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

Humboldt County Emergency Management

Oasis Consulting Services

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

$ 129,000.00 Requested

Submitted: 8/29/2025 11:29:25 AM (Pacific)

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

Additional Contacts
weston.noyes@humboldtcountynv.gov

Humboldt County Emergency Management

50 West Fifth St
Winnemucca, NV 89445
United States

County Manager
Don Kalkoske
don.kalkoske@humboldtcountynv.gov

Telephone17753753195
Fax
Web

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?

Humboldt County proposes a strategic cybersecurity enhancement initiative in partnership with Oasis Online Consulting, a Nevada-based IT services provider with over 20 years of experience supporting rural counties and educational institutions. The project aims to strengthen the county's cybersecurity posture by leveraging Oasis Online's comprehensive suite of services, which include network management, threat monitoring, incident response coordination, and policy compliance support.

What we would like to do:

- Deploy proactive network monitoring and diagnostics to detect vulnerabilities and prevent breaches.
- Implement secure server configurations and bandwidth management to ensure system integrity and performance.
- Coordinate with external cybersecurity experts for virtual risk assessments and incident response planning.
- Align technology policies and procurement practices with federal and state cybersecurity standards.

Why we are doing this: Humboldt County's current cybersecurity infrastructure faces increasing threats from phishing, ransomware, and unauthorized access attempts. As a rural county with limited internal IT resources, we require specialized support to maintain secure operations and protect sensitive data. Oasis Online has an existing contractual relationship with the county and a proven track record of delivering reliable, scalable, and locally informed technology services.

How this project improves cybersecurity protection:

- Reduces risk exposure through continuous monitoring and early threat detection.
- Improves incident response readiness by integrating external cybersecurity expertise and virtual walkthroughs.
- Ensures compliance with cybersecurity regulations through policy alignment and strategic planning.
- Builds long-term capacity by optimizing technology workflows for secure operations.

This project will result in a measurable improvement in Humboldt County's ability to prevent, detect, and respond to cybersecurity threats, ensuring the safety and integrity of public services and data.

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

Humboldt County's cybersecurity enhancement initiative, in partnership with Oasis Online Consulting, directly aligns with Objective 3 by implementing security protections that are proportionate to the county's risk profile and operational realities.

Once again, as a rural county with limited internal IT capacity, Humboldt faces elevated risks from phishing, ransomware, and unauthorized access attempts. Oasis Online's services are specifically designed to address these threats through a layered, risk-based approach:

- Network Monitoring and Diagnostics: Oasis Online deploys continuous monitoring tools to detect anomalies and vulnerabilities early, reducing the likelihood of successful cyberattacks.
- Secure Infrastructure Configuration: Servers and network components are configured to industry standards, minimizing exposure to external threats.
- Incident Response Coordination: Oasis facilitates virtual risk assessments and incident response planning with external cybersecurity experts, ensuring that the county is prepared to respond effectively to breaches.
- Policy and Compliance Support: Oasis helps align Humboldt's technology policies with federal and state cybersecurity frameworks, ensuring that protections are not only effective but also compliant.

By tailoring protections to Humboldt County's specific risk environment—balancing resource constraints with threat exposure—this project ensures that cybersecurity investments are both strategic and impactful. The result is a more resilient infrastructure that safeguards public data and services against current and emerging threats.

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

Humboldt County’s cybersecurity enhancement initiative, in partnership with Oasis Online Consulting, directly supports multiple program elements outlined in Question 3 of the State and Local Cybersecurity Grant Program (SLCGP). The project is designed to manage, monitor, and secure the county’s information systems, applications, and user accounts through a comprehensive and scalable service model.

Manage, Monitor, and Track Information Systems, Applications, and User Accounts

Oasis Online provides full-spectrum IT management services, including:

- User account creation and management.
- Software and hardware monitoring and updates.

Monitor, Audit, and Track Network Traffic and Activity

Oasis Online’s scope includes:

- Bandwidth monitoring.
- Network diagnostics and troubleshooting.

Support Legacy Systems and Unsupported Technologies

The project includes:

- Installation and maintenance of legacy systems such as Windows Server and various Linux distributions.
- Evaluation and recommendation of hardware upgrades. This ensures that older systems remain secure and compatible with modern cybersecurity protocols

Continuous Vulnerability Assessments and Threat Mitigation

Oasis Online coordinates with external cybersecurity experts and conducts ongoing diagnostics and backup solutions. Their services include:

- Remote management.
- Filtering and imaging solutions.
- Daily prioritization of help tickets and technical issues. These practices support a continuous cycle of vulnerability assessment and mitigation.

Ensure Continuity of Operations During Cybersecurity Incidents

Oasis Online’s BCP outlines procedures for maintaining critical operations during disruptions. It includes:

- Recovery time objectives (RTO) and recovery point objectives (RPO).
- Rapid restoration protocols for internal and client systems. This ensures Humboldt County can maintain essential services during and after a cybersecurity incident.

Ensure Continuity of Communication and Data Networks

Oasis Online acts as a liaison between Humboldt County and third-party vendors, ensuring:

- Secure and uninterrupted communication across platforms.
- Technology compatibility across departments and jurisdictions. This supports intergovernmental continuity in the event of a network disruption.

Modernization of IT and Operational Technology

Oasis Online assists with:

- Technology budgeting and procurement.
- Strategic planning for infrastructure upgrades.
- Policy alignment with cybersecurity objectives. This ensures that Humboldt County’s IT and operational technology systems evolve in tandem with cybersecurity best practices.

Ensure Access for Rural Areas

As a Nevada-based provider with deep experience in rural counties, Oasis Online ensures that Humboldt County—along with other underserved regions—has equitable access to cybersecurity services and support.

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 cybersecurity enhancement project will be implemented by Oasis Online Consulting in partnership with Humboldt County IT.
Implementation Process:
1. Initial Planning and Coordination.
The project will begin with strategic planning sessions between Oasis Online and Humboldt County leadership, including the Emergency Manager and IT stakeholders. These meetings—such as the Humboldt/Oasis Strategy Meeting—have already laid the groundwork for aligning cybersecurity goals with county operations.
2. Infrastructure Assessment and Configuration.
Oasis Online will conduct a thorough assessment of the county's existing IT infrastructure. This includes server installation and configuration, bandwidth monitoring, and network troubleshooting. Oasis staff will evaluate hardware and recommend upgrades to ensure compatibility and security.
3. Cybersecurity Monitoring and Protection.
The team will deploy diagnostics, backup solutions, imaging, and filtering technologies to monitor and protect county systems. Oasis also installs and configures remediation software and productivity tools across the network.
4. Vendor Liaison and Compliance Support.
Oasis will act as a liaison between Humboldt County and third-party vendors, including cybersecurity specialists. They will facilitate virtual site walkthroughs and risk assessments, ensuring compliance with federal and state cybersecurity frameworks.
5. Ongoing Management and Reporting.
Oasis Online will assist with technology budgeting, procurement, and policy alignment. They will provide regular updates to the county administration and the board, ensuring transparency and accountability throughout the project.
Personnel Performing the Work:
• Dan Slentz, CEO of Oasis Online, will oversee the project and serve as the primary point of contact.
• Oasis Online Technicians and Networking Team will perform the technical work, including system configuration, monitoring, and support.
• Administrative Staff from Humboldt County, including Carol Lynn and Alex Brooks, will coordinate with Oasis Online to ensure alignment with county needs.

9. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome of this project is to significantly strengthen Humboldt County's cybersecurity posture by implementing a comprehensive, locally managed protection strategy in partnership with Oasis Online Consulting. This initiative will result in improved threat detection, faster incident response, enhanced system resilience, and full compliance with cybersecurity standards. Ultimately, the project will safeguard county operations and sensitive data while building long-term capacity for secure technology management.

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.

89445

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.

The desired outcome of this project is to significantly strengthen Humboldt County’s cybersecurity posture by implementing a comprehensive, locally managed protection strategy which may at some point require expansion or reduction of services to be determined during the performance period.

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.

The FFY22 SLCGP project resulted in purchase and installation of firewalls which strengthened our network security. This new project will continue to build on the capacity begun with the FFY22 purchase.

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	$ 43,000.00
Organization	$ 43,000.00
Equipment	$ 43,000.00
Training	
Exercise	
M & A	
Total	**$ 129,000.00**

Category Budget Totals Narrative

The following list contains the scope of work included in the agreement with Oasis Consulting:
1. Network Management - Server installation/Configuration, Bandwidth Monitoring, Network Troubleshooting, Evaluating and Recommending Hardware, User Account Creation and Management.
2. Software/Hardware Monitoring and Update - Diagnostics, Backup Solutions, Imaging Solutions, Filtering Solutions.
3. Liaison between Third Party Vendors
4. Software Installations e.g. - Windows Server, Various Linux Distributions, Remediation Software, Office Productivity Software, Remote Management.
5. Personnel/Business Management - Research and approve technology purchases to ensure compatibility, Assist with technology budget, Serve as liaison to County Commission.
6. Help Desk Services - Assist with Help Desk operations, Help Technicians prioritize tickets and projects, Assist with day to day repairs, installations, upgrades, etc.

Line Item Detail Budget *top*

Line Item Detail

List Items (according to POETE categories)	Detailed Description	Quantity	Unit Cost	Total
PLANNING				
	Research and approve technology purchases to ensure compatibility - Assist with development of technology budget - Liaison with vendors and County leadership	1	$ 43,000.00	$ 43,000.00

			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
PLANNING Subtotal		**1**	**$ 43,000.00**	**$ 43,000.00**
ORGANIZATION				
	Assist with Help Desk operations - Assist with Technicians prioritization of tickets and projects	1	$ 43,000.00	$ 43,000.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
ORGANIZATION Subtotal		**1**	**$ 43,000.00**	**$ 43,000.00**
EQUIPMENT				
	Server configuration - Bandwidth monitoring - Network troubleshooting - Recommending hardware - Backup solutions - Diagnostics - Remediation software - Windows Server installation - etc.	1	$ 43,000.00	$ 43,000.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00

			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
EQUIPMENT Subtotal		**1**	**$ 43,000.00**	**$ 43,000.00**
TRAINING				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
TRAINING Subtotal		**0**	**$ 0.00**	**$ 0.00**
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		**3**	**$ 129,000.00**	**$129,000.00**

Document Uploads *top*

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

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

Application ID: 507389