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

Powered by ZoomGrants™ and

Nevada Office of Emergency Management / Homeland Security

FFY 2025 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/1/2025

Washoe County Sheriff's Office

FY25 Northern Nevada Cyber Center

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

$ 93,000.00 Requested

Submitted: 8/8/2025 12:23:13 PM (Pacific)

Project Contact
Aleesah Campbell
SOGrants@washoecounty.us
Tel: 7753283013

Additional Contacts
svanderwall@washoecounty.gov

Washoe County Sheriff's Office

911 Parr Blvd
Reno, NV 89512
United States

Sheriff
Darin Balaam
sogrants@washoecounty.us

Telephone7753283013
Fax
Web https://washoesheriff.com/

Pre-Application *top*

1. Is your organization one of the following types of entities?: County, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of government, regional government entity, agency or instrumentality of a local government, rural community, unincorporated town or village, or other public entity, tribe, or authorized tribal organization.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.

☑ Yes
☐ No

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

☑ Yes
□ No

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

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

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.
☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2025 SLCGP. Please acknowledge your understanding and agreement of this requirement.
☑ I understand and agree.

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

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Office of Emergency Management) may not use this funding to administer their own subawards.
☑ I understand and agree

Application Questions *top*

1. Is this agency considered a rural area (an area encompassing a population of less than 50,000 people)?
If your agency is not considered a rural area, but your project will support rural communities, select "No" and indicate in your narrative what percentage of your project will directly benefit rural Nevadans.
□ Yes
☑ No

2. There are four (4) objectives for FY 2025 SLCGP. Please select the objective with which your project most closely aligns.

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

☐ Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

☑ Objective 3: Implement security protections commensurate with risk.

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

3. Please select which of the SLCGP program elements your project addresses.

Projects may align with more than one element.

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

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

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

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

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

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

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

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

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

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

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

☑ 12. Leverage cybersecurity services offered by CISA. (See Application Question 10 for further details on these services.)

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

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

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

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

4. Describe your project in detail.

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

As the Detective Sergeant managing the Northern Nevada Cyber Center (NNCC) at the Washoe County Sheriff's Office, I oversee an Internet Crimes Against Children (ICAC) task force providing digital forensics and cyber support to Northern Nevada law enforcement. Our center handles sensitive child exploitation, cybercrime investigations, and digital evidence from government systems, including public safety networks. This project requests $93,000 in SLCGP funding to replace outdated hardware in digital forensics workstations, acquire advanced forensics software, provide cybersecurity training, and implement encrypted data transmission software. These align with SLCGP objectives and CISA's Cybersecurity Performance Goals (CPGs) like vulnerability management, data encryption, incident response, and workforce development.

What we would like to do:
(1) Replace old, unsupported hardware in digital forensics workstations ($30,000): Upgrade aging units with high-performance, secure hardware like forensic-grade computers with GPUs, encrypted SSDs, hardware MFA, and NIST-compliant builds.
(2) Purchase digital forensics software ($30,000): Acquire suites for in-depth host analysis by OS/file systems, used by investigators for post-crime disk analysis, deleted file recovery, and evidence database marking.
(3) Provide cybersecurity training ($30,000): Offer courses building skills in digital forensics, incident response, penetration testing, threat intelligence, network security, and secure coding, with real-world labs and GIAC-aligned certifications.
(4) Implement software for encrypted data transmission ($3,000): Deploy tools for secure remote access, including VPNs, SSH, and SSL for point-to-point or link encryption.

Our setup risks: Unsupported hardware lacks patches, vulnerable to exploits; limited software slows probes and risks breaches; training gaps impair ransomware response (e.g., Nevada agency attacks); unencrypted transmission enables interception of ICAC evidence. As a DEM subrecipient, this fixes assessment gaps, bolstering the state Cybersecurity Plan and local resilience. Without upgrades, we risk breaches, delayed cases, and CPG non-compliance on end-of-life tech.

These will cut agency risk, speed responses, align with SLCGP's 80% local/25% rural pass-through (NNCC serves rural areas), and protect public safety infrastructure from threats.

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

The listed project aligns with SLCGP Objective 3—"Implement security protections commensurate with risk"—by using risk assessments (e.g., vulnerabilities in outdated hardware and data transmission) to deploy targeted mitigations that reduce cybersecurity threats to government-operated systems at the Northern Nevada Cyber Center (NNCC). This objective focuses on applying best practices, such as those in CISA's Cybersecurity Performance Goals (CPGs), to protect against identified risks like exploits, breaches, and ransomware, building on governance and posture understanding from Objectives 1 and 2.

Specifically:
- Hardware replacement ($30,000): Replaces unsupported, vulnerable workstations with secure, NIST-compliant builds featuring encrypted SSDs and hardware MFA. This implements CPGs on vulnerability management (1.E: End end-of-life hardware) and access controls (2.A: MFA), directly mitigating exploit risks in forensics operations on public safety networks.
- Digital forensics software ($30,000): Deploys tools for disk analysis, file recovery, and evidence

marking, enabling rapid incident response and threat detection. This aligns with CPGs on logging (1.F) and system reconstitution (5.A), protecting against post-breach data loss in cybercrime investigations.
- Cybersecurity training ($30,000): Provides GIAC-aligned courses in forensics, incident response, and threat intelligence, equipping staff to apply risk-based protections like penetration testing. While supporting Objective 4, it enables Objective 3 by ensuring personnel can implement mitigations effectively.
- Encrypted data transmission software ($3,000): Implements VPNs, SSH, and SSL for secure evidence sharing, fulfilling CPG 3.B (Data encryption) to counter interception risks during ICAC collaborations.

Overall, the project scales protections to NNCC's high-risk environment (handling sensitive government data), lowering breach potential by ~30% per assessments, enhancing resilience for rural Northern Nevada public safety infrastructure, and complying with SLCGP's focus on risk-commensurate investments.

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

(3) Enhance preparation, response, and resilience of state/local government information systems, applications, and user accounts against cybersecurity risks/threats: Project upgrades outdated forensics workstations with NIST-compliant hardware (encrypted SSDs, MFA) to block exploits on ICAC/cyber systems. Forensics software boosts incident response via quick analysis/recovery; training hones threat detection/ransomware skills; encrypted transmission secures data sharing, cutting breaches and aiding recovery (CPG 5.A).

(5) Ensure state/local governments adopt cybersecurity best practices/methodologies: Implements CPG measures like ending end-of-life hardware (1.E), data encryption (3.B), and role-based training (4.A). Upgrades promote vulnerability management/secure coding, with tools for assessments. As Washoe Sheriff's Office, models practices for Northern Nevada, aiding statewide adoption via shared digital evidence capabilities.

(10) Assess/mitigate cybersecurity risks/threats to critical infrastructure/key resources impacting state information systems: NNCC bolsters public safety networks (e.g., ICAC data). Upgrades counter ransomware/exploits per assessments; training enables proactive mitigation; encrypted transmission protects evidence databases, aligning with CPGs on vulnerability/incident response to prevent statewide impacts.

(12) Leverage CISA cybersecurity services: Utilizes free tools like Cyber Hygiene Scanning for upgraded systems, Resilience Review for post-implementation eval. Training includes CISA exercises; participates in Federal Virtual Training Environment for GIAC certs. Forensics leverage Known Exploited Vulnerabilities Catalog for prioritizations, as post-award collaboration.

(15) Ensure rural areas' access/participation in cybersecurity services/programs: NNCC aids rural counties (e.g., Humboldt, Pershing) with forensics/cyber support for under-resourced agencies. Upgrades provide equitable access to secure transmission/training, meeting SLCGP's 25% rural pass-through and bridging urban-rural resilience gaps.

(16) Distribute funds/items/services/capabilities/activities to local governments: As DEM subrecipient, builds Washoe capabilities shared via forensics/training. Upgraded hardware/software enables joint response for rural locals, aligning with 80% pass-through and boosting statewide local cybersecurity.

7. Does your project address any of the following Key Cybersecurity Best Practices?

☑ Implement multi-factor authentication.
□ Implement enhanced logging.
☑ Data encryption for data at rest and in transit.
☑ End use of unsupported/end of life software and hardware that are accessible from the internet.
□ Prohibit use of known/fixed/default passwords and credentials.
☑ Ensure the ability to reconstitute systems (backups).
☑ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.

☐ Migration to the .gov internet domain.

8. Describe, in detail, how, and by whom, the proposed project will be implemented.
Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.
The proposed project at the Northern Nevada Cyber Center (NNCC), within the Washoe County Sheriff's Office, will be implemented under the direction of Detective Sergeant and NNCC manager, Samuel Van Der Wall, with oversight from the Washoe County IT Division and Nevada's Division of Emergency Management (DEM) as SLCGP subrecipient administrator. The 12–18-month process, starting post-award (Q4 2025), follows 2 CFR Part 200, SLCGP guidelines, and CISA's Cybersecurity Performance Goals (CPGs), with quarterly DEM reports and annual CISA metrics.

Phase 1: Planning and Procurement (Months 1-3): Team will work together with Washoe County IT to refine specs and issue RFPs for hardware, software, and training. Vendors will be selected. Staff will manage most installation and setup, with possible brief contracts if needed.

Phase 2: Acquisition and Setup (Months 4-6): Vendors will deliver items, and IT specialists and team members will install workstations (GPUs, encrypted SSDs, MFA), forensics software, and encrypted tools.

Phase 3: Training and Rollout (Months 7-12): Eight staff will take GIAC-aligned courses on incident response and threat intelligence from providers like SANS or CISA partners. These will be scheduled flexibly (such as with online options) and tools will be integrated into workflows for evidence sharing with rural partners.

Phase 4: Evaluation and Sustainment (Months 13-18): Team will assess via CISA Cyber Hygiene services (target 30% risk reduction), and Project Manager will manage adjustments and documentation. Internal staff handles maintenance.

This staff-driven approach builds capacity efficiently, mitigating delays with contingencies and phasing.

9. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcomes of this project include replacing vulnerable, outdated hardware and software at the Northern Nevada Cyber Center to eliminate cybersecurity risks from unsupported systems, thereby enhancing the resilience of government-operated networks used for digital forensics and ICAC investigations. Through targeted training and encrypted data transmission tools, our team will achieve faster incident response times, reduced breach potential by approximately 30%, and improved secure evidence sharing across Northern Nevada law enforcement agencies, including rural partners. Ultimately, these upgrades will align with CISA's Cybersecurity Performance Goals, bolstering statewide public safety infrastructure against threats like ransomware while promoting best practices and equitable access to cybersecurity capabilities for local governments.

10. FY 2025 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2025 SLCGP NOFO.
Please indicate your understanding of this policy.
☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (CISA). For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber Hygiene Services-- Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web

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

☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)

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

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

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.
Yes, this project is scalable due to its modular components, allowing adjustments based on funding, needs, or risk assessments without compromising core objectives.
- Hardware replacement ($30,000): Reducible by upgrading fewer (e.g., 2 instead of 4) workstations or opting for lower-spec models; expandable by adding more units or advanced features like AI-accelerated GPUs for broader forensics capacity.
- Digital forensics software ($30,000): Reducible via fewer licenses or basic versions; expandable with additional modules for cloud forensics or enterprise integrations.
- Cybersecurity training ($30,000): Reducible by training fewer staff or shorter courses; expandable with more participants, advanced certifications, or ongoing programs.
- Encrypted data transmission ($3,000): Reducible to free/open-source tools; expandable to premium enterprise solutions for multi-agency scalability.

These changes maintain alignment with SLCGP goals, ensuring cost-effective risk mitigation.

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

☑ Yes

☐ No

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

☐ Build

☑ Sustain

16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project.

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

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

Category Budget Totals *top*

Category Budget Breakdown	Costs
Planning	$ 0.00
Organization	$ 0.00
Equipment	$ 63,000.00
Training	$ 30,000.00
Exercise	$ 0.00
M & A	$ 0.00
Total	**$ 93,000.00**

Category Budget Totals Narrative

The project budget allocates $93,000 across four scalable components to enhance cybersecurity at the Northern Nevada Cyber Center. Anticipated challenges include procurement delays due to supply chain issues or vendor backlogs, potentially pushing milestones back; integration hurdles with existing systems requiring IT support; and scheduling conflicts for training amid ongoing investigations. To mitigate, we'll prioritize early vendor bids, conduct phased testing, and offer flexible online courses, ensuring alignment with SLCGP timelines.

Line Item Detail Budget *top*

Line Item Detail

List Items (according to POETE categories)	Detailed Description	Quantity	Unit Cost	Total
PLANNING				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00

			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
PLANNING Subtotal		**0**	**$ 0.00**	**$ 0.00**
ORGANIZATION				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
ORGANIZATION Subtotal		**0**	**$ 0.00**	**$ 0.00**
EQUIPMENT				
Hardware Replacement	04HW-01-INHW - The hardware replacement upgrades aging digital forensics workstations with secure, high-performance forensic-grade computers, including GPUs for processing, encrypted SSDs, hardware MFA modules, and NIST-compliant builds to address unsupported system vulnerabilities. Focus on phasing out end-of-life hardware, improving secure handling of ICAC and cybercrime investigations on government networks.	1	$ 30,000.00	$ 30,000.00
Forensic Software	05HS-00-FRNS - Software, Forensic - Digital forensics software suites enable in-depth analysis of hosts by operating system and file systems, aiding investigators in examining computer-related crimes through tools for disk analysis, deleted file recovery, and integrated databases to flag key data.	1	$ 30,000.00	$ 30,000.00
Encrypted Data Transmission Software	05EN-00-ETRN - Encrypted data transmission software encompasses network access solutions that deliver secure, encrypted user connections, primarily for remote access but also suitable for point-to-point or link encryption	1	$ 3,000.00	$ 3,000.00

	scenarios. This includes virtual private networks (VPNs) and protocols such as SSH and SSL to ensure protected data transfer.			
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
EQUIPMENT Subtotal		**3**	**$ 63,000.00**	**$ 63,000.00**
TRAINING				
Cybersecurity Training	Cybersecurity training courses provide practical skills to combat modern threats through topics like digital forensics, incident response, penetration testing, threat intelligence, network security, and secure coding, emphasizing real-world labs, simulations, and GIAC-aligned certifications for immediate application and validation.	1	$ 30,000.00	$ 30,000.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
TRAINING Subtotal		**1**	**$ 30,000.00**	**$ 30,000.00**
EXERCISE				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00

			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
EXERCISE Subtotal		**0**	**$ 0.00**	**$ 0.00**
MANAGEMENT AND ADMINISTRATION				
			$	$ 0.00
			$	$ 0.00
Total		**4**	**$ 93,000.00**	**$93,000.00**

Document Uploads *top*

Documents Requested *	**Required?**	**Attached Documents ***
A-133 Audit (Most Current)	☑	2023 Washoe County Single Audit
Travel Policy	☑	Washoe County Travel Procedure - January 2024
Payroll Policy	☑	WC Personnel Handbook
Procurement Policy	☑	Washoe County Purchasing Manual - revised Aug 2022
Milestones	☑	FY25 DEM SLCGP Cyber Grant Milestones Northern Nevada Cyber Center Personnel List

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

Application ID: 506107

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

Logout | Browser