Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Douglas County Emergency Mangement**

# Physical Security - Badge/Card Reader System

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

**$ 101,204.17** Requested

Submitted: 6/21/2023 3:42:36 PM (Pacific)

**Project Contact**
Kathy Lewis
kmlewis@eastforkfire.org
Tel: 7757829040

**Additional Contacts**
dswickard@douglasnv.us

**Douglas County Emergency Mangement**

1694 County Rd
Minden, NV 89423
United States

**Director of Finance**
Kathy Lewis
kmlewis@eastforkfire.org

| | |
|---|---|
| Telephone | 7757829040 |
| Fax | |
| Web | |
| EIN | 383972546 |
| UEI | |
| SAM Expires | |

## Pre-Application *top*

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

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

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

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions *top*

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

- [x] Yes
- [ ] No

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

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

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

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

Douglas County currently uses Lenel Alarm Monitoring to control door badge access in a limited capacity. This system is running on an end-of-life server OS and the upgrade path and licensing costs are prohibitive - in addition to not providing for robust & modern UI and/or business functionality. We are looking to migrate to a new software for better monitoring, control and reporting on when employees are accessing doors. We currently do not have badge/card access for all the doors that we would like to monitor and implementing this project will help us to eliminate the use of keys in our environment which will allow us to track who enters each door and when if necessary. This will serve to significantly increase our capacity as it pertains to physical security relative to cyber and elections security. Our current system is also standalone system, meaning user accounts are created and deactivated outside of normal user active directory accounts. Newer software's give us the ability to use LDAP to sync user accounts into the system. If a user is deactivated in active directory, their badge would also be deactivated at the same time helping us to minimize unauthorized access of doors and decreasing the risk of human error. This project would include migrating to the new system (purchasing of software licensing) and adding badge readers for doors that are currently only accessible with keys. Currently Douglas County has 86 doors with badge readers. We would like to add 36 door readers for areas that currently do not have badge access. The rooms/offices of these doors contain sensitive information, so it is vital that we can track who is accessing these doors. Some of the departments that would benefit from the addition badge readers on doors are County Managers Office (7 doors) Human Resources (3 doors) Assessor Office (3 doors) Recorder's Office (2 doors) Clerk/Treasurer Offices (9 doors) Sheriff Office Doors (9 doors) Technology Services (1) While most of our existing hardware can be migrated over into a new system. Some of our older hardware needs to be replaced as it is not compatible with a new system. We will need to replace one of our existing main controller boards. Every 2 doors we add also needs an additional downstream controller board that control the doors themselves. We would also like to add additional capabilities to be able to implement more readers to doors in the future. This project helps us to better manage, monitor, and track our badge access system by being able to tell who is access which doors and when.

**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 would be implemented by both the Technology Services department's Tier 2 team, who will be migrating the existing hardware into the new system and adding all additional boards/doors to the new system. Installing the hardware (door readers and additional boards) will be implemented by a vendor. As doors readers are installed by the Vendor, Technology Services will add the new doors to the system and add those doors to existing access levels and create new access levels as necessary for the security of the doors.

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

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

The desired outcome of this project is to increase our ability to monitor and track door access. The additional doors improve security and increase our ability to monitor and track door access by removing the use of keys in the environment. The new software has many more features and tracking/monitoring abilities than our existing software. It will also help to remove a level of human error by tying employee badges directly to employee's active directory accounts. This way as soon as an employee

is terminated, they lose their badge access as well. The new system also gives us the ability to set alerts when specific badges/doors are used, increasing our ability to track those very secure rooms.

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

- [ ] Yes
- [x] No

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

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**
*Please see the EHP Guidance attachment for more information on EHP reviews.*

- [ ] Yes
- [x] No

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

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

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

- [x] Yes
- [ ] No

**12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.**
We would prefer not to scale but if funding is an issue this project is scaleable. This project could be reduced in that we do not add any additional doors to the existing system. We need to purchase the additional licensing for our existing doors as well as replacing the incompatible equipment. This would reduce the total project cost to roughly $8500.00.

**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.*
89423

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

- [x] Build
- [ ] Sustain

**15. Is this request deployable to other jurisdictions?**

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

- [ ] Yes
- [x] No

**Line Item Detail Budget** *top*

## PLANNING COSTS

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

## ORGANIZATION COSTS

| Organizational Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| Contractor to Install Hardware | Contractor will be installing the physical hardware, roughly $1500 per 2 doors | 18 | $ 1,500.00 | $ 27,000.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Professional Services/Support required for configuration/implementation of the product/service |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |

| | | | | |
|---|---|---|---|---|
| | | $ | $ | |
| | | $ | $ | |
| | | $ | $ | |
| | | $ | $ | |
| | | $ | $ | |
| | | $ | $ | |
| | **18** | **$ 1,500.00** | **$ 27,000.00** | |

## 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 |
|---|---|---|---|---|---|---|---|---|
| Downstream board | Downstream boards have the ability to handle 2 doors | 18 | $ 1,000.00 | $ 18,000.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | System, Credentialing | 04AP-05-CRED |
| Request to Exit Motion Sensor | Unlocks doors from inside when you walk up to it | 36 | $ 250.00 | $ 9,000.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | System, Credentialing | 04AP-05-CRED |
| DPDT Recessed Door Contact | This gives us the ability to track if the door is being held open. | 36 | $ 250.00 | $ 9,000.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | System, Credentialing | 04AP-05-CRED |
| Electric Door Strike | This physically does the unlocking of the door | 36 | $ 250.00 | $ 9,000.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the | Hardware required to support the product/service | System, Credentialing | 04AP-05-CRED |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | value and provide justification for ongoing costs. | | | |
| Multiclass Single Gang Reader | This is what people will badge their cards against | 36 | $ 500.00 | $ 18,000.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | System, Credentialing | 04AP-05-CRED |
| Composite Cable | The cable to connect everything together. We need roughly 500 ft of cable for every two doors | 18 | $ 250.00 | $ 4,500.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | System, Credentialing | 04AP-05-CRED |
| | | | $ | $ | | | | |
| Software Licensing | Each door require additional licensing | 3 | $ 901.39 | $ 2,704.17 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Software/License Subscriptions required to support the product/service" | System, Credentialing | 04AP-05-CRED |
| Replace incompatible Hardware | Old system hardware not compatible with new system | 1 | $ 4,000.00 | $ 4,000.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | System, Credentialing | 04AP-05-CRED |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | **184** | **$ 7,401.39** | **$ 74,204.17** | | | | |

## 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) | ☑ | 2021-2022 Single Audit |

| | | |
|---|---|---|
| Travel Policy | ☑ | 300.06 Travel |
| Payroll Policy | ☑ | 200.11 Payroll |
| Procurement Policy | ☑ | 300.19 Procurement |
| Milestones<br>download template | ☑ | Physical Security - Avigilon ACM (Access Control Manager) BadgeCard Reader System |
| Capabilities Assessment<br>download template | ☑ | CapabilitiesAssessment Douglas County |

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

Application ID: 444164

| | | |
|---|---|---|
| | **Applicant Name** | Douglas County |
| | **Project Name:** | Physical Security - Badge/Card Reader System |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Create all existing doors in ACM | 9/1/2023 |
| 2 | Add Addititional Readers to doors | 9/1/2023 |
| 3 | Create all access levels in ACM | 10/1/2023 |
| 4 | Assign doors to access levels | 10/5/2023 |
| 5 | Completely migrate into ACM | 11/1/2023 |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | We use O365 to manage/monitor user accounts. | Fundamental |
| 2. Monitor, audit, and track network traffic and activity | We use the Palo Alto firewall UI to monitor and manage network traffic. We also have network tylemmetry sent to Arctic Wolf for monitoring, reporting and escalation. | Intermediary |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | Redundant Rapid Recovery Environment / Dated and dysfunctional. | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | We use Arctic Wolf to check for risks and then use Intune/patch my pc and AutoMox. | Intermediary |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | As we continue to close holes in our environment, we use best practices to create new policies. | Fundamental |
| a. Implement multi-factor authentication | For access to o365 resources. | Fundamental |
| b. Implement enhanced logging | We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| c. Data encryption for data at rest and in transit | In transit only | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | Firewalls, Network Switches, Badge access system. | Foundational |
| e. Prohibit use of known/fixed/default passwords and credentials | Passwords cannot be reused, and users notified when passwords are found on dark web. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | Equal Logics and Rapdid Recovery are old outdated systems and need to be be replaced. | Foundational |
| g. Migration to the .gov internet domain | We use the .us domain | Foundational |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | We do not use the .gov domain. | Foundational |
| 7. Ensure continuity of operations including by conducting exercises | We do not continually coduct exercises. | Foundational |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | We use KnowBe4 for Cybersecurity training and simulated phishing emails. We leverage the Storwinds Studios platform for technology related training opportunities for IT personnel. | Intermediary |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | N/A | Foundational |
| 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 eligible entity | We use o365 and Microsoft defender to detect and remediate endpoint/PC threats. We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | N/A | Foundational |
| 12. Leverage cybersecurity services offered by the Department | We have conducted assessments in coordination with CISA pen testing teams. | Fundamental |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | N/A | Fundamental |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | N/A | Fundamental |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | N/A | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | N/A | Foundational |




Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Douglas County Emergency Mangement**

# Firewall/Network Edge Refresh

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

**$ 86,915.00** Requested

Submitted: 6/21/2023 3:43:10 PM (Pacific)

**Project Contact**
Kathy Lewis
kmlewis@eastforkfire.org
Tel: 7757829040

**Additional Contacts**
*none entered*

**Douglas County Emergency Mangement**

1694 County Rd
Minden, NV 89423
United States

**Director of Finance**
Kathy Lewis
kmlewis@eastforkfire.org

| | |
|---|---|
| Telephone | 7757829040 |
| Fax | |
| Web | |
| EIN | 383972546 |
| UEI | |
| SAM Expires | |

## Pre-Application *top*

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

- [x] Yes
- [ ] No

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

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions top

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

- [x] Yes
- [ ] No

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

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

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

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

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

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

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

Existing firewalls have reached end of life and support will no longer be viable in our environment as upgrade paths and features will not be in sync with the rest of our firewall environment. This will secure our edge and ensure content and feature releases to deal with new and ever present threats are available to us. The new firewalls will increase our resiliency to attacks, and help to better monitor network traffic.

**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 Replacement of our existing end of life HA Firewalls will be accomplished as a coordinated effort between Douglas County System Administrators and professional services.

**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.*

Replace end of life network edge Palo Alto firewalls with a new pair that will bring service life in line with the rest of our internal and satellite firewall fleet. This will secure our edge and ensure content and feature releases to deal with new and ever present threats are available to us. This project improves our capabilities to respond to cybersecurity incidents and overall helps to ensure continuity of operations.

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

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

- [ ] Yes
- [x] No

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

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

N/A

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**

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

- [ ] Yes
- [x] No

**10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that**

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

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

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

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

- [ ] Yes
- [x] No

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

This project cannot be reduced because our existing firewalls are EOL and need to be replaced to protect our edge.

**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.*

89423

**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
- [x] Sustain

**15. Is this request deployable to other jurisdictions?**

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

- [ ] Yes
- [x] No

## Line Item Detail Budget *top*

### PLANNING COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | 0 | 0.00 | $ 0.00 | | | |

## ORGANIZATION COSTS

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

## EQUIPMENT COSTS

| Equipment Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. | AEL Name | AEL Number |
|---|---|---|---|---|---|---|---|---|
| Firewall | Firewall | 2 | $ 18,886.00 | $ 37,772.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate | Hardware required to support the product/service | Firewall, Network | 05NP-00-FWAL |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | the value and provide justification for ongoing costs. | | | |
| WildFire subscription | License Subscription | 2 | $ 3,479.00 | $ 6,958.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Software/License Subscriptions required to support the product/service | Firewall, Network | 05NP-00-FWAL |
| Advanced URL Filtering subscription | License Subscription | 2 | $ 5,112.00 | $ 10,224.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Software/License Subscriptions required to support the product/service | Firewall, Network | 05NP-00-FWAL |
| Advanced Threat Prevention subscription | License Subscription | 2 | $ 5,112.00 | $ 10,224.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Software/License Subscriptions required to support the product/service | Firewall, Network | 05NP-00-FWAL |
| VPN subscription | License Subscription | 2 | $ 3,577.00 | $ 7,154.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Software/License Subscriptions required to support the product/service | Firewall, Network | 05NP-00-FWAL |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| premium support | Support | 2 | $ 4,071.50 | $ 8,143.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Professional Services/Support required for configuration/implementation of the product/service | Firewall, Network | 05NP-00-FWAL |
| Professional Services | Support | 1 | $ 3,680.00 | $ 3,680.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Professional Services/Support required for configuration/implementation of the product/service | Firewall, Network | 05NP-00-FWAL |
| Professional Services - Remote Cutover Support) | Support | 2 | $ 1,280.00 | $ 2,560.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Professional Services/Support required for configuration/implementation of the product/service | Firewall, Network | 05NP-00-FWAL |
| Shipping | Shipping for Firewalls | 1 | $ 200.00 | $ 200.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | Firewall, Network | 05NP-00-FWAL |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | $ | $ | | | |
| | | | | $ | $ | | | |
| | | | 16 | $ 45,397.50 | $ 86,915.00 | | | |

## 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) | ☑ | 2021-2022 Single Audit |
| Travel Policy | ☑ | 300.06 |
| Payroll Policy | ☑ | 200.11 Payroll |
| Procurement Policy | ☑ | 300.19 Procurement |
| Milestones<br>download template | ☑ | Firewall Refresh |
| Capabilities Assessment<br>download template | ☑ | Capabilities Assessment |

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

Application ID: 444165

| | | |
|---|---|---|
| | **Applicant Name** | Douglas County |
| | **Project Name:** | Firewall/Network Edge Refresh |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Purchase firewalls to replace exisiting | 12/1/2024 |
| 2 | Setup Firewalls as redundant to existing firev | 4/1/2024 |
| 3 | transfer lead roles to new firewalls | 4/15/2024 |
| 4 | decomission old firewalls | 4/20/2024 |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | We use O365 to manage/monitor user accounts. | Fundamental |
| 2. Monitor, audit, and track network traffic and activity | We use the Palo Alto firewall UI to monitor and manage network traffic. We also have network tylemmetry sent to Arctic Wolf for monitoring, reporting and escalation. | Intermediary |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | Redundant Rapid Recovery Environment / Dated and dysfunctional. | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | We use Arctic Wolf to check for risks and then use Intune/patch my pc and AutoMox. | Intermediary |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | As we continue to close holes in our environment, we use best practices to create new policies. | Fundamental |
| a. Implement multi-factor authentication | For access to o365 resources. | Fundamental |
| b. Implement enhanced logging | We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| c. Data encryption for data at rest and in transit | In transit only | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | Firewalls, Network Switches, Badge access system. | Foundational |
| e. Prohibit use of known/fixed/default passwords and credentials | Passwords cannot be reused, and users notified when passwords are found on dark web. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | Equal Logics and Rapdid Recovery are old outdated systems and need to be be replaced. | Foundational |
| g. Migration to the .gov internet domain | We use the .us domain | Foundational |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | We do not use the .gov domain. | Foundational |
| 7. Ensure continuity of operations including by conducting exercises | We do not continually coduct exercises. | Foundational |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | We use KnowBe4 for Cybersecurity training and simulated phishing emails. We leverage the Storwinds Studios platform for technology related training opportunities for IT personnel. | Intermediary |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | N/A | Foundational |
| 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 eligible entity | We use o365 and Microsoft defender to detect and remediate endpoint/PC threats. We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | N/A | Foundational |
| 12. Leverage cybersecurity services offered by the Department | We have conducted assessments in coordination with CISA pen testing teams. | Fundamental |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | N/A | Fundamental |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | N/A | Fundamental |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | N/A | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | N/A | Foundational |

Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Douglas County Emergency Mangement**

# Multi-Factor Authentication for End-Users/Endpoints

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

**$ 4,772.00** Requested

Submitted: 6/21/2023 3:43:59 PM (Pacific)

**Project Contact**
Kathy Lewis
kmlewis@eastforkfire.org
Tel: 7757829040

**Additional Contacts**
*none entered*

**Douglas County Emergency Mangement**

1694 County Rd
Minden, NV 89423
United States

**Director of Finance**
Kathy Lewis
kmlewis@eastforkfire.org

| | |
|---|---|
| Telephone | 7757829040 |
| Fax | |
| Web | |
| EIN | 383972546 |
| UEI | |
| SAM Expires | |

## Pre-Application *top*

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

- [x] Yes
- [ ] No

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

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions *top*

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

- [x] Yes
- [ ] No

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

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

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

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

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

This project would implement MFA throughout our environment from an end-to-end perspective. The project gives us the opportunity to implement Endpoint MFA when logging onto Douglas County Computers. Enabling MFA on endpoint devices increases our resilience of user accounts and protects us if a user credentials are compromised, and a computer is lost/stolen. Our current o365 MFA policies do not require MFA to access o365 resources on a Douglas County device, so implementing MFA to login to the computer would cover us completely. This project would enhance our resilience of information's systems and user accounts by forcing users to do MFA when logging onto computers. The adding of MFA to end point logins greatly reduces our cybersecurity risks and threats.

**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 would be implemented with the help of Manage Engine's CSM when we purchase it. It would be implemented by the Technology Services Tier 2 team in coordination with Manage Engine support. We would start with implementation to our Alpha group (a group of users who we use for testing) and then eventually roll it out to the rest of the County.

**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.*

Require MFA for windows login. This secures the devices so only Douglas County employees with MFA are able to logon to Douglas County Devices.

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

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

- [ ] Yes
- [x] No

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

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

N/A

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**

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

- [ ] Yes
- [x] No

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

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

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

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

- [ ] Yes
- [x] No

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

This project can not be reduced because it a subscription for the entire user base.

**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.*

89423

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

- [x] Build
- [ ] Sustain

**15. Is this request deployable to other jurisdictions?**

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

- [ ] Yes
- [x] No

## Line Item Detail Budget *top*

### PLANNING COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | **0** | **0.00** | **$ 0.00** | | | |

## ORGANIZATION COSTS

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

## EQUIPMENT COSTS

| Equipment Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. | AEL Name | AEL Number |
|---|---|---|---|---|---|---|---|---|
| Subscription | License | 1 | $ 3,976.00 | $ 3,976.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for | Software/License Subscriptions required to support the product/service | Software, Risk Management | 04AP-04-RISK |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | ongoing costs. | | | |
| Annual Maintenance and Support | Support | 1 | $ 796.00 | $ 796.00 | Sustainability Funding will be built into annual base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Software/License Subscriptions required to support the product/service | Software, Risk Management | 04AP-04-RISK |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | **2** | **$ 4,772.00** | **$ 4,772.00** | | | | |

## 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) | ☑ | 2021 -2022 Single Audit |
| Travel Policy | ☑ | 300.06 Travel |
| Payroll Policy | ☑ | 200.11 Payroll |
| Procurement Policy | ☑ | 300.19 Procurement |
| Milestones<br>download template | ☑ | MFA for Endpoints |
| Capabilities Assessment<br>download template | ☑ | Capabilities Assessment |

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

Application ID: 444166

| | | |
|---|---|---|
| | **Applicant Name** | Douglas County |
| | **Project Name:** | Mutli-Factor Authentication for End-Users/Endpoints |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Evaluate Softwares | 12/1/2023 |
| 2 | Purchase Softwares | 5/1/2024 |
| 3 | Implement Software with Alpha Group | 5/15/2024 |
| 4 | Deploy Software to everyone | 5/30/2024 |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | We use O365 to manage/monitor user accounts. | Fundamental |
| 2. Monitor, audit, and track network traffic and activity | We use the Palo Alto firewall UI to monitor and manage network traffic. We also have network tylemmetry sent to Arctic Wolf for monitoring, reporting and escalation. | Intermediary |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | Redundant Rapid Recovery Environment / Dated and dysfunctional. | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | We use Arctic Wolf to check for risks and then use Intune/patch my pc and AutoMox. | Intermediary |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | As we continue to close holes in our environment, we use best practices to create new policies. | Fundamental |
| a. Implement multi-factor authentication | For access to o365 resources. | Fundamental |
| b. Implement enhanced logging | We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| c. Data encryption for data at rest and in transit | In transit only | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | Firewalls, Network Switches, Badge access system. | Foundational |
| e. Prohibit use of known/fixed/default passwords and credentials | Passwords cannot be reused, and users notified when passwords are found on dark web. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | Equal Logics and Rapdid Recovery are old outdated systems and need to be be replaced. | Foundational |
| g. Migration to the .gov internet domain | We use the .us domain | Foundational |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | We do not use the .gov domain. | Foundational |
| 7. Ensure continuity of operations including by conducting exercises | We do not continually coduct exercises. | Foundational |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | We use KnowBe4 for Cybersecurity training and simulated phishing emails. We leverage the Storwinds Studios platform for technology related training opportunities for IT personnel. | Intermediary |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | N/A | Foundational |
| 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 eligible entity | We use o365 and Microsoft defender to detect and remediate endpoint/PC threats. We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | N/A | Foundational |
| 12. Leverage cybersecurity services offered by the Department | We have conducted assessments in coordination with CISA pen testing teams. | Fundamental |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | N/A | Fundamental |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | N/A | Fundamental |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | N/A | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | N/A | Foundational |




Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Douglas County Emergency Mangement**

# Backup Datacenter Environment

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

**$ 119,292.08** Requested

Submitted: 6/21/2023 3:44:42 PM (Pacific)

**Project Contact**
Kathy Lewis
kmlewis@eastforkfire.org
Tel: 7757829040

**Additional Contacts**
*none entered*

**Douglas County Emergency Mangement**

1694 County Rd
Minden, NV 89423
United States

**Director of Finance**
Kathy Lewis
kmlewis@eastforkfire.org

| | |
|---|---|
| Telephone | 7757829040 |
| Fax | |
| Web | |
| EIN | 383972546 |
| UEI | |
| SAM Expires | |

## Pre-Application *top*

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

- [x] Yes
- [ ] No

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

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions top

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

- [x] Yes
- [ ] No

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

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] 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.**

Douglas County recently established a new offsite datacenter, and this project would create a redundant backup site to mirror the hardware profile that exists for our primary datacenter - which consists of 2 robust servers which serve as the VM hosts for the environment in addition to a storage array. This project establishes a backup site to give us redundancy and resiliency in the event of a catastrophic event or attack. The full package includes adding two VM hosts and storage array. This project would ensure continuity of operations and improve capabilities to respond to cybersecurity incidents. Having a secondary backup site enhances our preparation and shortens our response time in case there is a cyber-attack.

**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 project would be implemented by our Tier 2 team in coordination with professional services for implementation/configuration.

**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 main outcomes of this project would be resiliency and redundancy as a mirror image of our production environment.

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

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

- [ ] Yes
- [x] No

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

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

N/A

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**

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

- [ ] Yes
- [x] No

**10. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. --Cyber**

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

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

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

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

- [ ] Yes
- [x] No

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

This project can not be reduced because it is a full redundancy for our server environment.

**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.*

89423

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

- [x] Build
- [ ] Sustain

**15. Is this request deployable to other jurisdictions?**

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

- [ ] Yes
- [x] No

## Line Item Detail Budget *top*

### PLANNING COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | 0 | 0.00 | $ 0.00 | | | |

## ORGANIZATION COSTS

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

## EQUIPMENT COSTS

| Equipment Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. | AEL Name | AEL Number |
|---|---|---|---|---|---|---|---|---|
| Computer Server | Server to Host the VM's | 2 | $ 45,146.04 | $ 90,292.08 | Sustainability Funding will be built into base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide | Hardware required to support the product/service | Hardware, Computer, Integ | 04HW-01-INHW |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | justification for ongoing costs. | | | |
| Storage Array | Storage array for backup data | 1 | $ 19,000.00 | $ 19,000.00 | Sustainability Funding will be built into base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Hardware required to support the product/service | Hardware, Computer, Integ | 04HW-01-INHW |
| Implementation | Managed services to help standup redundancy | 1 | $ 10,000.00 | $ 10,000.00 | Sustainability Funding will be built into base budget. Utilizing Grant funding as the initial life will help demonstrate the value and provide justification for ongoing costs. | Professional Services/Support required for configuration/implementation of the product/service | Hardware, Computer, Integ | 04HW-01-INHW |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | **4** | **$ 74,146.04** | $ 119,292.08 | | | | |

## TRAINING COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | 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) | ☑ | 2021-2022 Single Audit |
| Travel Policy | ☑ | 300.06 Travel |
| Payroll Policy | ☑ | 200.11 Payroll |
| Procurement Policy | ☑ | 300.19 Procurement |
| Milestones<br>download template | ☑ | Backup Datacenter |
| Capabilities Assessment<br>download template | ☑ | Capabilities Assessment |

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

Application ID: 444167

| | | |
|---|---|---|
| | **Applicant Name** | Douglas County |
| | **Project Name:** | Backup Datacenter Environment |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Initiate purchasing of equipment | 8/1/2023 |
| 2 | Install and setup equipment | 3/1/2024 |
| 3 | Confirm backup enviornment is setup correc | 3/2/2024 |
| 4 | Test back up enviornment | 3/15/2024 |
| 5 | Project completed | 3/16/2024 |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | We use O365 to manage/monitor user accounts. | Fundamental |
| 2. Monitor, audit, and track network traffic and activity | We use the Palo Alto firewall UI to monitor and manage network traffic. We also have network tylemmetry sent to Arctic Wolf for monitoring, reporting and escalation. | Intermediary |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | Redundant Rapid Recovery Environment / Dated and dysfunctional. | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | We use Arctic Wolf to check for risks and then use Intune/patch my pc and AutoMox. | Intermediary |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | As we continue to close holes in our environment, we use best practices to create new policies. | Fundamental |
| a. Implement multi-factor authentication | For access to o365 resources. | Fundamental |
| b. Implement enhanced logging | We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| c. Data encryption for data at rest and in transit | In transit only | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | Firewalls, Network Switches, Badge access system. | Foundational |
| e. Prohibit use of known/fixed/default passwords and credentials | Passwords cannot be reused, and users notified when passwords are found on dark web. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | Equal Logics and Rapdid Recovery are old outdated systems and need to be be replaced. | Foundational |
| g. Migration to the .gov internet domain | We use the .us domain | Foundational |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | We do not use the .gov domain. | Foundational |
| 7. Ensure continuity of operations including by conducting exercises | We do not continually coduct exercises. | Foundational |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | We use KnowBe4 for Cybersecurity training and simulated phishing emails. We leverage the Storwinds Studios platform for technology related training opportunities for IT personnel. | Intermediary |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Douglas County NV | |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | N/A | Foundational |
| 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 eligible entity | We use o365 and Microsoft defender to detect and remediate endpoint/PC threats. We leverage sysmon and tylemmetry forwarding of all server/endpoint logs as well as network traffic to Arctic Wolf SOC for monitoring, reporting and escalation. | Intermediary |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | N/A | Foundational |
| 12. Leverage cybersecurity services offered by the Department | We have conducted assessments in coordination with CISA pen testing teams. | Fundamental |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | N/A | Fundamental |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | N/A | Fundamental |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | N/A | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | N/A | Foundational |




Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Supreme Court of Nevada - Nevada Judiciary**

# Nevada Cybersecurity for the Judiciary

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

**$ 925,000.00** Requested

Submitted: 6/22/2023 8:09:30 AM (Pacific)

**Project Contact**
Barbara Holmes
bholmes@nvcourts.nv.gov
Tel: 7175038371

**Additional Contacts**
grants@nvcourts.nv.gov

**Supreme Court of Nevada - Nevada Judiciary**

201 S Carson St Ste 250
Carson City, NV 89701
United States

**Chief Financial Officer**
Todd Myler
tmyler@nvcourts.nv.gov

Telephone 7175038371
Fax
Web https://nvcourts.gov/supreme
EIN 92-1932829
UEI RJT5R9FS71L5
SAM
Expires

## Pre-Application top

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

- [x] Yes
- [ ] No

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

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions *top*

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

- [ ] Yes
- [x] No

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

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] 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.
- [x] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [x] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [x] Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [x] 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 Nevada Judiciary Administrative Office of Courts (AOC) serves as a hub for operations of courts throughout the state. In that respect, while larger courts, such as in Clark County, may have their own technical resources, smaller rural courts throughout the state depend on the AOC for their networks, case management systems and other technical resources. All of the courts throughout the state use the statewide network that is provided by the AOC in some capacity. Many of the smaller, rural jurisdictions use the state provided case management system and it is central to their operations. The AOC also serves as the hub for transmission of data to justice partners, such as the Department of Transportation and the Department of Public Safety.

The AOC takes advantage of the state network at this time, yet maintains their own internal control over the judiciary subnets, DNS and LANS. The vulnerabilities that affect the judiciary have the potential for affecting other state agencies and operations and at this time, they are not clearly understood and/or controlled.

In addition to a lack of understanding of vulnerabilities, the judiciary, especially in rural locations, lacks an information security governance, protection, detection and response plan that would provide for quickly and efficiently addressing incidents. A communication plan is needed to better react to all courts involved as well as with justice partners, law enforcement and other remediation resources.

**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 project will involve a thorough assessment of cybersecurity vulnerabilities, threats and required controls as well as a path for correction throughout the statewide system. It will include steps to implement a governance plan and assistance with facilitation of initial meetings. Stakeholders from throughout the state will be involved in reviewing and determining asset priorities and classification of information as well as in developing a communication and response plan for cyber-attacks.

The most important result will be a a throughout assessment of information security issues throughout the state judiciary and a remediation plan to address these issues.

**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.*

Improved visibility into information security risks and vulnerabilities, implementation of proper controls and strategies for addressing and communicating incidents. An improved overall Information security posture through the assessment of vulnerabilities, implementation and monitoring of controls and detection/mediation tools.

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

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

- [ ] Yes
- [x] No

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

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**
*Please see the EHP Guidance attachment for more information on EHP reviews.*

- [ ] Yes
- [x] No

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

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

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

- [x] Yes
- [ ] No

**12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.**
This project can be scaled to improve local information security in the rural courts in Nevada. It can be reduced to minimize the overall goals of the project. At least 25% of the grant funding will benefit rural communities to improve and understand their overall information security..

If the grant must be broken into two pieces, it is possible that the Business Asset/Risk Analysis could be done separately from the Information Security Assessment.

**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.*
89701

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

- [x] Build
- [ ] Sustain

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

- [x] Yes
- [ ] No

**Line Item Detail Budget** *top*

## PLANNING COSTS

| Planning Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| Vulnerability Testing | CISA will perform monthly vulnerability testing | 1 | 0.00 | $ 0.00 | This is a free service provided by CISA. | Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives. |
| Conduct Business Risk Analysis and Information Security Assessment | This will be a through business risk analysis and information security assessment for the judiciary. | 1 | 200,000.00 | $ 200,000.00 | This activity will identify and classify business information assets and their priorities along with the classification of data within each asset. In addition, it will include and Information Security assessment that would identify risks and vulnerabilities. | Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives. |
| Facilitate governance in order to conduct BRA and information security assessment. | This would involve the formation of a governance committee that could prioritize the needs for Information Security. | 1 | 150,000.00 | $ 150,000.00 | This would involve facilitation of governance meetings and prioritization/categorization of business assets related to IT that would be needed to complete the business risk analysis and assessment. This would not be able to be done without external facilitation skills so it would need to be budgeted for in the future. | Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | operational technology cybersecurity objectives. |
| Establish a remediation plan for identified vulnerabilities. | Establish a remediation plan for identified vulnerabilities. | 1 | 100,000.00 | $ 100,000.00 | This would be maintained on an as needed basis using state court funds. | Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives. |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | **4** | **450,000.00** | **$ 450,000.00** | | |

## 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. |
|---|---|---|---|---|---|---|
| Developing/Maintain Project Plan | This item will allow for identifying an overall project plan and managing the project throughout its lifetime. | 1 | $ 130,000.00 | $ 130,000.00 | Project planning would have to be provided by in-house staff rather than contracted resources though other priorities may slow progress. | Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Identify/hire contracting staff | This will allow the project to be properly staffed. Full-time court staff members will also be allocated to the project, but there is a small IT staff for the judiciary. In addition, court IT lacks training and facilitation personnel. | 2 | $ 150,000.00 | $ 300,000.00 | Once in place, existing staff would take over the enhancement and maintenance, but AOC lacks full capabilities to implement this. | Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives. |
| Identify/meet with stakeholders | This will provide a baseline of stakeholders to involve in classification and asset identification. This will include stakeholders from rural and urban courts as well as IT staff. These stakeholders will assist in performing the Business Risk Analysis. This would include the cost of transporting stakeholders and staff for at least three regional meetings. | 3 | $ 15,000.00 | $ 45,000.00 | While AOC can identify stakeholders, there is a lack of staffing to convene and facilitate this process.In addition, this would include the cost of transporting stakeholders for at least three regional meetings. The need to use in-house staff would greatly slow progress toward a governance structure and only remote communication would be available which might be less effective in the overall project success. | Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives. |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | **6** | **$ 295,000.00** | **$ 475,000.00** | | |

## 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 |
|---|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | 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? |
|---|---|---|---|---|---|---|---|
| | | | $ 0.00 | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | | $ | $ | | |
| | 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) | ☑ | External Audit Memo<br>External Audit |
| Travel Policy | ☑ | Travel Policy |
| Payroll Policy | ☑ | Payroll Policy |
| Procurement Policy | ☑ | Financial Policy |
| Milestones<br>download template | ☑ | Grant Milestones<br>Grant Milestones |
| Capabilities Assessment<br>download template | ☑ | Capabilities Assessment |

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

Application ID: 443468

| | | |
|---|---|---|
| | **Applicant Name** | Supreme Court of Nevada - Judiciary |
| | **Project Name:** | Nevada Cybersecurity for the Judiciary |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Project Planning and Staff Hiring | Month 2 |
| 2 | Establish/Kickoff Stakeholder Committee | Month 3 |
| 3 | Conduct Business Analysis Activities | Month 6 |
| 4 | Conduct Information Security Assessment | Month 8 |
| 5 | Develop Remediation Plan | Month 12 |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Supreme Court of Nevada - Nevada Judiciary | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | The judiciary uses MS Office 365 online and maintains its own DNS, providing the ability to track and manage user accounts. Authentication is also a function/feature of the state case management system. There are some network management tools in place. More work needs to be done on identifying and tracking applications throughout the statewide judiciary | Fundamental |
| 2. Monitor, audit, and track network traffic and activity | Some network tools are use in the judiciary to track network traffic. More work needs to be done to implement a stronger auditing and auditing capability. | Fundamental |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | Wherever possible, the AOC is enhancing systems with these goals, but without a proper vulnerablity scan and continuous monitoring tools, this is a less structured process than it should be. | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | The AOC has begun the vulnerability scan application with CISA to provide for a monthly vulnerability scan. We are beginning to work through the NIST processes and procedures, but lack governance to fully implement and identify risk priorities. | Foundational |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | The AOC has just begun to work through the NIST Continuity of Operations Template to implement and adopt best practices and methodologies to enhance cybersecurity | Foundational |
| a. Implement multi-factor authentication | Multifactor authentication has been implemented where ever possible. Retrofitting of some applications may be needed to provide for this. | Intermediary |
| b. Implement enhanced logging | Some efforts have been made to enhance logging but monitoring the logs remains an issue. They can be used retrospectively, but this is not ideal. | Foundational |
| c. Data encryption for data at rest and in transit | Data in transit is encrypted, but the data that is sensitive or confidential needs to be identified and further efforts to encrypt such data should be made. | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | Efforts are in place to identify and replace software and hardware, though there are some legacy resources still in place. Most of these resources are not accessible from the internet, but an overall program needs to be put in place. | Foundational |
| e. Prohibit use of known/fixed/default passwords and credentials | The password policies for Office365 are prohibitive and use multi-factor authentication. Other legacy applications within the judiciary lack password and credential rule-governance. The process of replacing some of these systems is on-going, but a clearer identification and prioritization needs to be performed. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | Backups are in place for all systems, but the abillity to reconstitute them has not been tested. | Foundational |
| g. Migration to the .gov internet domain | The judiciary is on the .gov domain. | Intermediary |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | The AOC is in the process of identifying, accesssing and replacing many of its online services and will need dto continue with this process. | Intermediary |
| 7. Ensure continuity of operations including by conducting exercises | The judiciary is working on a continuity of operations plan and has put in place a group of stakeholders to further this task. It is not complete and exercises have not been conducted. | Foundational |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Supreme Court of Nevada - Nevada Judiciary | |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | The AOC has put together a security team and employed a CTO who is a Certified Information System Security Professional (CISSP) as well as a Certifed Data Privacy Solutions Engineer (CDPSE). Other members of the security team are working toward certification and some have pursued Comp Security+. The team is working together to bolster knowledge, skills and abilities. The judiciary is enhancing recruitment and retention through a review of employment scaling. | Intermediary |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | The judiciary has not put in place a continuity of communications plan. This will need to be developed in conjuction with an incident response plan. | Foundational |
| 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 eligible entity | The AOC is in the process of applying to CISA for their vulnerability accessment, which will form the basis of a strategy for risk mitigation. Crowdstrike is being used through MS-ISAC for incident detection and its use will be further advanced into vulnerability identification. But, further work needs to be done in this area so that pervention, detection and remediation are enhanced. | Foundational |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | The AOC is part of the regular sharing of information with other state departments. However, this could be enhanced. | Intermediary |
| 12. Leverage cybersecurity services offered by the Department | The AOC would like to better leverage cybersecurity services offered by the Department. | Foundational |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | The AOC has initiated a network modernization project and enhancement of systems overall. But, an assessment of vulnerabilities and determination of risk and risk tolerance is needed to further implement these initiatives. | Intermediary |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | The AOC is in the process of developing a NIST-based continuity plan in coordination with the overall COOP planning process. | Foundational |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | Additional work needs to be done to further involve rural communities in planning activities | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | Because the AOC serves as the primary IT provider for many local courts, the AOC is accustomed to detributing funds, services and capabilities to local governments | Advanced |




Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**City of Sparks, Nevada**
# Cybersecurity

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

**$ 109,050.00** Requested

Submitted: 6/22/2023 2:57:22 PM (Pacific)

**Project Contact**
Melissa Evans
mevans@cityofsparks.us
Tel: 7753232312

**Additional Contacts**
treid@cityofsparks.us

**City of Sparks, Nevada**

431 Prater Way
Sparks, NV 89431
United States

**Chief Financial Officer**
Jeff Cronk
jcronk@cityofsparks.us

Telephone 7753532312
Fax
Web
EIN JC8PKJTFNM
UEI
SAM Expires

## Pre-Application top

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

- [x] Yes
- [ ] No

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

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions *top*

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

- [ ] Yes
- [x] No

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

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [ ] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

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

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

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

Project 1 The intent of the project is to assess all of our Palo Alto firewalls. This should include the current configuration, and traffic flow rules, as well as security rules. We want to ensure that they meet the CIS baseline configuration as well to rule errant default settings.

Project 2 The intent of the project is to assess our current on-premise domain configuration. We are planning to migrate to a new clean domain and create a forest for the old domain. We intend to move only what is needed and ensure best practice/CIS controls are in place via GPO We also need to asses items of concern such as Role Based Access, least privilege, excess groups, and users. This project should also include our O365/Azure environment as we are starting to move assets to MS Azure.

Project 3 The intent of this project is to assess our O365/Email environment and ensure all security features are being configured/used correctly while maximizing uptime for users.

Project 4 The intent of this project is to assess our core infrastructure setup, DNS/DHCP/Domain controller, and ensure that it is configured to best practice and secured using any CIS baseline methodology as appropriate.

**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 project will require the use of professional services. It is recommended that professional services work together with IT staff to implement changes and be available if issues arise for remediation.

For timeline of the projects it is possible the 4 projects can be done within a one-year time frame. I am unsure at this time as to how much time within a year each project will take.

The IT staff Rich Brown or Ty Reid WILL MANAGE THE CONSULTANTS AND IT IS ESTIMATED NUMBER OF HOURS WILL BE DEDICATED TO THIS EFFORT. A minimum 10% of the total cost of the project, utilizing consultant services will be provided by staff as project management to meet the in-kind cost share requirement for the first year.

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

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

The desired outcome of these projects are to assess what we have implemented currently, and ensure it is configured correctly, while ensuring an appropriate balance is achieved between availability, conditionality, and integrity. Post assessment/changes: this will provide us with a solid foundation moving forward to manage/maintain and ensure that we are doing our due diligence and due care in the protection of the systems under our stewardship.

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

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

- ☐ Yes

- [x] No

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

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**
*Please see the EHP Guidance attachment for more information on EHP reviews.*

- [ ] Yes
- [x] No

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

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

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

- [x] Yes
- [ ] No

**12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.**
The project of assessing and changing/updating can be scaled to only a handful of firewalls, or only looking at just a certain set of security items in O365 or on the domain. Recommended to not scale if possible.

**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.*
89431

**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
- [x] Sustain

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

- [ ] Yes
- [x] No

## Line Item Detail Budget top

## PLANNING COSTS

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

## ORGANIZATION COSTS

| Organizational Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| Project 1 (NGFW/Management) | Health check service for next generation firewalls/management | 1 | $ 21,560.00 | $ 21,560.00 | The organization would sustain this project by reaching out to professional services to assess every year the config of our next generation firewalls and include the software used to manage it from a single web interface. Cost being a factor we will have to go with that we can cover, if cost is too great then we cannot sustain. | The purchase of this item will enhance the preparation, response, and resilience of information systems such as our next generation firewalls for the City of Sparks. |
| Project 1 (NGFW SecOps Optimzation) | SecOps Optimization Service for next | 1 | $ 28,490.00 | $ 28,490.00 | The organization would sustain | The purchase of this item will Implement a |

| | | | | | | |
|---|---|---|---|---|---|---|
| | generation firewalls | | | | this project by reaching out to professional services to assess every year the config of our current next generation firewalls. Cost being a factor we will have to go with that we can cover, if cost is too great then we cannot sustain. | process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on the next generation firewalls. |
| Project 2 (AD on prem) | Active Directory best practice config, CIS controls, and ongoing maintenince | 1 | $ 11,000.00 | $ 11,000.00 | The organization would sustain this project by reaching out to professional services to assess every year the config of our Domain. Cost being a factor we will have to go with that we can cover, if cost is too great then we could try pushing the assessment out one year or further. | The purchase within this element will enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by to assessing our current on-premise domain configuration, we are planning to migrate to a new clean domain, and create a forest for the old domain, move only what is needed and ensure best practice/CIS controls are in place via GPO, also need to asses items of concern such as Role Based Access, least privilege, excess groups and users. This project should also include our O365/Azure environment as we are starting to move assets to MS Azure. |
| Project 2 (Cloud ID Mgmt/Cloud AD) | current cloud service provider identity management/ cloud Active Directory best practice config, CIS controls and ongoing maintenance | 1 | $ 18,000.00 | $ 18,000.00 | The organization would sustain this project by reaching out to professional services to assess every year the config of our cloud provider identity management / cloud active directory . Cost being a factor we will have to go with that we can cover, if | Purchasing this element will 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 by assessing our current cloud provider |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | cost is too great then we can try pushing the assessment out one year or further. | identity management / cloud Active active directory configuration and to implement changes based on findings, ensure best practice, CIS controls are in place. |
| Project 3 (Cloud email security enhancment) | Current cloud email service provider for best practice config- maximize security tools already available | 1 | $ 15,000.00 | $ 15,000.00 | The organization would sustain this project by reaching out to professional services to assess every year the config of our current cloud email service provider. Cost being a factor we will have to go with that we can cover, if cost is too great then we can try pushing the assessment out one year or further. | Purchasing this element will 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 by assessing our current cloud email service provider standard and security configuration to ensure all security features are being configured/used correctly while maximizing uptime for users. |
| Project 4 (Core IT infrastructure) | Assess core IT infrastructure. | 1 | $ 15,000.00 | $ 15,000.00 | The organization would sustain this project by reaching out to professional services to assess every year the config of our IT core infrastructure environment. Cost being a factor we will have to go with that we can cover, if cost is too great then we can try pushing the assessment out one year or further. | Purchasing this element will 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 by assessing our core infrastructure setup, DNS/DHCP/Domain controller and ensure that it is configured to best practice and secured using any CIS baseline methodology as appropriate. |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | $ | $ | | |
| | | | | | | $ | $ | | |
| | | | | | | $ | $ | | |
| | | | | | | $ | $ | | |
| | | | | | 6 | $ 109,050.00 | $ 109,050.00 | | |

## EQUIPMENT COSTS

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

## TRAINING COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | |
| | | 0 | $ 0.00 | $ 0.00 | | | 0 |

## EXERCISE COSTS

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

### Document Uploads *top*

| Documents Requested * | Required? | Attached Documents * |
|---|---|---|
| A-133 Audit (Most Current) | ☑ | 2022 City of Sparks Audit from Annual Financial Report<br>City of Sparks entire Annual Financial Report |
| Travel Policy | ☑ | City of Sparks Travel Policy |
| Payroll Policy | ☑ | City of Sparks Payroll Policy |
| Procurement Policy | ☑ | City of Sparks Procurement Policy<br>City of Sparks non federal funding policy<br>City of Sparks Purchasing Requirements |
| Milestones<br>download template | ☑ | Project 1<br>Project 2<br>Project 3<br>Project 4 |
| Capabilities Assessment<br>download template | ☑ | Capabilities Assessment COS v2 |

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

| | | |
|---|---|---|
| | **Applicant Name** | Ty Reid |
| | **Project Name:** | Project 1  Palo Alto Health check and Sec OPS Optimzatior |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Complete initial health check service for the NFGW/Panorama Palo Alto Firewalls | 10-Jan |
| 2 | Complete SecOps Optimization Service for NGFW | 22-Jun |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | INFO## Professional services assess/recommend/implement changes based on current | |
| 7 | config and environmental needs to ensure best balance of security and usability. | |
| 8 | Initial health check for PA's should be completed before optimizing SecOps | |
| 9 | At this time, it is difficult to project quarterly check in milestones due to scope and time constrants, these should be obtainable within 12 months once the finance aspect is secured. | |
| 10 | | |

*Please add additional rows as necessary for your project

| | | |
|---|---|---|
| | **Applicant Name** | Ty Reid |
| | **Project Name:** | Project 2 |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Assess - enhance - improve current on prem AD environment using CIS best practice/guidance | 22-Jun |
| 2 | Address: Role Based Access, least privilege, excess groups and users. | |
| 3 | | |
| 4 | Assess O365/Azure enviorment as well to ensure that align with CIS best practice/guidance. | 22-Jun |
| 5 | | |
| 6 | | |
| 7 | INFO## Professional services assess/recommend/implement changes based on current | |
| 8 | config and environmental needs to ensure best balance of security and usability. | |
| 9 | Initial on prem AD needs to be completed, O365/Azure environment is small but can be completed | |
| 10 | After local AD assessment and changes should move to Azure. | |
| | At this time, it is difficult to project quarterly check in milestones due to scope and time constraints, these should be obtainable within 12 months once the finance aspect is secured. | |

*Please add additional rows as necessary for your project

| | | |
|---|---|---|
| | **Applicant Name** | Ty Reid |
| | **Project Name:** | Project 3 |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Assess our 0365/EMAIL environment and ensure all security features are being used/configured correctly. | 24-Jun |
| 2 | Items of concern - there are a large number of security features MS has rolled out over the years. | |
| 3 | There has been no visibility on this side when those features were available and how to properly configure | |
| 4 | turn them on for the enterprise. Also out of country logins, we hardly if ever have users needing access | |
| 5 | out of country - this enables a large attack surface for threat actors. | |
| 6 | | |
| 7 | | |
| 8 | INFO## Professional services assess/recommend/implement changes based on current | |
| 9 | config and environmental needs to ensure best balance of security and usability. | |
| 10 | At this time, it is difficult to project quarterly check in milestones due to scope and time constraints, these should be obtainable within 12 months once the finance aspect is secured. | |

*Please add additional rows as necessary for your project

| | | |
|---|---|---|
| | **Applicant Name** | Ty Reid |
| | **Project Name:** | Project 4 |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Assess our core infrastructure setup, DNS/DHCP/Domain controller and ensure that it is configured to best practice and secured using any CIS baseline methodology as approp | 22-Jun |
| 2 | Items of concern primarly - Secure DNS/DHCP best practice move to PA/Switchs/Domain controller management, group policy to work station best practice CIS usage. | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | INFO## Professional services assess/recommend/implement changes based on current | |
| 9 | config and environmental needs to ensure best balance of security and usability. | |
| 10 | At this time, it is difficult to project quarterly check in milestones due to scope and time constraints, these should be obtainable within 12 months once the finance aspect is secured. | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | City of Sparks | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | Arctic Wolf SOC as a service monitors and tracks information for system/applications, and user accounts. | Intermediary |
| 2. Monitor, audit, and track network traffic and activity | Arctic Wolf SOC as a service monitors, audits and tracks network traffic and activity, alerts on anything suspicious | Intermediary |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | The Id management in AD, 0365 Azure, as well as the IT infrastrucuture services such as DNS/DHCP/DC need more review and robust management upkeep. The Palo Altos should be baselined for best practice so as it aligns with CIS benchmarks. | Fundamental |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | Arctic Wolf SOC as a service vulnerabilty scanner is used, results shared bi weekly with IT administrators. | Intermediary |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | NIST is refrenced but we are using CIS 18 primarly. | Intermediary |
| a. Implement multi-factor authentication | We are in the process of compelting MFA for our end users, FD and Maintenance are left. | Intermediary |
| b. Implement enhanced logging | Syslog is used - this data is sent to our SOC as a service, Arctic Wolf. | Intermediary |
| c. Data encryption for data at rest and in transit | Backups are encrypted in rest and transit | Fundamental |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | We are aware of end of life an unsupported but not yet enacted a plan that involves its own seperation from the production network. | Fundamental |
| e. Prohibit use of known/fixed/default passwords and credentials | This has been completed - the use of password vault for IT implemented. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | Metallic backup testing done monthly, planned for weekly via scripting and validation | Intermediary |
| g. Migration to the .gov internet domain | Request placed - awaiting confirmation. | Fundamental |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | Request placed - awaiting confirmation. | Fundamental |
| 7. Ensure continuity of operations including by conducting exercises | TTX planning has started, IR document compelted. Planned start date October 2023 | Foundational |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | FEDVTE available for IT concerining NICE | Foundational |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | IR plan includes alternate methods of commuinications and data networks. | Foundational |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | City of Sparks | |
| 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 eligible entity | Arcic Wolf monlthly calls and bi-weekly security review calls with IT | Intermediary |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | Foundational | Foundational |
| 12. Leverage cybersecurity services offered by the Department | MS-ISAC/CIS services are used | Intermediary |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | Foundational | Foundational |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | This is completed as items of concern come up, also a full response to multiple threats is in our IR documentation | Intermediary |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | Foundational | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | Foundational | Foundational |




Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**White Pine County**
# White Pine County SLCGP FY2022

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

**$ 39,740.75** Requested

Submitted: 6/22/2023 3:51:22 PM (Pacific)

**Project Contact**
Tabatha Hamilton
edcoffice@whitepinecountynv.gov
Tel: 7752936594

**Additional Contacts**
*none entered*

**White Pine County**

801 Clark St
Ely, NV 89301
United States

| | |
|---|---|
| Telephone | 7752936594 |
| Fax | 17752897711 |
| Web | whitepinecounty.net |
| EIN | 88-6000166 |
| UEI | VJ96KY794XZ5 |
| SAM Expires | 6/26/2018 |

**White Pine County Commission Chairman**
Shane Bybee
sbybee@whitepinecountynv.gov

## Pre-Application *top*

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

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

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

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions *top*

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

- [x] Yes
- [ ] No

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

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

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

- [ ] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

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

- [ ] 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.**

White Pine County is a rural county, home to less than 10,000 people. THis project would provide security for all residents by ensuring the their local government has a secure cyber system and thus can continue routine and safe operation. White Pine County's #1 goal for this project is to hire a consultant for professional services and firewall configurations for cybersecurity software that has been purchased by the County. Another goal of this project includes sending an Information Technology (IT) employee to the DEFCON Cyber security conference in Las Vegas, NV.

**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.*

Once award is received, the award will go before the County Commission for approval. Once approved, the White Pine County IT Office will obtain 2 appropriate quotes/proposals professional services/network configuration . These quotes/proposals will then be provided to the White Pine County Grant specialist/Finance office. The County IT Manager will enter into a contract with the most reasonable and responsive proposals. The Grant Specialist will ensure that the contract(s) is approved by the board of County Commissioners. Once the contract(s) is fully executed and approved, the IT manager will issue a notice to proceed and oversee the professional services being provided. These services will be invoiced regularly. Invoice will be provided to the County Grant specialist's Office who will then enter the invoice for payment. Once the final invoice is paid, a final quarterly report and reimbursement request will be completed and submitted by the County Grant specialists. Meanwhile the IT manager will ensure that conference travel and registration is lined out in accordance to county policy. One IT personnel will attend the next available DEFCON Cyber Security conference. The County Grant Specialists will be responsible for oversight of the project and ensuring the project reporting and other requirements are met throughout the project timeframe.

**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 first desired outcome of this project are to have a fully installed and functional cybersecurity software system throughout the entire county. The second desired outcome is to have one IT employee trained on all relevant cyber security subject matter at a DEFCON conference.

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

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

- [ ] Yes
- [x] No

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

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

N/A- This will be used for 10% cost share.

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**

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

- [ ] Yes
- [x] No

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

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

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

- [ ] Yes
- [x] No

**12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.**
The only possible way to scale this project is to fund only the firewall configuration project or only the cybersecurity conference project. There is no way to scale the costs to send one person to a conference and there is a finite number of firewall configurations necessary to ensure that the County has secure software.

**13. Project Location: Provide the 5-digit zip code where the project will be executed.**
*The project location could be distinct from the sub-recipient address.*
89301

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

- [x] Build
- [ ] Sustain

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

- [ ] Yes
- [x] No

## Line Item Detail Budget *top*

## PLANNING COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | **0** | **0.00** | **$ 0.00** | | | |

## ORGANIZATION COSTS

| Organizational Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| Professional Services | Network Firewall Configuration Services | 1 | $ 38,375.75 | $ 38,375.75 | This project is a one time service to allow for firewall configurations for updated security software that is being purchased by the County | These professional services are necessary to complete the installation of updated cybersecurity for the county. |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | **1** | | **$ 38,375.75** | **$ 38,375.75** | | |

## EQUIPMENT COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | **0** | **$ 0.00** | $ 0.00 | | | |

## TRAINING COSTS

| Training Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. | Do you plan to coordinate this training with the State Training Officer? |
|---|---|---|---|---|---|---|---|
| DEFCON Training/Travel | Registration | 1 | $ 465.00 | $ 465.00 | This project is a one time cost to send 1 employee to be versed in all relative Cyber Security subject matter. | This training will allow for the County to have 1 employee that is versed in all relative Cyber Security subject matter. | N/A |
| DEFCON Training/Travel | Per Diem | 1 | $ 311.00 | $ 311.00 | | | |
| DEFCON Training/Travel | Mileage | 1 | $ 109.00 | $ 109.00 | | | |
| DEFCON Training/Travel | Lodging | 1 | $ 480.00 | $ 480.00 | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | **4** | **$ 1,365.00** | $ 1,365.00 | | | **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) | ☑ | WPC Audit |
| Travel Policy | ☑ | Travel Policy and Procedures |
| Payroll Policy | ☑ | Compensation Policy<br>Travel Voucher based on GSA Rates<br>Quote |
| Procurement Policy | ☑ | Grant Management Policy<br>Fixed Asset Policy<br>Purchase Order Policy<br>Procurement Policy |
| Milestones<br>download template | ☑ | Milestones |
| Capabilities Assessment<br>download template | ☑ | WPC Capabilities |

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

Application ID: 443318

| | | |
|---|---|---|
| | **Applicant Name** | White Pine County |
| | **Project Name:** | |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Award | 7/1/2023 |
| 1 | Quotes | 8/1/2023 |
| 1 | Create PO | 8/15/2023 |
| 1 | Travel Arrangements/ Registration | 7/15/2023 |
| 1 | Create PO | 8/1/2023 |
| 1 | Contract Execution | 8/9/2023 |
| 1 | Attendance of training | 8/14/2023 |
| 1 | Execution of professional services | 12/31/2023 |
| 1 | Final payments | 2/1/2024 |
| 1 | Reimbursement | 3/1/2024 |
| 1 | Final Report | 3/31/2024 |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | White Pine County | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | Process developed and being implemented. | Foundational |
| 2. Monitor, audit, and track network traffic and activity | limited capabilities. New firewalls have been purchased and professional services to be engaged for setup/coniguration. | Foundational |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | BCDR process/planning has been started. | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | Risk assessment process is being developed | Foundational |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | Information Security Policy has been drafted and will be presented to County Comission on 6/28/23 for approval. | Foundational |
| a. Implement multi-factor authentication | only a few sytems in use have multi factor so far | Foundational |
| b. Implement enhanced logging | None | Foundational |
| c. Data encryption for data at rest and in transit | Not currently | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | In progress | Foundational |
| e. Prohibit use of known/fixed/default passwords and credentials | This will be addressed with new Information Security Policy | Foundational |
| f. Ensure the ability to reconstitute systems (backups) | Testing never been preformed by previous managed service provider. New infrastructure is currently being implemented allowing for better backups and backup testing. | Foundational |
| g. Migration to the .gov internet domain | Done | Intermediary |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | Website is a .net not .gov. Working to move that to .gov. | Foundational |
| 7. Ensure continuity of operations including by conducting exercises | BCDR plan will periodic testing | Foundational |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | Per new Information Security Policy, cyber security training will be provided within 30 days of hire and once annually for all county employees. | Foundational |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | Gaps being assessed | Foundational |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | White Pine County | |
| 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 eligible entity | Redundancy and fault tollerance gaps being identified and assesed based on criticality and risk. | Foundational |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | Albert sensor in use for Intrusion Detection | Fundamental |
| 12. Leverage cybersecurity services offered by the Department | working with CISA to leverage provided services | Foundational |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | New IT security policy is a first step | Foundational |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | New IT security policy is a first step | Foundational |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | Security plan to include all rural White Pine County and sub entities. | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | Steps have been taken in White Pine County to streamline purchases and equipment across departments through the IT department to better conform with proposed securty policy. | Foundational |

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Washoe County Emergency Management & Homeland Security Program**

# Washoe County: Incident Response Plan

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

**$ 35,000.00** Requested

Submitted: 6/22/2023 4:16:36 PM (Pacific)

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

**Additional Contacts**
jnadams@washoecounty.gov, jawood@washoecounty.gov,
ehohman@washoecounty.gov,JAwood@washoecounty.gov,tzemach@washoecounty.gov,JAwood@washoecounty.gov,mailto:TZemach@washoecounty.gov,jnadams@washoecounty.gov

**Washoe County Emergency Management & Homeland Security Program**
5195 Spectrum Blvd
Reno, NV 89509

**Program Coordinator**
Francisco Ceballos
Fceballos@washoecounty.gov

Telephone7753994811
Fax
Web www.readywashoe.com
EIN 262800962
UEI
SAM
Expires 11/10/2021

## Pre-Application top

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

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

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

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

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

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

## Application Questions top

**1. Is this agency within a rural area?**
*A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)*
- [x] Yes
- [ ] No

**2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)**
- [x] Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- [ ] Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- [ ] Objective 3: Implement security protections commensurate with risk.
- [ ] Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

**3. Please select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)**
*Projects may align with more than one element.*
- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [x] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
- [ ] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [x] Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [x] 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.**
As a governmental organization, Washoe County must adhere to and comply with the Nevada Revised Statutes (NRS) Chapter 603A.210. This policy states that governmental organizations must "comply with the current version of the Center for

Internet Security (CIS) Controls as published by the Center for Internet Security, Inc." One of the controls, specifically control 17, highlights establishing and maintaining an incident response plan to prepare, detect, and respond to an attack. Therefore, to adequately protect digital data for all employees and constituents (including rural staff), the county must implement cybersecurity safeguards, such as an incident response plan, to mitigate security incidents. By developing and executing a robust cybersecurity plan, which includes a well-defined incident response strategy, the county can swiftly recognize and address security breaches to minimize impact, reduce downtimes, and limit potential damage to the county's assets and sensitive information. The county, therefore, will generate a well-defined framework for every phase of the process, including notifying personnel and documentation for making changes to security controls. Approximately 36% of the total funding request will be dedicated to rural communities in 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.*
To ensure Washoe County's cybersecurity safeguards are comprehensive and effective, a vendor will be selected to create and execute a detailed plan that complies with legal statutes and regulations. Therefore, the county will be informed of the best practices to maximize its effectiveness in their environment while adhering to CIS compliance standards.

**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.*
Developing a cybersecurity incident response plan will allow the county to establish a documented cybersecurity governance structure that adheres to Nevada law and will set the vision for the county's cyber risk management.

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

**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.*
89502

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

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

## Line Item Detail Budget top

### PLANNING COSTS

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

### ORGANIZATION COSTS

| Organizational Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| Incident Response Plan Development Services | Professional services to complete the County incident response plan including runbook scenarios for handing different types of attacks. | 1 | $ 35,000.00 | $ 35,000.00 | This a one-time request to complete our Incident Response (IR) Plan. Additional funding would not be required or requested. | As required by NRS 603A and the CIS controls, this would allow the County to complete our IR Plan Documentation. |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | **1** | **$ 35,000.00** | $ 35,000.00 | | |

## 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 |
|---|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | 0 | $ 0.00 | $ 0.00 | | | | |

## TRAINING COSTS

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

## EXERCISE COSTS

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

**Document Uploads** *top*

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

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

Application ID: 443738

| | | |
|---|---|---|
| | **Applicant Name** | Kelly Echeverria |
| | **Project Name:** | Washoe County: Incident Response Plan |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Select a vendor to create a detailed Incident Response Plan | 3 months after funds received |
| 2 | Washoe County will begin to execute and implement the plan | 3-4 months after funds received |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Washoe County | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | Systems are monitored using Palo Alto's Cortex XDR, installed on every endpoint. Policies specific to sites, and specific to permitted/unpermitted software, are in development. | Intermediary |
| 2. Monitor, audit, and track network traffic and activity | We are upgrading to Palo Alto NGFWs, all sites have or will soon have a local firewall, and the county as a whole is protected by edge firewalls, all traffic is monitored and logged for review. | Advanced |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | A disaster recovery plan is in development, including redundant networks and data centers, and backup/recovery systems. | Fundamental |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | The county will select a vendor to create and execute a detailed incident response plan that complies with legal statutes and regulations. Therefore, the county will be informed of the best practices to maximize its effectiveness in their environment while adhering to CIS compliance standards. | Fundamental |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | The county is beginning to implement and document CIS controls and safeguards. | Fundamental |
| a. Implement multi-factor authentication | MFA is implemented using Duo and Microsoft Authenticator. | Advanced |
| b. Implement enhanced logging | The county currently uses Proficio for enhanced logging. | Advanced |
| c. Data encryption for data at rest and in transit | The county is working on implementing BitLocker on all endpoints. | Fundamental |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | The county is replacing unsupported equipment according to their end of life date. | Intermediary |
| e. Prohibit use of known/fixed/default passwords and credentials | Washoe County implements a password policy that is CJIS and CIS compliant. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | BCDR is being developed and rolled into an overall disaster recovery plan. | Foundational |
| g. Migration to the .gov internet domain | Currently in progress. | Intermediary |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | Currently in progress. | Intermediary |
| 7. Ensure continuity of operations including by conducting exercises | A disaster recovery plan is in development, including redundant networks and data centers, and backup/recovery systems. | Fundamental |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | All county employees are mandated to undergo cybersecurity training along with quarterly phishing campaigns. | Intermediary |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | The county is considering upgrading all backup connections. | Fundamental |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Washoe County | |
| 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 eligible entity | The county will conduct annual penetration tests from a suitable vendor to pinpoint deficiencies within its environment and discover areas for improvement. | Fundamental |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | The county is participating in the rollout of a state-wide security operations center to share threat intel and collaborates with OCDC. | Foundational |
| 12. Leverage cybersecurity services offered by the Department | The Cybersecurity and Infrastructure Security Agency (CISA) completes a penetration test on Washoe County's infrastructure every two years. | Intermediary |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | The county will conduct annual penetration tests from a suitable vendor to pinpoint deficiencies within its environment and discover areas for improvement. | Fundamental |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | The county will select a vendor to create and execute a detailed incident response plan that complies with legal statutes and regulations. Therefore, the county will be informed of the best practices to maximize its effectiveness in their environment while adhering to CIS compliance standards. | Foundational |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | Rural communities receive the same infrastructure upgrade as the county's more urban sites. | Advanced |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | Washoe County shares regional information with nearby government entities such as the City of Reno and the City of Sparks. | Intermediary |

Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Washoe County Emergency Management & Homeland Security Program**

# Washoe County: Annual Penetration Testing

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

**$ 44,000.00** Requested

Submitted: 6/22/2023 4:20:55 PM (Pacific)

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

**Additional Contacts**
jnadams@washoecounty.gov, jawood@washoecounty.gov, ehohman@washoecounty.gov,JAwood@washoecounty.gov,tzemach@washoecounty.gov

**Washoe County Emergency Management & Homeland Security Program**

5195 Spectrum Blvd
Reno, NV 89509

**Program Coordinator**
Francisco Ceballos
Fceballos@washoecounty.gov

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

## Pre-Application *top*

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

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

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

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

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

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

## Application Questions *top*

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

- [x] Yes
- [ ] No

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

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

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

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [x] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
- [ ] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [x] Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [x] 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.**
As a governmental organization, Washoe County must adhere and comply with Nevada Revised Statutes (NRS) Chapter 603A.210. In this policy, it is stated that governmental organizations must "comply with the current version of the Center for Internet Security (CIS) Controls as published by the Center for Internet Security, Inc." CIS Control 18 specifies establishing and performing annual penetration tests, as it is an imperative practice for an organization to ensure the resilience of various networks and systems, identify vulnerabilities and weaknesses, mitigate risks effectively, and to provide trust to employees and vendors. By conducting annual penetration testing, the county can simulate the actions of an attacker and learn to respond to various attack scenarios. Additionally, implementing this change would be advantageous for the county's rural communities, as conducting a penetration test would enhance the security of all network devices county-wide. Approximately 36% of the total funding request will be dedicated to rural communities in 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.*
Currently, the Cybersecurity and Infrastructure Security Agency (CISA) completes a penetration test on Washoe County's infrastructure every two years. However, CISA is experiencing processing delays and cannot conduct supplementary evaluations. Therefore, Washoe County will source a selected vendor to complete a penetration test for the years CISA does not perform the test.

**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.*

By conducting annual penetration testing, the county can comply with the CIS Controls and Chapter 603A of the NRS statute. Thus, the county will improve its cyber hygiene, pinpointing deficiencies within our environment and discovering areas for improvement.

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

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

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**
*Please see the EHP Guidance attachment for more information on EHP reviews.*
- [ ] Yes
- [x] No

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

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

**12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.**
Washoe County Technology Services will hire a vendor to conduct the penetration tests. If less funding is available, we would reduce the amount available to hire a vendor.

**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.*
89502

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

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

## Line Item Detail Budget top

### PLANNING COSTS

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | | | $ | | | |
| | | 0 | 0.00 | $ 0.00 | | | |

## ORGANIZATION COSTS

| Organizational Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| Annual PEN Testing | Annual penetration testing using third-party provider. | 1 | $ 44,000.00 | $ 44,000.00 | Technology Services would request additional annual budgetary authority from Washoe County, which has been previously denied, to continue this program. | This is the funding for our request to complete our annual pen testing as required by CIS controls. |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | 1 | $ 44,000.00 | $ 44,000.00 | | |

## 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 |
|---|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | 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 | Describe how the purchase(s) within this element tie into the project as described in the | Do you plan to coordinate this training with the State |
|---|---|---|---|---|---|---|---|

| | | | | discontinued? | Application Questions section. | Training Officer? |
|---|---|---|---|---|---|---|
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | | $ $ | | | |
| | | 0 | $ 0.00 | $ 0.00 | | 0 |

## EXERCISE COSTS

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

### Document Uploads *top*

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

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

Application ID: 443335

| | | |
|---|---|---|
| | **Applicant Name** | Kelly Echeverria |
| | **Project Name:** | Washoe County: Annual Pen Testing |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Washoe County hires a vendor to conduct the penetration test | 6 months after funds received |
| 2 | Washoe County will use the results from the test to evaluate their environment and discover areas for improvement | 6-7 months after funds received |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Washoe County | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | Systems are monitored using Palo Alto's Cortex XDR, installed on every endpoint. Policies specific to sites, and specific to permitted/unpermitted software, are in development. | Intermediary |
| 2. Monitor, audit, and track network traffic and activity | We are upgrading to Palo Alto NGFWs, all sites have or will soon have a local firewall, and the county as a whole is protected by edge firewalls, all traffic is monitored and logged for review. | Advanced |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | A disaster recovery plan is in development, including redundant networks and data centers, and backup/recovery systems. | Fundamental |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | The county will select a vendor to create and execute a detailed incident response plan that complies with legal statutes and regulations. Therefore, the county will be informed of the best practices to maximize its effectiveness in their environment while adhering to CIS compliance standards. | Fundamental |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | The county is beginning to implement and document CIS controls and safeguards. | Fundamental |
| a. Implement multi-factor authentication | MFA is implemented using Duo and Microsoft Authenticator. | Advanced |
| b. Implement enhanced logging | The county currently uses Proficio for enhanced logging. | Advanced |
| c. Data encryption for data at rest and in transit | The county is working on implementing BitLocker on all endpoints. | Fundamental |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | The county is replacing unsupported equipment according to their end of life date. | Intermediary |
| e. Prohibit use of known/fixed/default passwords and credentials | Washoe County implements a password policy that is CJIS and CIS compliant. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | BCDR is being developed and rolled into an overall disaster recovery plan. | Foundational |
| g. Migration to the .gov internet domain | Currently in progress. | Intermediary |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | Currently in progress. | Intermediary |
| 7. Ensure continuity of operations including by conducting exercises | A disaster recovery plan is in development, including redundant networks and data centers, and backup/recovery systems. | Fundamental |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | All county employees are mandated to undergo cybersecurity training along with quarterly phishing campaigns. | Intermediary |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | The county is considering upgrading all backup connections. | Fundamental |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Washoe County | |
| 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 eligible entity | The county will conduct annual penetration tests from a suitable vendor to pinpoint deficiencies within its environment and discover areas for improvement. | Fundamental |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | The county is participating in the rollout of a state-wide security operations center to share threat intel and collaborates with OCDC. | Foundational |
| 12. Leverage cybersecurity services offered by the Department | The Cybersecurity and Infrastructure Security Agency (CISA) completes a penetration test on Washoe County's infrastructure every two years. | Intermediary |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | The county will conduct annual penetration tests from a suitable vendor to pinpoint deficiencies within its environment and discover areas for improvement. | Fundamental |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | The county will select a vendor to create and execute a detailed incident response plan that complies with legal statutes and regulations. Therefore, the county will be informed of the best practices to maximize its effectiveness in their environment while adhering to CIS compliance standards. | Foundational |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | Rural communities receive the same infrastructure upgrade as the county's more urban sites. | Advanced |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | Washoe County shares regional information with nearby government entities such as the City of Reno and the City of Sparks. | Intermediary |

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Washoe County Emergency Management & Homeland Security Program**

# Washoe County: Cortex XDR Host Insights

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

**$ 27,931.00** Requested

Submitted: 6/22/2023 4:22:10 PM (Pacific)

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

**Additional Contacts**
jnadams@washoecounty.gov, jawood@washoecounty.gov,
ehohman@washoecounty.gov,JAwood@washoecounty.gov,tzemach@washoecounty.gov,JAwood@washoecounty.gov,mailto:TZemach@washoecounty.gov,jnadams@washoecounty.gov

**Washoe County Emergency Management & Homeland Security Program**
5195 Spectrum Blvd
Reno, NV 89509

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

**Program Coordinator**
Francisco Ceballos
Fceballos@washoecounty.gov

## Pre-Application *top*

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

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

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

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

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

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

## Application Questions *top*

**1. Is this agency within a rural area?**
*A rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce (SLCGP: F.2.b)*
- [x] Yes
- [ ] No

**2. There are four (4) main objectives for FY 2022 SLCGP. Please select the objective with which your project most closely aligns. (SLCGP: A.10.b and Appendix A)**
- [ ] Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- [ ] Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- [x] Objective 3: Implement security protections commensurate with risk.
- [ ] Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

**3. Please select which of the SLCGP program elements your project addresses. (SLCGP: Appendix A)**
*Projects may align with more than one element.*
- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [x] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [ ] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [x] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
- [ ] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [x] Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [x] 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.**
As a governmental organization, Washoe County must adhere to and comply with Nevada Revised Statutes (NRS) Chapter 603A.210. In this policy, it is stated that governmental organizations must "comply with the current version of the Center for

Internet Security (CIS) Controls as published by the Center for Internet Security, Inc." Specifically, in the CIS Controls, numerous safeguards relate to security measures such as software inventory, access control, and the use of continuous vulnerability management tools (CIS Controls 2, 6, and 7, respectively.
Currently, Washoe County uses Cortex XDR to conduct threat investigation and prevention across endpoints and networks. However, with the host insights add-on module, the team will have extended endpoint visibility, with the ability to find and remove malicious files promptly, provide visibility to quickly identify threats, and improve vulnerability management with Common Vulnerabilities and Exposure (CVE) metrics. This change will affect all county endpoints and networks, including rural communities. Approximately 36% of the total funding request will be dedicated to rural communities in 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.*
Host Insights leverages the Cortex XDR agent to conduct endpoint scans, gathering valuable details including services, drivers, shares, and disks. Therefore, the Washoe County cybersecurity team will install this additional module to enhance the capabilities of Cortex XDR.

**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.*
Adding the host insight module to Cortex XDR will improve the county's security posture by providing enhanced endpoint visibility and reporting while being CIS-compliant. Therefore, the county can strengthen its monitoring, analysis, and response to malicious threats.

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

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

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**
*Please see the EHP Guidance attachment for more information on EHP reviews.*
- [ ] Yes
- [x] No

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

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

**12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.**
This project is not scalable because the add-on to Cortex XDR can either be added or removed to the county's XDR platform.

**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.*
89502

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

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

**Line Item Detail Budget** *top*

## PLANNING COSTS

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

## ORGANIZATION COSTS

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

## EQUIPMENT COSTS

| Equipment Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. | AEL Name | AEL Number |
|---|---|---|---|---|---|---|---|---|
| Palo Alto Cortex Host Insight | Host Insight addon for Cortex XDR EDR solution. | 5,300 | $ 5.27 | $ 27,931.00 | Technology Services would submit a request to the County for additional budget authority to carry out this project. If denied, Washoe County would not renew the licensing for this module. | This add-on provides additional insight into cybersecurity related activities and issues on the County endpoints. | Software, Malware/Anti-Vi | 05HS-00-MALW |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | 5,300 | $ 5.27 | $ 27,931.00 | | | | |

## TRAINING COSTS

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

## EXERCISE COSTS

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

**Document Uploads** *top*

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

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

Application ID: 443741

| | | |
|---|---|---|
| | **Applicant Name** | Kelly Echeverria |
| | **Project Name:** | Washoe County: Cortex XDR Host Insights |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Washoe County will add the host insights module to their Cortex XDR agent | A week after funds received |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Washoe County | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | Systems are monitored using Palo Alto's Cortex XDR, installed on every endpoint. Policies specific to sites, and specific to permitted/unpermitted software, are in development. | Intermediary |
| 2. Monitor, audit, and track network traffic and activity | We are upgrading to Palo Alto NGFWs, all sites have or will soon have a local firewall, and the county as a whole is protected by edge firewalls, all traffic is monitored and logged for review. | Advanced |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | A disaster recovery plan is in development, including redundant networks and data centers, and backup/recovery systems. | Fundamental |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | The county will select a vendor to create and execute a detailed incident response plan that complies with legal statutes and regulations. Therefore, the county will be informed of the best practices to maximize its effectiveness in their environment while adhering to CIS compliance standards. | Fundamental |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | The county is beginning to implement and document CIS controls and safeguards. | Fundamental |
| a. Implement multi-factor authentication | MFA is implemented using Duo and Microsoft Authenticator. | Advanced |
| b. Implement enhanced logging | The county currently uses Proficio for enhanced logging. | Advanced |
| c. Data encryption for data at rest and in transit | The county is working on implementing BitLocker on all endpoints. | Fundamental |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | The county is replacing unsupported equipment according to their end of life date. | Intermediary |
| e. Prohibit use of known/fixed/default passwords and credentials | Washoe County implements a password policy that is CJIS and CIS compliant. | Intermediary |
| f. Ensure the ability to reconstitute systems (backups) | BCDR is being developed and rolled into an overall disaster recovery plan. | Foundational |
| g. Migration to the .gov internet domain | Currently in progress. | Intermediary |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | Currently in progress. | Intermediary |
| 7. Ensure continuity of operations including by conducting exercises | A disaster recovery plan is in development, including redundant networks and data centers, and backup/recovery systems. | Fundamental |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | All county employees are mandated to undergo cybersecurity training along with quarterly phishing campaigns. | Intermediary |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | The county is considering upgrading all backup connections. | Fundamental |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Washoe County | |
| 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 eligible entity | The county will conduct annual penetration tests from a suitable vendor to pinpoint deficiencies within its environment and discover areas for improvement. | Fundamental |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | The county is participating in the rollout of a state-wide security operations center to share threat intel and collaborates with OCDC. | Foundational |
| 12. Leverage cybersecurity services offered by the Department | The Cybersecurity and Infrastructure Security Agency (CISA) completes a penetration test on Washoe County's infrastructure every two years. | Intermediary |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | The county will conduct annual penetration tests from a suitable vendor to pinpoint deficiencies within its environment and discover areas for improvement. | Fundamental |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | The county will select a vendor to create and execute a detailed incident response plan that complies with legal statutes and regulations. Therefore, the county will be informed of the best practices to maximize its effectiveness in their environment while adhering to CIS compliance standards. | Foundational |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | Rural communities receive the same infrastructure upgrade as the county's more urban sites. | Advanced |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | Washoe County shares regional information with nearby government entities such as the City of Reno and the City of Sparks. | Intermediary |

Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

**Pershing County, Nevada**

# Pershing County Multifactor Authentication

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

**$ 28,580.00** Requested

Submitted: 6/22/2023 9:37:06 PM (Pacific)

**Project Contact**
Justin Abbott
jabbott@pershingcountynv.gov
Tel: 7754420102 ext. 2401

**Additional Contacts**
rchilds@pershingcountynv.gov,lrackley@pershingcountynv.gov

**Pershing County, Nevada**

PO Box 736
340 Main Street
Lovelock, NV 89419
United States

**Clerk-Treasurer**
Lacey Donaldson
ldonaldson@pershingcountynv.gov

Telephone 7754420102
Fax
Web www.pershingcountynv.gov
EIN 88-6000131
UEI NKFYECJG42K5
SAM
Expires

## Pre-Application *top*

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

- [x] Yes
- [ ] No

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

- [x] Yes
- [ ] No

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

- [x] I understand and agree.

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

*in the "Resource Document" tab.*

- [x] I understand and agree.

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

- [x] I understand and agree.

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

*See SLCGP: C.4 for more information.*

- [x] I understand and agree.

## Application Questions top

**1. Is this agency within a rural area?**

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

- [x] Yes
- [ ] No

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

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

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

*Projects may align with more than one element.*

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [x] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [ ] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
- [ ] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [x] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [ ] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [ ] Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting

neighboring entities, including adjacent states and countries.

- [ ] Ensure adequate access to, and participation in, the services and programs described in SLCGP: Appendix C by rural areas within the state.
- [ ] Distribute funds, items, services, capabilities, or activities to local governments.

**4. Describe your project, in detail, including how it achieves the objective identified in Question 2 and any elements identified in Question 3.**
Pershing County intends to evaluate and implement multi-factor authentication (MFA) and modernize user account access controls for Windows user accounts to enhance security of user accounts and the information they can access.

By leveraging cloud-based solutions such as cloud-based IAM, Pershing County can reduce the number of passwords users are forced to track by implementing Single Sign-On for Windows accounts, consolidating four Active Directory domains into a single, centrally managed forest, reducing the complexity and number of implemented identity access controls, simplifying monitoring and logging of account usage, and enhances the security posture of Pershing County technology systems while allowing the County to remain flexible in meeting the needs of both law enforcement and and civil service users.

By leveraging MFA, Pershing County can increase confidence that only authorized users are able to access restricted County data, helping to mitigate risk associated with passwords and credential theft. MFA is considered an industry best practice and, in the case of Pershing County, provide the greatest increase in cybersecurity for the value.

**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 project will be implemented by Pershing County's Information Technology Department (PCIT), with a staff of one manager and one technician, supplemented by J4 Systems, a contractor that PCIT has worked with in the past on network projects such as replacing end-of-life network infrastructure devices and re-organization of local area networks.

Phase 1 will involve planning the deployment of cloud-based IAM solutions, and the procurement of the necessary licenses from vendors. PCIT will work with consultants J4 Systems to accomplish this step.

Phase 2 will be the preparation of the current IAM systems by establishing a forest trust between top-level domains into an AD forest and connection tools from the SaaS solution. PCIT will work with consultants J4 Systems to accomplish this step.

Phase 3 will be the setup and deployment of Multi-factor Authentication to all user accounts. PCIT will work with consultant J4 Systems to accomplish this step.

Phase 4 will include post-implementation support for users and systems to ensure that Pershing County systems continue to works as expected. PCIT will work with J4 Systems to accomplish this step. As-Built Documentation of the new setup will also be developed during this phase with J4 Systems handling the primary work of creating the documentation.

**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 cloud-based Identity Access Management SaaS solutions to enable centralized monitoring and maintenance of user accounts. Leverage Identity Access Management SaaS solutions to secure accounts by implementing Multi-Factor Authentication across all County users and Internet-facing systems.

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

- [ ] Yes
- [x] No

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

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**
*Please see the EHP Guidance attachment for more information on EHP reviews.*

- [ ] Yes
- [x] No

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

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

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

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

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

- [ ] Yes
- [x] No

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

The project is already reduced to a minimum viable level that features implementation of one level of cybersecurity. The decentralized nature of the Pershing County technology environment requires work to implement solutions that can be leveraged across all facilities and involve remote users such as law enforcement vehicle terminals and sub-stations.

**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.*

89419

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

- [x] Build
- [ ] Sustain

**15. Is this request deployable to other jurisdictions?**

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

- [ ] Yes
- [x] No

## Line Item Detail Budget top

### PLANNING COSTS

| Planning Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| Consultant Hours - Phase 1 | Review of environment, develop plan | 8 | 160.00 | $ 1,280.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | In order to effectively implement a new security control, a detailed accounting of the current environment and an actionable change plan is required. |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | 8 | 160.00 | $ 1,280.00 | | |

## 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. |
|---|---|---|---|---|---|---|
| Consultant Hours - Phase 2 | Forest Merge and Local-To-SaaS Sync setup | 24 | $ 160.00 | $ 3,840.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | In order to associate on-prem user accounts with a centralized IAM solution, our existing AD domains must be joined in a forest and on-prem-to-cloud account synchronization tools installed, providing a foundation for the security controls to build on. |
| Consultant Hours - Phase 2 | Deploy MFA | 8 | $ 190.00 | $ 1,520.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | Implementing MFA help to increase security on user accounts and reduce risk of credential compromise. |
| Consultant Hours - Phase 3 | Merge Domains | 24 | $ 160.00 | $ 3,840.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | Merge domains mitigates the risk associated with forest trusts by consolidating all Pershing County domains under a single domain, reducing the attack service and eliminating unnecessary AD Domains. |
| Consultant Hours - Phase 4 | Create As Built Documentation | 6 | $ 160.00 | $ 960.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | Documentation of technology environment is critical to later enhancement and evaluation of any new potential risks, which enables PCIT to continue to mitigate those risks. |
| | | | | $ | $ | |
| | | | | $ | $ | |
| | | | | $ | $ | |
| | | | | $ | $ | |
| | | | | $ | $ | |
| | | | | $ | $ | |
| | | | | $ | $ | |
| | | | | $ | $ | |
| | | | | $ | $ | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | $ | $ | | | |
| | | | 62 | $ 670.00 | $ 10,160.00 | | | |

## 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 |
|---|---|---|---|---|---|---|---|---|
| Fingerprint Readers | Desktop USB Fingerprint reader for Windows Hello, FIDO, U2F, and FIDO2 | 80 | $ 74.25 | $ 5,940.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | Fingerprint readers provide biometric authentication as a second authentication factor and are the primary second authentication factor provided to user workstations. | Device, Biometric User Au | 05AU-00-BIOM |
| Physical Security Tokens | Tray of 50 Physical Security Tokens | 1 | $ 4,000.00 | $ 4,000.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | Security key tokens are physical devices that contain a private key that is registered to user's account. They must be physically attached to a workstations or server that requires a log-in and a typically require some sort of physical interaction when prompted by the authenticating system to verify the user's physical presence. These are primarily for users that require remote authentication or server authentication when a fingerprint reader is not feasible. | System, Remote Authentica | 05AU-00-TOKN |
| User Licenses for Cloud Identity Management SaaS | Annual user licenses | 100 | $ 72.00 | $ 7,200.00 | Pershing County would seek grant funding through other sources such as NV POOL/PACT Risk Management grants other State of Nevada or US Government grant programs. If no other grant program is required, by eliminating less important IT projects starting with non-cybersecurity initiatives. | As the foundational piece of technology, the IAM platform gives us the ability to add multi-factor authentication and implement single sign-on using a variety of methods such as authenticator apps for smartphones, FIDO2 physical security tokens, and one-time passwords delivered through a variety of means. | Applications, Software as | 04AP-11-SAAS |
| | | | | $ | $ | | | |
| | | | | $ | $ | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | 181 | $ 4,146.25 | $ 17,140.00 | | | | |

## TRAINING COSTS

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

## EXERCISE COSTS

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

| | | | | | |
|---|---|---|---|---|---|
| | | $ | $ | | |
| | 0 | $ 0.00 | $ 0.00 | | 0 |
| **Total** | **0** | **$ 0.00** | **$0.00** | | **0** |

## Document Uploads *top*

| Documents Requested * | Required? | Attached Documents * |
|---|---|---|
| A-133 Audit (Most Current) | ☑ | A-113 Audit |
| Travel Policy | ☑ | Pershing County Travel Policy |
| Payroll Policy | ☑ | Payroll Policy |
| Procurement Policy | ☑ | Pershing Procurement Policy |
| Milestones<br>download template | ☑ | Updated Project Milestones - 06-26-23 |
| Capabilities Assessment<br>download template | ☑ | Capabilities Assessment |

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

Application ID: 444224

| | | |
|---|---|---|
| | **Applicant Name** | Pershing County, Nevada |
| | **Project Name:** | Pershing County Multifactor Authentication |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Phase 1 - Planning and Procurement | 30-Sep |
| 2 | Phase 2 - Prepare On-Prem Systems | 31-Oct |
| 3 | Phase 3 - Deploy Cloud IAM Solution | 30-Nov |
| 4 | Phase 4 - Post-Deployment | 29-Dec |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Pershing County | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | Multiple on-prem active directory domains, CIS Albert IDS, DarkTrace IPS, Office 365 enabled Azure AD | Fundamental |
| 2. Monitor, audit, and track network traffic and activity | CIS Albert IDS, DarkTrace IPS | Fundamental |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | Multiple on-prem backup solutions spread throughout county facilities including: Magnetic tape, removable drive, Unitrends backup appliance (no unified backup platform, no geographic distribution) | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | NV POOL/PACT Passive Network Assessment Program, CIS Albert IDS, DarkTrace IPS, NV SoS CyberHygiene program | Fundamental |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | | |
| a. Implement multi-factor authentication | Office 365-enabled Azure AD, elections system requires Digital Persona MFA | Foundational |
| b. Implement enhanced logging | DarkTrace IPS, Juniper SRX-300 firewall basic logging | Foundational |
| c. Data encryption for data at rest and in transit | IPSec and SSLVPN tunnels established between facilitlies, no encryption at rest | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | Final legacy system, IBM Power 7 server with legacy software in the process of sundowning. Critical systems with no simple replacement all that is left. | Intermediary |
| e. Prohibit use of known/fixed/default passwords and credentials | Strong passwords required | Fundamental |
| f. Ensure the ability to reconstitute systems (backups) | Processes ensure backups are running, no restore tests performed | Foundational |
| g. Migration to the .gov internet domain | Most public-facing systems migrated to pershingcountynv.gov | Intermediary |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | Most public-facing systems migrated to pershingcountynv.gov | Intermediary |
| 7. Ensure continuity of operations including by conducting exercises | No exercise plan in place for cybersecurity incidents, working with cyberinsurance provider POOL/PACT to develop plans. | Foundational |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | Economic devleopment engages with JOIN and NevadaWORKS to devleop general workforce training programs. Pershing County is getting ready to engage in a salary study to inform a larger push to develop policies to attract and retain employees. When possible, third-party consultants provided by the Pershing County cyberinsurance provider POOL/PACT are utilitzed. | Foundational |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | Pershing County is developing a continuity and response plan with the assistance of our cyberinsurance provider POOL/PACT | Foundational |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | Pershing County | |
| 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 eligible entity | Pershing County uses programs available throught the NV Secretary of State and cyberinsurance provider POOL/PACT to evaluate and mitigate risks and threats to County systems. | Fundamental |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | Through NV POOL/PACT and NV Secretary of State, Pershing County is a member of MS-ISAC/EI-ISAC | Fundamental |
| 12. Leverage cybersecurity services offered by the Department | The application for the SLCGP is the first step Pershing County is taking in utilizing Department of Emergency Management resources | Foundational |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | Pershing County uses programs available throught the NV Secretary of State and cyberinsurance provider POOL/PACT to evaluate and mitigate risks and threats to County systems. | Foundational |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | Pershing County uses programs available throught the NV Secretary of State and cyberinsurance provider POOL/PACT to evaluate and mitigate risks and threats to County systems. | Foundational |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | The application for the SLCGP is the first step Pershing County is taking in utilizing Department of Emergency Management resources | Foundational |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | The application for the SLCGP is the first step Pershing County is taking in utilizing Department of Emergency Management resources | Foundational |




Nevada Office of the Military, Division of Emergency Management

**FFY 2022 State and Local Cybersecurity Grant Program (SLCGP)**
Deadline: 6/28/2023

### State of Nevada - Office of Cyber Defense Coordination
# NV Shared Cyber Threat Intelligence Platform

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

**$ 150,000.00** Requested

Submitted: 6/23/2023 8:38:26 AM (Pacific)

**Project Contact**
Dianne Haigney
dhaigney@ocdc.nv.gov
Tel: 7754316360

**Additional Contacts**
*none entered*

**State of Nevada - Office of Cyber Defense Coordination**

555 Wright Way
Carson City, NV 89711
United States

**Administrator**
Aakin Patel
aakin.patel@ocdc.nv.gov

| | |
|---|---|
| Telephone | 7754316360 |
| Fax | |
| Web | |
| EIN | 866000022 |
| UEI | |
| SAM Expires | |

## Pre-Application top

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

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

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

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

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

- [x] I understand and agree.

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

- [x] I understand and agree.

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

- [x] I understand and agree.

## Application Questions *top*

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

- [ ] Yes
- [x] No

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

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

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

- [x] Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
- [x] Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
- [ ] Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
- [x] Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed in SLCGP: Appendix C.5.
- [ ] Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
- [x] Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
- [ ] Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state,

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

- [x] Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
- [ ] Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
- [x] Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
- [ ] Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
- [ ] Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [x] 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.**

Create a shared technical threat analysis and alert management tool for use by any entities within the state of Nevada, including any rural entities. This project will also serve as the functional base for the implementation of a shared statewide SEIM (Security Event and Incident Management) and SOC (Security Operations Center) once fully deployed.

This supports the Question 2 Objective of “Implement Security Protections Commensurate with Risk” as it allows entities making use of this tool to become aware of risk and work on implementing security protections to counter that.

This project directly allows an entity to manage, monitor and track cybersecurity related activities on information technology systems, including legacy systems, deployed within entities that will participate. It can also be used to monitor network traffic and activity and allow for enhanced response and resilience through actively blocking traffic and activities that are detected and determined as being dangerous. Additionally, part of the aim of the project is to allow entities and agencies to easily share this information with each other, in order to enhance the state’s capabilities to react across the board to threats detected within one entity, and have a good, centralized resource for cyberthreat activity indicators.

We are focusing our efforts entirely on what would most benefit rural areas with a minimum 80% or $120,000 of $150,000 awarded to be invested solely in rural areas, however, our work is open to non-rural entities as well should they choose to use it. We anticipate rural funding allocation to exceed 80%. The needs of the rural areas will drive our products direction.

**5. 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 project will be implemented by OCDC staff, in conjunction with contractor resources where needed. The OCDC currently has an Open Source Engineer on staff, who will be doing the bulk of the implementation and configuration for these tools. We will reach out to expertise with a contractor when they are unable to do the work internally.

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

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

The desired outcome is a supported and functional SEIM and SOC tool that can be deployed to various entities as desired, and which can be used to communicate threat intelligence between agencies for shared threat intelligence and activity monitoring.

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

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

- [ ] Yes
- [x] No

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

*If you are not retaining M&A, please enter "N/A"*
0

**9. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?**
*Please see the EHP Guidance attachment for more information on EHP reviews.*

- [ ] Yes
- [x] No

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

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

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

- [x] Yes
- [ ] No

**12. Describe the ways in which the project can be scaled or reduced or the reasons why it cannot.**
We can scale in multiple ways:

Make additional use of contractors to speed development of the necessary tools.

Subsidize or completely cover hardware/software licensing costs for rural/partner entities.

Increase initial deployment scopes.

**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.*
89711

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

- [x] Build
- [ ] Sustain

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

- [x] Yes
- [ ] No

**Line Item Detail Budget** *top*

## PLANNING COSTS

| Planning Cost Name | Line Item Description | Quantity | Unit Cost | Total | How would your organization sustain this project if grant funding was reduced or discontinued? | Describe how the purchase(s) within this element tie into the project as described in the Application Questions section. |
|---|---|---|---|---|---|---|
| | | | 0.00 | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | | | $ | | |
| | | **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. |
|---|---|---|---|---|---|---|
| Direct support for partner entities | Working with rural and other entities to ensure smoother deployment of support projects. | 1 | $ 15,000.00 | $ 15,000.00 | Work at finding alternate funding within our budget or via other grants. | This would be used to directly support deployment of the project with partner entities, and to provide hands on support for their technical needs to get the project online. This would include travel to relevant rural entities for direct support. |
| Contractor/Consulting services | ElasticSearch support and consulting | 1 | $ 47,400.00 | $ 47,400.00 | We would either seek alternate sources of funding, or wait till next legislative appropriation cycle for this, and meanwhile work as best we can without direct training, but with contractor/consultant help. | This will provide the specialty expertise that is directly needed to get most of our objectives implemented and guide our in-house staff through the process so they can |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | sustain the project in the future. |
| Whole Community Outreach | Whole Community Outreach | 1 | $ 7,500.00 | $ 7,500.00 | Work at finding alternate funding within our budget or via other grants. | This will allow us to start outreach programs to make other entities aware of our support and service, and provide easy-to-use data / threat sharing mechanisms. |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | | $ | $ | | |
| | | **3** | **$ 69,900.00** | **$ 69,900.00** | | |

## 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 |
|---|---|---|---|---|---|---|---|---|
| Hardware servers | Servers to run log analysis and collection tools | 2 | $ 18,000.00 | $ 36,000.00 | Look for legislative appropriations in next legislative cycle | These servers would be used to run software and services to support all elements of the SLCGP specified in the Application Questions section. | Hardware, Computer, Integ | 04HW-01-INHW |
| Software licensing | ElasticSearch licenses | 3 | $ 6,000.00 | $ 18,000.00 | Use the opensource, unsupported version to start off and then get legislative appropriations in the next cycle. | This software is key to our log collection and threat analysis portions of the project. | System, Security Informat | 05NP-00-SIEM |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |
| | | | $ | $ | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | | | $ | $ | | |
| | | **5** | | **$ 24,000.00** | **$ 54,000.00** | | |

## 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? |
|---|---|---|---|---|---|---|---|
| Training for SOC/SEIM Analysts | SANS Training Vouchers | 3 | $ 8,700.00 | $ 26,100.00 | We would either seek alternate sources of funding, or else wait till next legislative appropriation cycle for this, and meanwhile work as best we can without direct training, but with contractor/consultant help. | This training would allow us to better create useful threat sharing intelligence to distribute amongst all our partner entities. | No |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | | $ | $ | | | |
| | | **3** | **$ 8,700.00** | **$ 26,100.00** | | | **0** |

## EXERCISE COSTS

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

| | | | | | |
|---|---|---|---|---|---|
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | | $ $ | | |
| | | 0 | $ 0.00 $ 0.00 | | 0 |
| **Total** | | **0** | **$ 0.00** $0.00 | | **0** |

## Document Uploads *top*

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

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

Application ID: 444205

| | | |
|---|---|---|
| | **Applicant Name** | Office of Cyber Defense Coordination |
| | **Project Name:** | NV Shared Cyber Threat Intelligence Platform |
| | **Project Funding Stream:** | FY 2022 SLCGP |
| | Milestone Description* | Date of Expected Completion |
| 1 | Create initial log collection system | Fall 2023 |
| 2 | Implement initial threat analytics on collected data | March, 2024 |
| 3 | Implement centralized threat reporting receiver | June, 2024 |
| 4 | Implement threat sharing between endpoints and central recieiver | August, 2024 |
| 5 | Implement outbound threat sharing feeds to share threats with partner entities | December, 2024 |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |

*Please add additional rows as necessary for your project

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | NV Office of Cyber Defense Coordination | |
| **Cybersecurity Plan Required Elements** | **Brief Description of Current Cybersecurity Capabilities For Each Element** | **Select capability level from:**<br>Foundational<br>Fundamental<br>Intermediary<br>Advanced |
| 1. Manage, monitor, and track information systems, applications, and user accounts | N/A - OCDC does not ahve any systems they manage. | |
| 2. Monitor, audit, and track network traffic and activity | N/A - OCDC does not ahve any networks they manage. | |
| 3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| 4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk | OCDC acts in an advisory capacity to other entities for this function, partnering with the National Guard's assessment capabilities. | Foundational |
| 5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST) | OCDC acts in an advisory capacity to other entities for this function. | Fundamental |
| a. Implement multi-factor authentication | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| b. Implement enhanced logging | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| c. Data encryption for data at rest and in transit | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| d. End use of unsupported/end of life software and hardware that are accessible from the Internet | N/A - OCDC does not manage any systems of this sort. | |
| e. Prohibit use of known/fixed/default passwords and credentials | OCDC is attempting to start up a program to support testing for this. | Foundational |
| f. Ensure the ability to reconstitute systems (backups) | N/A - OCDC does not manage any systems of this sort. | |
| g. Migration to the .gov internet domain | This has been completed for the OCDC, and we are actively working with other entities to encourage this. | Advanced |
| 6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| 7. Ensure continuity of operations including by conducting exercises | OCDC partners with DEM and other entities to participate in and conduct exercises | Advanced |
| 8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity) | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| 9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks | OCDC acts in an advisory capacity to other entities for this function. | Foundational |

| FY 2022 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM<br>CAPABILITIES ASSESSMENT WORKSHEET | | |
|---|---|---|
| **ENTITY NAME:** | NV Office of Cyber Defense Coordination | |
| 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 eligible entity | OCDC acts in an advisory capacity to other entities for this function, partnering with the National Guard's assessment capabilities. | Foundational |
| 11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department | OCDC is attempting to start up a program to support this functionality, which is what this grant application is for. | Foundational |
| 12. Leverage cybersecurity services offered by the Department | OCDC acts in an advisory capacity to other entities for this function. | Fundamental |
| 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats | OCDC acts in an advisory capacity to other entities for this function. | Foundational |
| 15. Ensure rural communities have adequate access to, and participation in plan activities | OCDC is actively working to bring this functionality to rural communities. | Fundamental |
| 16. Distribute funds, items, services, capabilities, or activities to local governments | N/A - OCDC does not manage funds distribution | |