these services and m	nembersnips.	
			•			· · · · · · · · · · · · · · · · · · ·	vaccined to since up for those if our p	
	is awa		et signed u	p ioi trie	se s	ervices, but understand we will be	e required to sign up for them if our p	rojeci
		oroject scaleal	ble? Can a	ny part	of i	t be reduced?		
	✓ Yes							
	☐ No							
	12 Describ	e the wave in	which the	nroject	car	n be scaled or reduced or the re	easons why it cannot	
	We could im	plement a sing	le firewall r	ather tha	an ai		duce the resiliency of the project outo	come
						ode where the project will be e	xecuted.	
	89445	iocation could	De distilict	irom tne	Suc	o-recipient address.		
							apability, or the intent of the proje	
		capability gap	. Select "s	ustain"	if th	e project strictly maintains a c	ore capability at its existing/curre	nt
	level. ✓ Build							
	Sustair	2						
	□ Sustan	1						
	15. Is this re	equest deploy	able to oth	ner juris	dict	ions?		
			supports m	ultiple ju	risdi	ictions (e.g., multiple cities). Sele	ct "No" if the project primarily support	ts a
	single entity	·.						
	Yes							
	✓ No							
Line	Item Detail	Budget top						
	PLANNI	NG COST	S					
	Diamaina	l in a lane		l lmit			Describe how the purchase(s)	
	Planning Cost Name	Line Item Description	Quantity	Unit To	otal	sustain this project if grant funding was reduced or	within this element tie into the project as described in the	
	OOSt Hame	Description		0031		discontinued?	Application Questions section.	
					\$		• •	
					\$			
					\$			
					\$			
					\$			

\$

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

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit T	otal	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

• •	t 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	Ψ.	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	LOTAL	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
	0.00	
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 $^{\text{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 447811

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

	Applicant Name	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 Telephone775-684-5709

Carson City, NV 89701 Fax

United States Web https://www.nvsos.gov/sos

EIN 88-6000022

ASO 3 UEI
Ashley Griffitts SAM
dalea@sos.nv.gov 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?
✓ 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).

Yes No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

mind fede purc 200.: Eme You prov	and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and brity businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-ral entities should also, to the greatest extent practicable under a federal award, provide a preference for the hase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part 322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of rgency Management (DEM) in advance of the procurement. may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract isions guide, in the "Resource Document" tab. I understand and agree.
of fu fund	nch jurisdiction must complete its own application. The submitter of the grant application will be the recipient nds. Without an application, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant s to other agencies/organizations. I understand and agree.
ackr	ntities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please nowledge your understanding and agreement of this requirement. SLCGP: C.4 for more information.
4	I understand and agree.
olicatio	on Questions <u>top</u>
A rui mosi	this agency within a rural area? ral area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b) Yes
~	No
clos	nere are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most ely 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,
J	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. PI	ease select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)
	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.
✓	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.
1/2	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.
	Describe your project, in detail, including how it achieves the objective identified in Question 2 and any ments identified in Question 3.
The obj and according expression	e Secretary of State is modernizing legacy systems through a series of projects within Orion portfolio. One of the main ectives is to enhance security protection across all platforms that are utilized by constituents across the state and local distate governments. The Switch rack expansion with servers is required in our outsourced data center and is necessary to commodate the new systems coming online for project Orion. To ensure the continuity of operation the switch rack pansion with servers will maintain even spacing between equipment, encouraging ventilation, and reducing the need for ernal cooling. In the event of a cybersecurity incident the racks allow for the equipment to be as accessible as possible, ditionally, this will organize the equipment to ensure that ongoing Maintenace is easy. This is a five-year plan that includes racks the expansion, storage, power, and hosting of the servers.
De	Project Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. scribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work.
	e SLCGP: Appendix A for sample evidence of implementation. e rack expiation and the servers will be set up and maintained by the switch facility.
Se Thi	Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. e SLCGP: Appendix A for examples of project outcome formats. s will allow for the Secretary of State to move forward with other cybersecurity initiatives to support project Orion. With the way technologies coupled with the legacy systems we need to ensure their security this project will enable us to do that.
M8	Will you be retaining funds for Management & Administration (M&A)? A may be retained at up to 5% of the total cost of the project. Yes No
	f retaining M&A, what is the amount you will retain? You are not retaining M&A, please enter "N/A"
wh Ple	Does this project require new construction, renovation, retrofitting, or modifications of an existing structure ich would necessitate an Environmental Planning and Historic Preservation (EHP) review? Passe see the EHP Guidance attachment for more information on EHP reviews. Yes No
in a pai	REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate a limited number of free services by CISA. For these required services and memberships, please note that rticipation is not required for submission and approval of a grant but is a post-award requirementCyber giene Services Web Application Scanning is an "internet scanning-as-a-service." This service assesses the

	configuration	ons. Addition	ally, CISA	can recom		ty in accordance with industry and sexternal network presence by	
	executing of	ontinuous sc	ans of pub	lic, static I	Ps for accessible services and	vulnerabilities. This service provides	3
	vulnerabilit started. Ind information advisories/ annual self on the Nation MS-ISAC. E year of the Cybersecur Please view	y_info@cisa. licate in the b i, visit CISA's cyber-hygiend -assessment onal Institute intities and th award/subaw ity Review (N	dhs.gov wi ody of you Cyber Hyg e-services. designed t of Standar eir subrect vard period CSR) https endix G for a	ith the sub ir email that giene Informationwi- o measure ds and Tectipients sho d of performational in additional in	at you are requesting this serve mation Page: https://www.cisa de Cybersecurity Review (NCS) agaps and capabilities of a SL chnology Cybersecurity Frame buld complete the NCSR, admin mance and annually. For more security.org/ms-isac/services/not/ormation on these services and	rgiene Services – SLCGP" to get ice as part of the SLGCP. For more .gov/topics/cyber-threats-and-BR) The NCSR is a free, anonymous It's cybersecurity programs. It is base work and is sponsored by DHS and thistered by the MS-ISAC, during the formation, visit Nationwide esr (cisecurity.org).	ed the
		ency has not y	•		•	pe required to sign up for them if our pro	jec
	11. Is this p Yes No	oroject scalea	ble? Can a	ny part of	it be reduced?		
	™ No						
		echnologies be			n be scaled or reduced or the legacy systems currently in exis	reasons why it cannot. tence we are unable to reduce or scale	
					ode where the project will be ab-recipient address.	executed.	
		apability gap				capability, or the intent of the projec core capability at its existing/current	
	Select "Yes single entity					ect "No" if the project primarily supports	а
	Yes ✓ No						
	14 a.m. D.4.a.i.l	Durdmet ten					
Line	item Detail	Budget <u>top</u>					
	PLANNI	NG COST	S				
	Planning Cost Name	Line Item Description	Quantity	Unit Cost		n 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	Γotal	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

Switch This is a five-Rack/Server year plan for Expansion maintenance 1 \$ \$ The organization active year plan for 268,000.00 268,000.00 will be able to sustain this by event happens Integ including this as a servers are line item in the budget moving and easy to forward. \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	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
\$ \$	Rack/Server	year plan for storage and	-	·	00.00	will be able to sustain this by including this as a line item in the budget moving	a cybersecurity event happens servers are easily accessible and easy to	Computer, Integ	
				\$	\$				
\$ \$				\$	\$				
				\$	\$				

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

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

Application ID: 449037

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

	Applicant Name	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



Powered by ZoomGrants™ and

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

(775) 482-8192 or (775) Telephone

751-7075

(775) 482-8198 or (775)

AAV

Fax 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	ate,
territory, local, or tribal government?	

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).

✓ Yes

No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known. I understand and agree.

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

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ☐ 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. 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. 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.
4	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. D	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any
eler	ents identified in Question 3.
	Cyber Security Incident Response Plan for Nye County's Information Technology Department dictates that in the event of
	ijor cyber security incident, the Emergency Operations Center (EOC) at Nye County DEM in Pahrump will become the
	of operations for the response to the incident. This will enable the IT department to have immediate access to elected
	appointed County leadership, Department Heads and DEM staff in a single, secure location to provide timely decision
mak	ng and response activities in order to ensure continuity of government operations as well as continuity of
com	nunications. To ensure a high level of security for the electronics, radios and other communications equipment that will
nee	to be leasted at the EOC it is presented appears to explane compilities in and ground the DEM/EOC complex
1100	i to be located at the EOC, it is necessary to enhance surveillance capabilities in and around the Deivi/EOC complex.
1100	to be located at the EOC, it is necessary to enhance surveillance capabilities in and around the DEM/EOC complex.
To t	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the
To t	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for
To t	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the
To t DEN cons	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control.
To to DEN cons	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control.
To t DEN cons 5. P Des	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform
To t DEN cons 5. P Des the	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work.
To t DEN cons 5. P Des the	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform
To to DEM constant of the See	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation.
To t DEN cons 5. P Des the See Nye	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye
To to DEM constant S. P Des the See Nye Cou	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants
To t DEN cons 5. P Des the See Nye Cou Adm	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Caribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye bety DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants in instration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County
To to to DEM consider S. P Des the See Nye Could Adm DEM	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye noty DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County
To to to DEM consider S. P Des the See Nye Could Adm DEM	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Caribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye bety DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants in instration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County
To to to DEM consider S. P Des the See Nye Could Adm DEM	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye noty DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County
To to to DEM consistency of the See Nye Could Adm DEM Final	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye noty DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County
To to to DEM consistency of the See Nye Could Adm DEM Final Upon	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Caribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants in instration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County It will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nece/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. *In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants
To to to DEM consistency of the See Nye Could Adm DEM Final Upon Adm	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Caribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants in instration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County It will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nece/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. *In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT
To to to DEM consistency of the See Nye Could Adm DEM Final Upon Adm and	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. **SLCGP: Appendix A for sample evidence of implementation.** County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye by DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County It will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nec/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. **In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration
To to to DEM consistency of the See Nye Could Adm DEM Final Upon Adm and	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. *Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Caribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. *SLCGP: Appendix A for sample evidence of implementation. *County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants in instration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County It will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nece/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. *In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT
To to to DEM consistency of the See Nye Could Adm DEM Final Upon Adm and will in the See See See See See See See See See S	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. To ject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants in instration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nec/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. The receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report.
To to to DEM consider See Nye Could Adm DEM Final Upo Adm and will:	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. **Roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. **SLCGP: Appendix A for sample evidence of implementation.** County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye try DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County ince/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. **In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants in instration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report.
To to to DEM consider See Nye Could Adm DEM Final Upo Adm and will:	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. To ject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants in instration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nec/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. The receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report.
To to to DEM consider See Nye Could Adm DEM Final Upon Adm and will see Could Could Could Could Could DEM Could Could Could DEM Could Could DEM Co	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Beribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye that DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nec/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report. Interly Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration.
To to to DEM consider See Nye Could Adm DEM Final Upon Adm and will side Could	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Beribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye try DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County moc/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. The receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration ubmit close out financial reports and Nye County DEM will submit project close out report. The receipt of process of the project and Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration.
5. P Des the See Nye Cou Adm DEN Fina Upo Adm and will:	at end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nece/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. The receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report. Tetrly Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. Toject Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.
5. P Des the See Nye Cou Adm DEN Fina Upo Adm and will:	nat end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Beribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye try DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County moc/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. The receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration ubmit close out financial reports and Nye County DEM will submit project close out report. The receipt of process of the project and Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration.
5. P Des the See Nye Cou Adm DEN Fina Upo Adm and will: Qua Cou	at end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. Toject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nece/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. The receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report. Tetrly Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. Toject Outcomes - Describe, in a few sentences, the desired outcome(s) of your project.
To to to DEM consistency of the See Nye Could Adm DEM Final Upon Adm and will: Qual Could 6. P See Incressitation	ata end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. **Roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. **SLCGP: Appendix A for sample evidence of implementation.** **County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye try DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County Ince/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. **A receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report. **Tetrly Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Describeted System of Project Outcome formats.** **Appendix A for examples of project outcome formats.** **asset safety/security and access control at Nye County's EOC for elected and appointed officials, IT Staff and DEM/EOC in the event of a major cybersecurity incident.
5. P Des the See Nye Cou Adm DEN Fina Upo Adm and will: Qua Cou 6. P See Incress that 7. W	ata end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. **Roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. British the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. **SLCGP: Appendix A for sample evidence of implementation.** **County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nec/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. **In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration ubmit close out financial reports and Nye County DEM will submit project close out report. **Territy Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Territy Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Territy Project Reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Territy Project Reporting w
5. P Des the See Nye Cou Adm DEN Fina Upo Adm and will: Qua Cou 6. P See Incress that 7. W	ata end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. **Roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. **SLCGP: Appendix A for sample evidence of implementation.** **County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye try DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County I will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County Ince/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. **A receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration submit close out financial reports and Nye County DEM will submit project close out report. **Tetrly Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Describeted System of Project Outcome formats.** **Appendix A for examples of project outcome formats.** **asset safety/security and access control at Nye County's EOC for elected and appointed officials, IT Staff and DEM/EOC in the event of a major cybersecurity incident.
To t DEN cons 5. P Des the See Nye Cou Adm DEN Fina Upo Adm and will: Qua Cou 6. P See Incres Staf	ata end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. **Roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. British the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. **SLCGP: Appendix A for sample evidence of implementation.** **County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye may DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nec/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. **In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants inistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration ubmit close out financial reports and Nye County DEM will submit project close out report. **Territy Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Territy Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Territy Project Reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. **Territy Project Reporting w
To t DEN cons 5. P Des the See Nye Cou Adm DEN Fina Upo Adm and will: Qua Cou 6. P See Incres Staf	ata end, we are requesting this grant funding to purchase and install surveillance cameras around the perimeter of the complex and within the EOC and hallways leading to the EOC and a monitor to be mounted in the EOC to allow for tant monitoring and access control. To ject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLGGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for indoor and outdoor security cameras. In coordination with Nye County IT, Nye thy DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants inistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nece/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. In receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants instration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT Facilities Management will install the security cameras. Upon completion of the project, Finance/Grants Administration ubmit close out financial reports and Nye County DEM will submit project close out report. Interly Project reporting will be completed by Nye County DEM, Quarterly Financial reporting will be completed by Nye try Finance/Grants Administration. It staff and DEM/EOC in the event of a major cybersecurity incident.

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. ✓ Yes No	
10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participal 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 base on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the fyear 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 not yet signed up for these services, but und	s, ed the first
11. Is this project scaleable? Can any part of it be reduced? ✓ 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 to close a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current level. ☑ Build ☐ Sustain	
15. Is this request deployable to other jurisdictions? Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports single entity. ☐ Yes ✓ No	а
ine Item Detail Budget <u>top</u>	

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

ORGANIZATION COSTS

ONOANIZA	11014 000					
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		Would not be required.	5% M&A
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		1	\$ 135.00	125.00		
			135.00	135.00		

EQUIPMENT COSTS

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

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	sustain this project if grant funding was reduced or discontinued?	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	т.	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		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 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 9	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 $^{\text{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 449319

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

	Applicant Name	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



Powered by ZoomGrants™ and

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

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 Nve **County Commissioners**

Bruce Jabbour bjjabbour@nyecountynv.gov Telephone (775) 482-8192 or (775) 751-7075

(775) 482-8198 or Fax (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?		

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).

Yes ☐ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

enti puro 200 Eme You prov	inesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All non-federal ties should also, to the greatest extent practicable under a federal award, provide a preference for the chase, acquisition, or use of goods, products, or materials produced in the United States, per 2 C.F.R. Part .322. (NOFO, Section H.5.a). Any sole source procurement must be pre-approved in writing by the Division of ergency Management (DEM) in advance of the procurement. I may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract visions guide, in the "Resource Document" tab. I understand and agree.
5. E of fu	ach jurisdiction must complete its own application. The submitter of the grant application will be the recipient unds. Without an application, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant ds to other agencies/organizations. I understand and agree.
ack See	ntities applying as a subgrantee must meet a 10% cost share requirement for the FY 2022 SLCGP. Please nowledge your understanding and agreement of this requirement. SLCGP: C.4 for more information. I understand and agree.
Application	on Questions <u>top</u>
A ru mos ☑	s this agency within a rural area? Iral area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the st recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b) Yes No
	here are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most
	Sely 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.
✓	Objective 3: Implement security protections commensurate with risk.
	Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	lease select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A) jects 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.
✓	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. De	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any
elem This an ex bette report perfo	project is to upgrade one of our current firewalls, consolidate our current web filter into the new upgraded firewall and add stended retention logging and reporting server for activity and events on the firewall. This upgrade with extended logging will r allow us to monitor, audit and track activity and security events as well as review for changes in state, correlation and tring of events to help identify, assess and mitigate cybersecurity risks. The improved processing and memory rmance of the upgraded device will also allow for inspection of SSL secure web traffic in addition to running Intrusion and Advanced Threat Protection on the same device.
100%	6 of this funding will support rural communities throughout Nye County.
Mork See Nye Nye	SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for upgraded firewall appliance and subscription. In coordination with Nye County IT, County DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants
Desc work See Nye Nye Adm DEM	cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the to the state of the contractor of the state of the contractor of the contra
Desc worl See Nye Nye Adm DEM Final Upor Adm insta	cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the to. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for upgraded firewall appliance and subscription. In coordination with Nye County IT, County DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants nistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County
Desc worl See Nye Nye Adm DEM Final Upor Adm insta and	cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the contractor. SLCGP: Appendix A for sample evidence of implementation. County IT will obtain cost estimates for upgraded firewall appliance and subscription. In coordination with Nye County IT, County DEM will prepare and submit grant application via ZoomGrants. If approved for funding, Nye County Finance/Grants nistration will request approval to accept from the Nye County BOCC. Upon acceptance from the BOCC, Nye County will request updated cost estimates, obtain bids/quotes as necessary, and submit requisitions to the Nye County nice/Purchasing department who will generate purchase orders and submit to selected vendors to make the purchases. The receipt of purchased system, Nye County DEM will submit invoices for payment, to Nye County Finance/Grants nistration. Finance/Grants Management will submit requests for reimbursement (RFR) to DHS Grants. Nye County IT will lit the firewall software. Upon completion of project, Finance/Grants Administration will submit close out financial reports
Nye Nye Adm DEM Final Upor Adm insta and Cour 6. Pr See The device firew	cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the control of the control o
Description See Nye Nye Adm DEM Final Upor Adm insta and Quar Cour 6. Pr See The device firew revie	cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the control of the project will be accomplished. Identify who (i.e., staff, contractor) will perform the control of the project outcome formats. If approved (i.e., staff, contractor) will perform the control of project outcome for post event auditing and reafine to help reduce our risk and help work together with other agencies by will be to enhance our web filtering capability thru inspection of SSL Secure web traffic, consolidate both ealt traffic for post event auditing and correlation to help reduce our risk and help work together with other agencies by

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

wou	oes this project require new construction, renovation, retrofitting, or modifications of an existing structure value and the construction (EHP) review?
	se see the EHP Guidance attachment for more information on EHP reviews.
	Yes
~	No
a limparting the and linformation of the configuration of the configurat	REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participation in the services by CISA. For these required services and memberships, please note that icipation is not required for submission and approval of a grant but is a post-award requirementCyber iene Services Web Application Scanning is an "internet scanning-as-a-service." This service assesses the alth" of your publicly accessible web applications by checking for known vulnerabilities and weak figurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and ernment best practices and standards. Vulnerability Scanning evaluates external network presence by cuting continuous scans of public, static IPs for accessible services and vulnerabilities. This service provide kly vulnerability reports and ad-hoc alerts. To register for these services, email vulnerability_info@cisa.dhs the subject line "Requesting Cyber Hygiene Services - SLCGP" to get started. Indicate in the body of your ill that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygien remation Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwice ersecurity Review (NCSR) The NCSR is a free, anonymous, annual self-assessment designed to measure grapabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and nnology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipiental complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period commance and annually. For more information, visit Nationwide Cybersecurity Review (NCSR) sc://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
-	se view SCLGP: Appendix G for additional information on these services and memberships.
	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 prois awarded
	s this project scaleable? Can any part of it be reduced? Yes No
The	Describe the ways in which the project can be scaled or reduced or the reasons why it cannot. firewall upgrade, consolidation, and addition of the logging server cannot be scaled down as removing any one compod render the intent ineffective.
	Project Location: Provide the 5-digit zip code where the project will be executed. project location could be distinct from the sub-recipient address.
to cl leve	Build or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project ose a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current. Build
	Sustain
Sele singi	s this request deployable to other jurisdictions? cct "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports le entity. Yes
	No
	NO .
tem	Detail Budget <u>top</u>
PI A	ANNING COSTS
/	Harmond Language Traffic Browled and a more lands

Planning Line Item **Cost Name Description**

Quantity Unit Total sustain this project if grant funding was reduced or

How would your organization Describe how the purchase(s) within this element tie into the project as described in the

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

ORGANIZATION COSTS

ORGANIZA	HON COS	010				
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		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

	• •	Line Item Description	Quantity Unit Cost	How would your organization sustain this Total 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	•	Seek alternate grant funding	Update current firewall and consolidate current web filter and add extended logging	Firewall, network	
Firewall advanced threat protection subscription	Firewall subscription	1 46,080	T	\$ Seek alternate 2 grant funding	Provide advanced threat protection, energize updates, instant replacement, malware protection, advanced remote, insights subscriptions for 36 months	Firewall, network	
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		2 59,250	\$ 6.49 59,256.4	\$.9			

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

EXER	CISE COS	STS					
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 $^{\text{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 448162

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

	Applicant Name	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

inadams@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

FIN 262800962

GPR1NY74XPQ5 UEI

SAM

11/10/2021 **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?
✓ 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).

Yes □ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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.

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 in the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state to role governments within the state, to address cybersecurity risks and 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. □ Interest the state of the state. □ Interest 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 cybersecurity review process that ensures slignment between information technology and operational technology cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity review process that ensures slignment between information technology and operational technology cybersecurity review process that ensures slignment between information technology and operational technology cybersecurity review process that ensures a subject to the state of the		Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by
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 ricks 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 rolectives. □ Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the states should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries. □ Institute 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 (SIDC) is seeking funding to enhance the critical judicial network and database systems. As a separate branch of government, SIDC is funded within Washoe County but must maintain completely separate networks and database systems from the Executive Branch. The SIDC plans to implement this funding to improve and continuity test and evaluate the security of its network by him grove our posture and standard to harden against Cyber-attacks and intrusions. This professional assessment will include an assessement of our current state in accordance with National Inst		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,
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 obsersecurity 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 inition accessment of our current state in accordance with National Instituty test and evaluate the security of inition accessment of current state in accordance with National Instituty test and evaluate the security of its network by thining a cyber security auditing company to take a deep dive int		
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 review process that ensures alignment between information technology and operational technology cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity planning Committees as ensured to the consider consulting of the consulting to the consulting to improve and database systems from the Executive Branch. The SalDC plans to implement this funding to improve and scandard 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 SalDC will also utilize this funding to this rap professional cyber security and then provide remediation to harden security standards. Additional Not Generation Firewall interfaces and firevalls will also be added to allow the Court network trained to be segmented, filtered, and inspected against cyber-attacks and intrusions. Additional network switches would be purchased to replace out-of-date and insecure swi		infrastructure and key resources, the degradation of which may impact the performance of information systems within
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 states 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 (SIDC) 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 segm		
ensures alignment between information technology and operational technology cybersecurity objectives. □ Develop and coordinate strategies to address cybersecurity risks and cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries. □ Insure 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 our posture and standard to harden against Cyber-attacks and intrusions. This 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 objected against cyber attacks and the project will be implemented 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 led by Cou		
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 invove 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 Courty. 5. Project Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. Describe the process by which the project will b		
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 Nett Generation Firewall interfaces and firewalls will also be added to allow the Court howork 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 mi		associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also
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 Washoc 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 SLGGP: 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		
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 strives to provide the timely, f		Distribute funds, items, services, capabilities, or activities to local governments.
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 No		lications, and security and improve our posture and standard to harden against Cyber-attacks and intrusions. This
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 No	and firm Add segi	essional assessment will include an assessment of our current state in accordance with National Institute of Standards Technology (NIST) standards and framework. The SJDC will also utilize this funding to hire a professional cyber security to evaluate our active directory and cloud security and then provide remediation to harden security standards. itional Next Generation Firewall interfaces and firewalls will also be added to allow the Court network traffic to be mented, filtered, and inspected against cyber-attacks and intrusions. Additional network switches would be purchased to
M&A may be retained at up to 5% of the total cost of the project. ✓ Yes ✓ No	and firm Add segureplates 5. P Des the See The assected	essional assessment will include an assessment of our current state in accordance with National Institute of Standards Technology (NIST) standards and framework. The SJDC will also utilize this funding to hire a professional cyber security to evaluate our active directory and cloud security and then provide remediation to harden security standards. Itional Next Generation Firewall interfaces and firewalls will also be added to allow the Court network traffic to be mented, filtered, and inspected against cyber-attacks and intrusions. Additional network switches would be purchased to acc out-of-date and insecure switches. If awarded, 36% of funding will benefit rural Washoe County. Project Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. In the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. PSJCCP: Appendix A for sample evidence of implementation. SJDC, Court Tech team will be responsible for acquiring necessary quotes, purchasing the equipment, and hiring the essment teams/contractors in accordance with the milestone timeline. This project will be led by Court Tech Manager, and Galindo. Assessment review and follow-up will be conducted by all and reported to the Second Judicial District Court
9. If rotaining M.S.A. what is the amount you will retain?	seg replayed See The associated Celin Learn network elim	essional assessment will include an assessment of our current state in accordance with National Institute of Standards Technology (NIST) standards and framework. The SJDC will also utilize this funding to hire a professional cyber security to evaluate our active directory and cloud security and then provide remediation to harden security standards, itional Next Generation Firewall interfaces and firewalls will also be added to allow the Court network traffic to be mented, filtered, and inspected against cyber-attacks and intrusions. Additional network switches would be purchased to acce out-of-date and insecure switches. If awarded, 36% of funding will benefit rural Washoe County. Project Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. In the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. Project Pappendix A for sample evidence of implementation. SJDC, Court Tech team will be responsible for acquiring necessary quotes, purchasing the equipment, and hiring the essment teams/contractors in accordance with the milestone timeline. This project will be led by Court Tech Manager, and Galindo. Assessment review and follow-up will be conducted by all and reported to the Second Judicial District Court dership Team. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. Project Outcomes - Describe, in a few sentences, the desired outcome(s) of

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

	Does this project require new construction, renovation, retrofitting, or modifications of an existing structure
	ich would necessitate an Environmental Planning and Historic Preservation (EHP) review?
	ease see the EHP Guidance attachment for more information on EHP reviews. Yes
•	No No
in a par Hyg "he cor gov exe wee vul	REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate a limited number of free services by CISA. For these required services and memberships, please note that ricipation is not required for submission and approval of a grant but is a post-award requirementCyber giene Services Web Application Scanning is an "internet scanning-as-a-service." This service assesses the ealth" of your publicly accessible web applications by checking for known vulnerabilities and weak infigurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and evernment best practices and standards. Vulnerability Scanning evaluates external network presence by ecuting continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides ekly vulnerability reports and ad-hoc alerts. To register for these services, email (inerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get urted. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more formation, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-
adv anr on MS yea Cyl	visories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous, nual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the firm of the award/subaward period of performance and annually. For more information, visit Nationwide bersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
~	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 projectis awarded
4	Is this project scaleable? Can any part of it be reduced? Yes No
	1 INO
If n	Describe the ways in which the project can be scaled or reduced or the reasons why it cannot. ecessary, the Second Judicial District Court could eliminate Firewall and Interfaces assessment, but that would keep that a of the network at a higher risk for cyber-attacks and intrusions.
	Project Location: Provide the 5-digit zip code where the project will be executed. e project location could be distinct from the sub-recipient address. 501
	Build or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project close a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current rel.
~	Build
1	Sustain
Sel	Is this request deployable to other jurisdictions? lect "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports agle entity.
	Yes
4	No No
Iten	n Detail Budget <u>top</u>

Describe how the purchase(s) within this

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	organization sustain this project if grant funding was reduced or discontinued?	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		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		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	00 000 00	\$		
			22,000.00	22,000.00		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit To	tal	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

_ 	ENI COSI	•					
Equipment Cost Name	Line Item Description	Quantity	Unit Cost Tota	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		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.	provides additional insight into cybersecurity related activities and issues to enhance cyber- security at	Firewall network	
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		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.	provides additional insight into cybersecurity related activities and issues to enhance cyber- security at	Firewall network	
Internet and Network Content filtering	5. Internet and Network Content filtering to increase Cyber Security.	1	·	SJDC would submit an 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.	provides additional insight into cybersecurity related activities and issues to enhance cyber- security at	Firewall network	
Network switches	6. Network switches to replace out of date and insecure switches	1		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	provides additional insight into cybersecurity related activities	Firewall network	

			available from the State of Nevada, Administrative Offices of the Court if available.	enhance cyber- security at s Second Judicial District Court.
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	
	4	\$	\$	
	5	5,000.00 55,000.	00	

TRAINING COSTS

111/4111							
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
			0.00	0.00			

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?	purchase(s) within this element tie into the project as described in the Application Questions section.	coordinate this exercise with the State Exercise Officer?
			\$	\$			
			\$	\$			
			\$	\$			

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

Document Uploads top

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

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

Application ID: 449722

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

	Applicant Name	Second Judicial District Court
		SJDC's Cyber-Security Audit and
	Project Name:	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



Powered by ZoomGrants™ and

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

inadams@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

FIN 262800962

GPR1NY74XPQ5 UEI

SAM

11/10/2021 **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?
✓ 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).

Yes

□ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. Per FEMA legal opinion, locals may not use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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.

- 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.
 - 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.

Appli

~	I understand and agree.
catio	on Questions <u>top</u>
A rui mos	this agency within a rural area? ral area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the trecent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b) Yes No
	nere are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most ely 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.
	Objective 3: Implement security protections commensurate with risk.
	Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
	ease select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)
	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.
✓	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.
know inter addi with be a	are wireless and filtering systems by purchasing wireless access points since wireless points are a common target and we point for cyber intrusion and exploitation. In addition to purchasing the access points, SJDC would like to purchase an enet proxy for cyber security with zero trust access. The last added component to enhance the security would be tional security for the end users. By purchasing end-point protection for all users against malware, viruses, and anomalies 24/7 monitoring, the SJDC Court Tech team could be notified immediately upon a potential risk or breach of security and ble to close off that user prior to the risk of infecting the whole system. If awarded, 36% of funding will benefit rural shoe County.
Des the See SJD	roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. C, Court Tech team will be responsible for acquiring necessary quotes, and purchasing the equipment. This project will be by Court Tech Manager, Celina Galindo. Assessment review and follow up will be conducted by all and reported to the
	ond Judicial District Court Leadership Team.
See Second that back	roject Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. SLCGP: Appendix A for examples of project outcome formats. and Judicial District Court strives to provide the timely, fair, and efficient administration of justice under the law, in a matter instills and sustains the public's confidence in the judicial system. In order to provide this justice, a strong, safe, network abone must be in place. Without the security of the justice documents, the public's confidence would be eliminated. With funding, SJDC strives to enhance the wireless cybersecurity to provide faith in the justice system for everyone.
M& <i>F</i>	Fill you be retaining funds for Management & Administration (M&A)? A may be retained at up to 5% of the total cost of the project. Yes No
8. If	retaining M&A, what is the amount you will retain? u are not retaining M&A, please enter "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.

✓ No				
in a limited number of frequition participation is not requitive. Hygiene Services Web "health" of your publicitions. Addition government best practice executing continuous so weekly vulnerability rep vulnerability_info@cisal started. Indicate in the binformation, visit CISA's advisories/cyber-hygien annual self-assessment on the National Institute MS-ISAC. Entities and the year of the award/subave Cybersecurity Review (National Please view SCLGP: Appears wiew	ee services ired for sub Application y accessible ally, CISA cores and standard of sample of Standard period period (ICSR) https ired for a for	s by CISA. In mission are seen recommendards. Vulic, static If-hoc alerts the subject of measure ds and Tector of perforn cil/www.cisedditional internal int	For these required services and approval of a grant but is a part of a grant but is a grant of a gra	vin accordance with industry and external network presence by vulnerabilities. This service provides and the services – SLCGP" to get the as part of the SLGCP. For more gov/topics/cyber-threats-and-R) The NCSR is a free, anonymous, as cybersecurity programs. It is based york and is sponsored by DHS and the stered by the MS-ISAC, during the first information, visit Nationwide or (cisecurity.org).
Our agency has sign	ed up for the	se services	already	
Our agency has not y is awarded	vet signed up	o for these s	services, but understand we will be	e required to sign up for them if our project
If necessary, the Second	which the	project cal	n be scaled or reduced or the r	nt requests, but that would decrease the
13. Project Location: Pro <i>The project location could</i> 89501			ode where the project will be e b-recipient address.	xecuted.
to close a capability gap level. Build Sustain 15. Is this request deploy	o. Select "su	ustain" if th	ne project strictly maintains a c	apability, or the intent of the project is ore capability at its existing/current ct "No" if the project primarily supports a
single entity.	σαρροπο πι	лиріс јапва	icuons (e.g., manipie cines). Gele	et No II the project primarily supports a
Yes				
✓ No				
-				
a Ham Detall De La Co				
ne Item Detail Budget <u>top</u>				
PLANNING COST	S			
Planning Line Item Cost Name Description	Quantity	Unit Cost	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

ONOMINE	11011 000					
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?	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	т.	SJDC would submit a request to the County for additional budget authority to	This add-on provides additional insight into	Hardware, computer	

	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.	related activities and issues to enhance cyber- security at Second Judicial District Court.	Hardware, computer	
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		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				
			-0,000.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	How would your organization sustain this project if grant funding was reduced or discontinued?	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
0.00	0.00	

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	✓	<u>Milestones</u>
Capabilities Assessment	✓	Capabilities

download template	
* ZoomGrants™ is not responsible for the content of uploaded documents.	
Application ID: 449721	
Become a <u>fan of ZoomGrants™</u> on Facebook	
Problems? Contact us at Questions@ZoomGrants.com	
©2002-2023 GrantAnalyst.com. All rights reserved. "ZoomGrants" and the ZoomGrants logo are trademarks of GrantAnalyst.com, LLC. Logout Browser	
<u>Loque</u> <u>Drowser</u>	

	Applicant Name	Casard Indiaial District Count
	Applicant Name	Second Judicial District Court
		SJDC's Cyber-Secure Wireless and
	Project Name:	Filtering
	Project Funding Stream:	FY 2022 SLCGP
	Milestone Description*	Date of Expected Completion
	Acceptance of Funding by Washoe County	Assume award notification by
1	Board of County Commissioners (BCC),	1/1/2024. Within 90 days of
	Setting up of separate grant tracking of	receipt of Award notification. By
	fiscal expenses within financial system	end of March 2024
	niscar expenses within infancial system	Cha of Waren 2024
2	Ohtoin maaaaan oo aa taa firana wan da wa fa w	within 00 days of societ of Award
2	Obtain necessary quotes from vendors for	within 90 days of receipt of Award
	all equipment	notification. By end of March 2024
3		within 45 days of acceptance of
	Issue of Purchase Orders for equipment	funds by BCC. By mid May 2024
		within 90 days of receipt of
4		equipment. may vary depending
4		on product backlog/shipment
	Install of equipment	issues.
_		
5	Final review and report of project to DEM	By end of December 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?
✓ 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).

4	Yes
1	Nο

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known. I understand and agree.

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

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. 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 al 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.
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 limitation 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 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 resource 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 group
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
✓ 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

✓ No	
in a limited number participation is not hygiene Services- "health" of your pronfigurations. As government best executing continuity weekly vulnerability_inforstarted. Indicate in information, visit advisories/cyber-hannual self-assession the National Instance. Entities year of the award. Cybersecurity Rev	AICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate of free services by CISA. For these required services and memberships, please note that equired for submission and approval of a grant but is a post-award requirementCyber Neb Application Scanning is an "internet scanning-as-a-service." This service assesses the olicly accessible web applications by checking for known vulnerabilities and weak itionally, CISA can recommend ways to enhance security in accordance with industry and actices and standards. Vulnerability Scanning evaluates external network presence by a scans of public, static IPs for accessible services and vulnerabilities. This service provides reports and ad-hoc alerts. To register for these services, email cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get he body of your email that you are requesting this service as part of the SLGCP. For more SA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-giene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous, ment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based tute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the did their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first albaward period of performance and annually. For more information, visit Nationwide w (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
	Appendix G for additional information on these services and memberships.
	signed up for these services already not yet signed up for these services, but understand we will be required to sign up for them if our project
This project could be systems. The project	ys in which the project can be scaled or reduced or the reasons why it cannot. scaled up to support additional information systems, but licensing typically covers a set amount of allows IT staff to monitor and audit accounts and shared resources. The scope could expand or contract se or decrease our resource usage.
	: Provide the 5-digit zip code where the project will be executed. ould be distinct from the sub-recipient address.
	Select "build" if this project focuses on starting a new capability, or the intent of the project is gap. Select "sustain" if the project strictly maintains a core capability at its existing/current
	eployable to other jurisdictions? eployable to other jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a
tem Detail Budg	<u>top</u>

PLANNING COSTS

Planning Line Item
Cost Name Description

Quantity

Unit Total How would your organization Describe how the purchase(s) sustain this project if grant funding was reduced or discontinued?

How would your organization 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

ONOMINE	11011 000					
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		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	\$ 2,515.00 2,		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.	g 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 Software Directory licensing for Auditing cloud Software directory License services auditing	1 \$ 995.00 995	\$ WCSD will 5.00 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.	Risk Management	04AP- 04-RISK
File Directory Software Auditing licensing for Software file server auditing	1 \$ 2,995.00 2,995	\$ WCSD will 5.00 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.	Risk Management	04AP- 04-RISK
	\$	\$	unuono.		
	\$	\$			
	\$	\$			
	\$	\$			
	\$	\$			
	\$	\$			
	\$	\$			
	\$	\$			
	\$	\$			
	\$	\$			
		Φ.			
	\$ 3 \$	\$ \$			

TRAIN	ING COST	ΓS					
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

A-133 Audit (Most Current)	Y	FY22 Audit
Travel Policy	~	Travel Policy
Payroll Policy	✓	Payroll Policy
		Payroll Regulation
Procurement Policy	✓	Procurement Policy
Milestones	~	Auditing Software
download template		
Capabilities Assessment download template	✓	WCSD Capabilities assessment

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

Application ID: 448882

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

_			
	Applicant Name	Washoe County School District	
	Project Name:	WCSD Account and File Auditing Soft	ware License
	Project Funding Stream:	FY 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?	
✓ 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).

•			
4	Yes		
	No		

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known. I understand and agree.

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

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. 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

	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.
	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any nents identified in Question 3.
Cour agair bread toolir infrast network accoursely relations	project is to purchase and implement a cloud-based assessment and response system that will supplement Washoe may School District's existing endpoint detection and response system. This system will be used to perform broad queries must endpoints for threat hunting and artifact collection. These capabilities will enable WCSD's IT security staff to identify a chand immediately respond thereto. This will assist WCSD IT department to overcome key weaknesses in existing mg. It will be built on a cloud infrastructure provider using open source tooling. Putting the system on a third-party's cloud structure will allow the system to reach systems even if they were deployed across the District or on other public works. This system will be supported using open-source and free tooling. From a technical perspective, this will emplish Objective 2: "Understand their current cybersecurity posture and areas for improvement based on continuous mg, evaluation, and structured assessments" because the tooling supports broad queries against endpoints and can wort some incident response capabilities. WCSD is large, geographically-dispersed public entity. However, WCSD has a invely small IT department. Performing these functions through any other means is technically impractical with current straints and limitations. This software is necessary to support WCSD's daily operations, and provide a safe and secure as a support wcsd's daily operations, and provide a safe and secure as a support wcsd's daily operations.
Desc	roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work.
This itself	SLCGP: Appendix A for sample evidence of implementation. project will be implemented by internal IT department staff. The third-party cloud provider will support hosting. The tooling is not supported by a third-party vendor and relies on free and open source tools. The work for this project is performed in ralized consoles and does not require on-hands installation of new equipment, systems, or software.
See Imple	roject Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. SLCGP: Appendix A for examples of project outcome formats. ement a cloud-based threat hunting and response platform to assess the security posture of all WCSD systems on nal and external networks.
M&A	fill you be retaining funds for Management & Administration (M&A)? A may be retained at up to 5% of the total cost of the project. Yes No
	retaining M&A, what is the amount you will retain? u are not retaining M&A, please enter "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.

✓	No Yes
in a parti Hygi "hea conf gove exec weel vuln start infor advis annu on the MS-I year Cybe Pleas	EQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate imited number of free services by CISA. For these required services and memberships, please note that cipation is not required for submission and approval of a grant but is a post-award requirement. "Cyber ene Services." Web Application Scanning is an "internet scanning-as-a-service." This service assesses the Ith" of your publicly accessible web applications by checking for known vulnerabilities and weak igurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and rnment best practices and standards. Vulnerability Scanning evaluates external network presence by uting continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides they vulnerability reports and ad-hoc alerts. To register for these services, email erability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get end. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more mation, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-sories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR)-" The NCSR is a free, anonymous, all self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the SAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first of the award/subaward period of performance and annually. For more information, visit Nationwide resecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
	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
12. E This that p back 13. F	rescribe the ways in which the project can be scaled or reduced or the reasons why it cannot. project can be scaled up or down by adding or removing hosts from the cloud provider. The front-end is a load balancer bushes traffic to a back-end system. This architecture allows WCSD's IT department to add more load-balancers and resources to support threat hunting and response actions. Project Location: Provide the 5-digit zip code where the project will be executed. Project location could be distinct from the sub-recipient address.
to cl leve	uild or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project is ose a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current
Sele singl	s this request deployable to other jurisdictions? ct "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a e entity. Yes No
ne Item	Detail Budget <u>top</u>
PL/	ANNING COSTS
Plan Cost	How would your organization Describe how the purchase(s) ning Line Item Name Description How would your organization Describe how the purchase(s) sustain this project if grant 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.
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
			\$	\$		
		0	\$	\$		
			0.00	0.00		

EQUIPMENT COSTS

|--|

Cloud	Cloud	1	Ф.	Ф	WCSD will austain	\$6.012 in the	Applications	ΟΛΛΡ
Cloud Infrastructure	Cloud infrastructure consumption costs, including computing and storage resources, cloud portal, and vendor support.	1		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.	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,		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 $^{\text{TM}}$ is not responsible for the content of uploaded documents.

Application ID: 448898

	Applicant Name	Washoe County School District
		WCSD Cloud Assessment and
	Project Name:	
	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



Powered by ZoomGrants™ and

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 Telephone 7757893435 Reno, NV 89512 Fax 775-333-5012 **United States**

Web www.washoeschools.net EIN 8860000919

Director of Grants UEI **DEA6NNBHBTV3**

Lauren Ohlin SAM lohlin@washoeschools.net **Expires**

Pre-Application top

·· <u> </u>	
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?	
✓ 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). ✓ Yes

No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known. I understand and agree.

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

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. 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.
	escribe your project, in detail, including how it achieves the objective identified in Question 2 and any nents identified in Question 3.
91% From beca WCS men pers oper	rnal and external email traffic. Email security is critical because it is the main avenue for cyber attacks to occur with over 5 of cyber attacks starting with a phishing email. This project will provide licensing and a vendor-supported implementation. In a technical perspective, this will accomplish Objective 3: "Implement security protections commensurate with risk" ause it supports secure email and prevents bad actors from gaining a foothold in the environment using targeted phishing. SD is a large, geographically-dispersed public entity. However, the internal IT department has only one dedicated staff inber supporting email security. Implementing this system will prevent malicious email and also free up the existing sonnel to implement more advanced cybersecurity needs. This software is necessary to support WCSD's daily business rations, and provide a safe and secure learning environment for our 62,000 students, including those in rural areas of shoe County.
Des	roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work.
See This proje will p ensu	SLCGP: Appendix A for sample evidence of implementation. Is project will be implemented by internal IT department staff. Because WCSD's enterprise email system is hosted, the ect will integrate the environment with a vendor solution that is provided by their isolated cloud environment. This project primarily be performed by internal staff working in coordination with a vendor to ensure mail flow is not impacted while uring their system gains visibility to the organization's email system. This work will be performed in a centralized console does not require on-hands installation of new equipment, systems, or software.
See Impl	roject Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. SLCGP: Appendix A for examples of project outcome formats. lement an email security solution to protect all users from internal and external email threats, including malware, phishing, business email compromise.
7. W M&A	Vill you be retaining funds for Management & Administration (M&A)? A may be retained at up to 5% of the total cost of the project. Yes No
8. If	retaining M&A, what is the amount you will retain? ou are not retaining M&A, please enter "N/A"
whice Plea	oes this project require new construction, renovation, retrofitting, or modifications of an existing structure ch would necessitate an Environmental Planning and Historic Preservation (EHP) review? ase see the EHP Guidance attachment for more information on EHP reviews. Yes

•	No No
in pa Hy "h co go ex vu sta inf ad an on Ms ye Cy	REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate a limited number of free services by CISA. For these required services and memberships, please note that riticipation is not required for submission and approval of a grant but is a post-award requirement. "Cyber regiene Services." Web Application Scanning is an "internet scanning-as-a-service." This service assesses the ealth" of your publicly accessible web applications by checking for known vulnerabilities and weak infigurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and overnment best practices and standards. Vulnerability Scanning evaluates external network presence by ecuting continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides eakly vulnerability reports and ad-hoc alerts. To register for these services, email linerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services - SLCGP" to get arted. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more formation, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-visories/cyber-hygiene-services. "Nationwide Cybersecurity Review (NCSR)"—The NCSR is a free, anonymous, nual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the SISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first are of the award/subaward period of performance and annually. For more information, visit Nationwide bersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org). ease view SCLGP: Appendix G for additional information on these services and memberships. Our agency has not yet 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
	. Is this project scaleable? Can any part of it be reduced? ✓ Yes No
Th thr org rat	Describe the ways in which the project can be scaled or reduced or the reasons why it cannot. is project will support ingress/egress, as well as intra-organization email security. This is critical because most email reats come from outside the organization, but internal threats, such as business email compromise, come from inside the ganization (intra-org). This project will cover all staff and student accounts. Limiting implementation to just staff members, ther than including student accounts, would drastically degrade WCSD's capabilities in the event of a compromise of udent accounts.
Th	. Project Location: Provide the 5-digit zip code where the project will be executed. see project location could be distinct from the sub-recipient address. 512
to lev	. Build or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project is close a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current vel. Build Sustain
Se sir	. Is this request deployable to other jurisdictions? elect "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a negle entity. Yes No
ne Iter	m Detail Budget <u>top</u>
PI	LANNING COSTS How would your organization Describe how the purchase(s)
	riow would your organization beschibe now the purchase(s)

Planning Line Item Cost Name Description

Quantity Unit

Unit Total 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 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	

product,			will allow WCSD to
including cloud portal		may include reallocated budget	implement an
and vendor		priorities to	security suite for all
support		ensure that the	accounts and
зарроп		level of continued	
		supports for these	
		products are	common vector for
		necessary.	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.
	\$	\$	organizations.
		\$	
		\$	
		\$	
		\$	
		\$	
		\$	
		\$	
		\$	
		\$	
		\$	
		\$	
		\$	
75,		\$	
73,	3.33 249,750.0		

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
0.00	0.00	

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost		How would your organization sustain this project if grant funding was reduced or discontinued?	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 9	\$ 0.00 \$0	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 $^{\text{TM}}$ 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



Powered by ZoomGrants™ and

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?
✓ 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).

✓ Yes No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. 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

	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.
adm MFA geog supp scho proje adm 62,0 user	ors rather than just a password. WCSD maintains an internal IT department that has MFA implemented for all logins on inistrator accounts. This project will expand access to MFA and provide licensing and onboarding to WCSD's existing a platform for the remaining users that maintain some level of administrative permissions. WCSD is a large, graphically-dispersed public entity. However WCSD's IT department is relatively small, requiring individual technicians to port many schools. Because of this limitation, IT personnel are unable to provide constant technical support to each pool. Therefore, administrative permissions are granted to multiple users on site, as designated by the site Principal. This sect will actively support Objective 3: Implement security protections commensurate with risk by specifically protecting inistrator accounts that are necessary to perform daily business and a safe and secure learning environment for WCSD's 00 students, including those in rural areas of Washoe County. This will allow the IT department to monitor and audit all accounts. It will also prevent bad actors from compromising systems and immediately pivoting to other systems on a red network.
Descent See This authors admuser.	roject Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. cribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform work. SLCGP: Appendix A for sample evidence of implementation. project will be implemented by WCSD's IT department staff. There already exists an implementation of multi-factor entication using hardware tokens for IT staff. This project involves several key steps that will be extended to all remaining inistrators. First, the web portal will be updated with a detailed policy describing when a second prompt is required. The largent will be installed on computers, and then the user/agent will be enrolled into the system to ensure that their bunt triggers the second prompt. This is largely automated, but requires coordination across technology departments and
See	roject Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. SLCGP: Appendix A for examples of project outcome formats. ement Multi-Factor Authentication (MFA), prioritizing privileged users, internet-facing systems, and cloud accounts.
M& <i>F</i>	fill you be retaining funds for Management & Administration (M&A)? A may be retained at up to 5% of the total cost of the project. Yes No
	retaining M&A, what is the amount you will retain? u are not retaining M&A, please enter "N/A"

9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure

Plea	ch would necessitate an Environmental Planning and Historic Preservation (EHP) review? see see the EHP Guidance attachment for more information on EHP reviews.
	Yes No
_	NO .
in a partifyging the starting of the starting of the starting on the starting of the starting	REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participal limited number of free services by CISA. For these required services and memberships, please note that icipation is not required for submission and approval of a grant but is a post-award requirementCyber iene Services Web Application Scanning is an "internet scanning-as-a-service." This service assesses the alth" of your publicly accessible web applications by checking for known vulnerabilities and weak figurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and ernment best practices and standards. Vulnerability Scanning evaluates external network presence by cuting continuous scans of public, static IPs for accessible services and vulnerabilities. This service provid kly vulnerability reports and ad-hoc alerts. To register for these services, email terability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get ted. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more remation, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-isories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymousla self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is bathe National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the rof the award/subaward period of performance and annually. For more information, visit Nationwide
	ersecurity Review (NCSR) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).
	se view SCLGP: Appendix G for additional information on these services and memberships. 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 p is awarded
12. [This	No Describe the ways in which the project can be scaled or reduced or the reasons why it cannot. project could be scaled up to support MFA for the entire District staff or staff and students. The current system iguration and license uses minimal additional "signal intelligence factors" to make decisions on whether access show
shou	uld not be granted. Improvements will include higher tiers of licensing or integrations with existing tooling to register cific endpoints and applications in a much more firm "zero trust" methodology.
	Project Location: Provide the 5-digit zip code where the project will be executed. project location could be distinct from the sub-recipient address.
to cl	Build or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/curreel. Build
	Sustain
	- Cuotam
Sele	s this request deployable to other jurisdictions? ect "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily support le entity.
	Yes
✓	No
	Detail Budget top

PLANNING COSTS

Planning Line Item Cost Name Description	Quantity Cost Tota	sustain this project if grant funding was reduced or discontinued?	within this element tie into the project as described in the Application Questions section.
	\$		
	\$)	
	\$		
	\$		
	\$	3	
	\$		
	\$		
	\$		
	\$		
	\$		
	\$	3	
	\$	3	
	\$	3	
	\$		
	0 0.00 \$		

ORGANIZATION COSTS

ONOAMEA	11011 000	, 10				
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

	: Line Item : Description	Quantity	Unit Tota	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	AEL Number
MFA software	Software licensing for	700	•	WCSD will sustain this project through	\$18,872 is the total cost for this licensing project.	,	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.	
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
		700	\$ 26.96 18,872.0	\$ 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
0.0	0.00	

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
				0.00			
Total		0 \$	0.00	\$0.00			0

Document Uploads top

Documents Requested *	Required? At	ttached Documents *
A-133 Audit (Most Current)	✓ <u>FY</u>	Y22 Audit
Travel Policy	✓ <u>Tra</u>	ravel Policy
Payroll Policy		ayroll Policy ayroll Regulation
	1 6	ayron regulation
Procurement Policy	✓ Pr	rocurement Policy
Milestones download template	✓ <u>M</u>	FA milestones



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

Application ID: 448671

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

	Applicant Name	Washoe County School District	
	Project Name:	Multi-Factor Authentication (MFA) L	icense
	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?	
Voc	

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).

Yes

No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.

Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

I understand and agree.

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

because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200. All procurement must be free and open competition. Applicants are also required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. Part 200.321. All nonfederal 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. 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. 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. 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 ✓ 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. 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. 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.						
0	Distribute funds, items, services, capabilities, or activities to local governments.						
	Describe your project, in detail, including how it achieves the objective identified in Question 2 and any ments identified in Question 3.						
est cor hel are	sed on what they discover is actively in use. In a "known compromise" test, the penetration tester starts with a foothold ablished in the network and more closely mirrors what an actual bad actor would discover when compromising an internal imputer. The proposed test will involve testing at WCSD's central IT office, as well as at an individual school. This test will p IT internal staff understand and prioritize remediations that will help understand the current cybersecurity posture and as for improvement, while also enhancing network preparation, response, and resilience in the event of a legitimate cyber each.						
De: the	Project Implementation - Describe, in detail, how, and by whom, the proposed project will be implemented. scribe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform						
WC spe and an per	e SLCGP: Appendix A for sample evidence of implementation. CSD will coordinate this penetration test internally and work with a third-party vendor to perform the test. The test will be ecifically scoped to encompass two separate sites within the WCSD's enterprise network. This will ensure that the project ditest is realistic and based on "real world" scenarios. The third-party contractor will perform the actual work. While we have internal IT security staff, the intent is to make sure that the test most directly mirrors a legitimate adversary, their respective, and capabilities. Performing the test internally would prevent IT staff from understanding how the adversary receives our environment.						
Se	Project Outcomes - Describe, in a few sentences, the desired outcome(s) of your project. e SLCGP: Appendix A for examples of project outcome formats. CSD will improve preparation, response, and resilience of information systems, applications, and user accounts owned or						
	erated by WCSD against cybersecurity risks and cybersecurity threats by understanding an adversary's perspective.						
	Will you be retaining funds for Management & Administration (M&A)? A may be retained at up to 5% of the total cost of the project. Yes						
~	No No						
	f retaining M&A, what is the amount you will retain? You are not retaining M&A, please enter "N/A"						
wh	Does this project require new construction, renovation, retrofitting, or modifications of an existing structure ich would necessitate an Environmental Planning and Historic Preservation (EHP) review? Passe see the EHP Guidance attachment for more information on EHP reviews. Yes No						

	How would your organization Describe how the purchase(s) Planning Line Item Quantity Unit Total sustain this project if grant within this element tie into the
	PLANNING COSTS
Line It	tem Detail Budget <u>top</u>
	INO NO
	Yes✓ No
	single entity.
	Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a
	15. Is this request deployable to other jurisdictions?
	☐ Sustain
	■ Build
	level.
	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
	The project location could be distinct from the sub-recipient address. 89512
	13. Project Location: Provide the 5-digit zip code where the project will be executed.
,	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.
	□ No
	✓ Yes
	11. Is this project scaleable? Can any part of it be reduced?
	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
	Our agency has signed up for these services already
	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.
,	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
	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
	information, visit CISA's Cyber Hygiene Information Page: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-servicesNationwide Cybersecurity Review (NCSR) The NCSR is a free, anonymous,
	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
	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
	government best practices and standards. Vulnerability Scanning evaluates external network presence by
	configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and
	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
	participation is not required for submission and approval of a grant but is a post-award requirementCyber
	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

Cost Name Description

Quantity Unit 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 To	tal	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 Number
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			
			\$	\$			

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

TRAINING COSTS

Training	Line Item		Unit		How would your organization sustain	Describe how the purchase(s) within this element tie into the	Do you plan to coordinate this
Cost Name	Description	Quantity	Cost	Total	this project if grant funding was reduced or discontinued?	project as described in the Application Questions section.	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.	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	• •	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.	attackers using
	\$	5	
	\$	5	
	\$	5	
	\$	\$	
	\$	\$	
	\$	\$	
	\$	\$	
	\$	5	
	\$	5	
	\$	5	
	\$	5	
	\$	5	
	\$	5	
	1 \$ 16,081.00 \$ 16,081.0	0	0
Total	1 \$ 16,081.00 \$16,081.0	0	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
		WOOD and 1999 and and
Capabilities Assessment download template	✓	WCSD capabilities assessment

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

Application ID: 448865

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

	Applicant Name	Washoe County School District
	Project Name:	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