

# STATE OF NEVADA CYBERSECURITY PLAN



Federal Fiscal Year 2022

Approved by the NEVADA CYBER SECURITY TASK FORCE on MMMM DD, 2023  
Version 3.0

DRAFT – INTERNAL WORKING DOCUMENT

DRAFT

# TABLE OF CONTENTS

<b>Letter from THE NEVADA CYBER SECURITY TASK FORCE.....</b>	<b>1</b>
<b>Introduction .....</b>	<b>3</b>
Vision and Mission .....	5
Cybersecurity Program Goals and Objectives .....	5
<b>Cybersecurity Plan Elements .....</b>	<b>6</b>
Manage, Monitor, and Track .....	6
Monitor, Audit, and Track .....	7
Enhance Preparedness .....	7
Assessment and Mitigation .....	8
Best Practices and Methodologies .....	9
Safe Online Services .....	10
Continuity of Operations .....	10
Workforce .....	11
Continuity of Communications and Data Networks.....	12
Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources.....	12
Cyber Threat Indicator Information Sharing.....	13
Leverage CISA Services .....	14
Information Technology and Operational Technology Modernization Review .....	14
Cybersecurity Risk and Threat Strategies .....	15
Rural Communities .....	16
<b>Funding &amp; Services.....</b>	<b>17</b>
Distribution to Local Governments .....	18
<b>Assess Capabilities.....</b>	<b>19</b>
<b>Implementation Plan .....</b>	<b>20</b>
Organization, Roles and Responsibilities .....	20
Resource Overview and Timeline Summary.....	21
<b>Metrics .....</b>	<b>23</b>
<b>Appendix A: Cybersecurity Plan Capabilities Assessment .....</b>	<b>25</b>
<b>Appendix B: Project Summary Worksheet .....</b>	<b>29</b>
<b>Appendix C: Entity Metrics.....</b>	<b>35</b>
<b>Appendix D: Acronyms.....</b>	<b>37</b>



## LETTER FROM THE NEVADA CYBER SECURITY TASK FORCE

Greetings,

The Cyber Security Task Force for the State of Nevada is pleased to present to you the 2023-2025 Nevada Cybersecurity Plan. The Cybersecurity Plan represents the State's continued commitment to improving cybersecurity and supporting our State, as well as cybersecurity practitioners across our local jurisdictions. In addition, this update meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the Governor's Office; Executive, Legislative and Judicial Branches of State government, including the Department of Health and Human Services, the Division of Emergency Management/Homeland Security (DEM), the Office of Cyber Defense Coordination (OCDC), and the Office of Information Security; the Secretary of State's office; the Nevada System of Higher Education; and representatives from school districts, counties (urban and rural), National Guard, Tribal authorities, and business, collaborated to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on securing the State's infrastructure, information, computing environment, and vital resources. They are designed to support our entity in planning for new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the SLCGP required plan elements.

As we continue to enhance cybersecurity, we must remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.

Sincerely,

---

Robert Dehnhardt  
State CISO  
Department of Administration, Office of Information Security

---

Tim Robb  
Special Advisor to the Governor, Cyber Security Task Force Chair  
Office of the Governor



## INTRODUCTION



The Cybersecurity Plan is a three-year strategic planning document that contains the following components:

- **Vision and Mission:** Articulates the vision and mission for improving cybersecurity resilience interoperability over the next one-to-three-years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within Nevada as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of the Nevada’s cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of Nevada’s state or local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** Describes how inputs from local governments as used in order to reduce overall cybersecurity risk across the eligible entity. This is especially important in order to develop a holistic cybersecurity plan.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within Nevada along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the Nevada’s plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation plan must include the resources and timeline where practicable.
- **Metrics:** Describes how Nevada will measure the outputs and outcomes of the program across the entity.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework<sup>1</sup>, included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

<sup>1</sup> <https://www.nist.gov/cyberframework/getting-started>

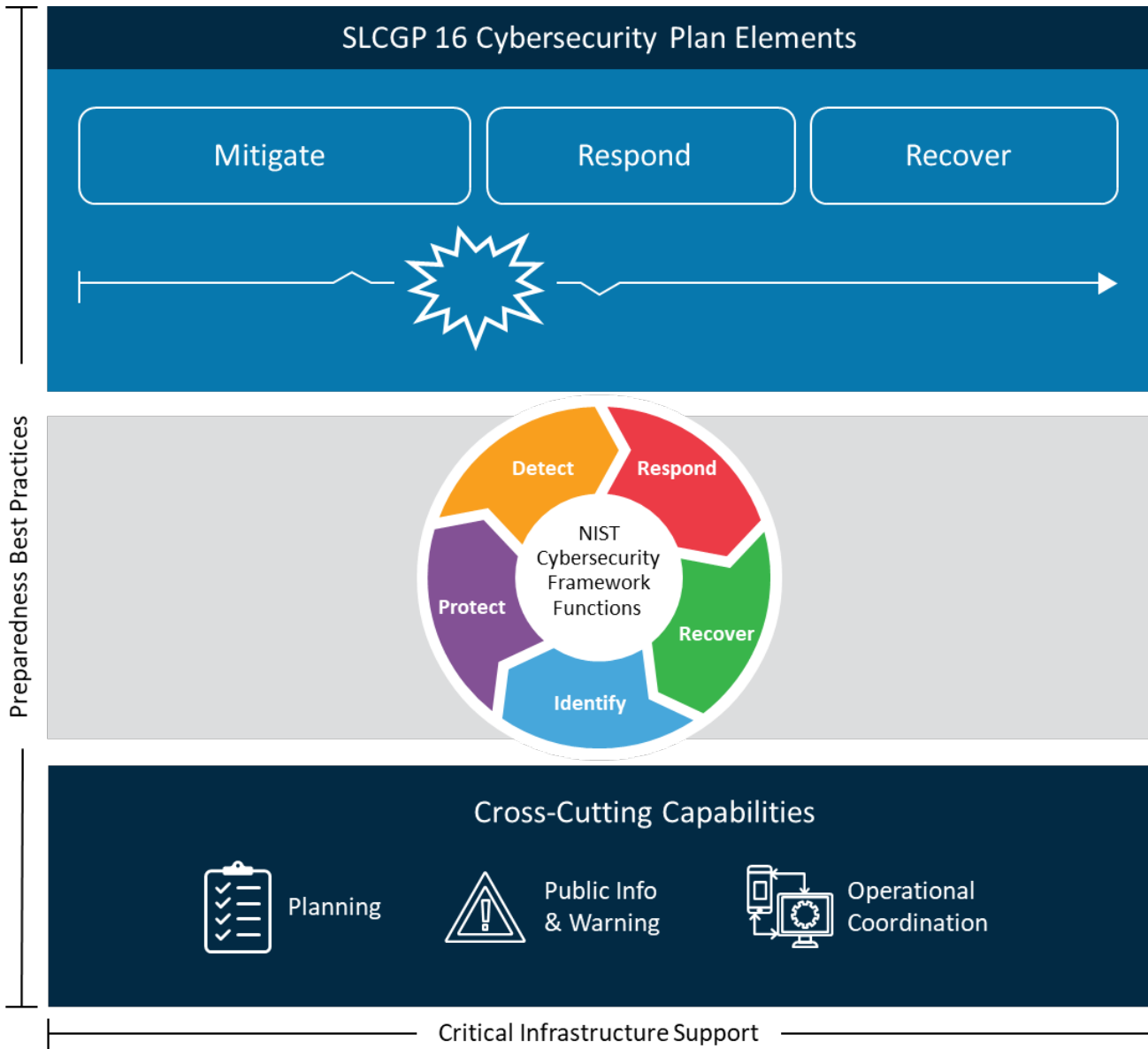


Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans



## Vision and Mission

This section describes Nevada’s vision and mission for improving cybersecurity:

**Vision:**

*A comprehensive security culture and community consisting of proactive and collaborative partnerships building engagement, trust, and resilient security management at all levels of government within the State.*

**Mission:**

*Provide guidance and support for entity security initiatives, policy, standards and best practices, and access to enterprise-level security tools and services.*

## Cybersecurity Program Goals and Objectives

The overall goal of the Plan is to reduce cyber risk while enhancing Nevada’s resilience. This Plan embraces the principles of a collective defense model and whole-of-government approach to cybersecurity. Throughout the period of performance for the SLCGP, the following goals, objectives, and action items will be pursued to full execute the Plan. Integrated within and across these objectives are three of four SLCGP goals and 16 key elements set out in the SLCGP Notice of Funding Opportunity (NOFO).

Nevada’s Cybersecurity goals and objectives include the following:

Nevada’s Cybersecurity Program	
Program Goal	Program Objectives
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.	1.1 Establish a structured outreach program targeting local government IT leaders and emergency managers, fostering communication and collaboration for consequence management and grants coordination.
2. Understand Nevada’s current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structure assessments.	2.1 Establish a state-wide cybersecurity capabilities assessment program with actionable results and improvement tracking.
	2.2 Enhance information and intelligence sharing between the OCDC and local government IT leaders and emergency managers.
3. Implement security protections commensurate with risk.	3.1 Ensure Multi-Factor Authentication (MFA) enabled where possible for devices with access to Nevada’s sensitive information or critical systems

## CYBERSECURITY PLAN ELEMENTS

This plan incorporates the following governance:

- Executive Branch Information Security Program Policy and Standards provide authorizations, governance and best practices aligned with Center of Internet Security (CIS) and NIST frameworks. This governance is developed by the State Information Security Committee, under authority granted in Nevada Revised Statute (NRS) 242.111.
- NRS 480.920 establishes OCDC, with duties including development of strategies, standards and guidelines for preparation, risk mitigation and protection of systems operated or maintained by agencies within the State, and coordination of state-wide programs for awareness and training regarding security risk. The Office is tasked with establishing partnerships with local governments to assist and receive assistance with these duties.
- NRS 603A establishes security and privacy requirements for Personal Identifiable Information for all government entities within the State that are categorized as “data collectors” as defined in the statute.

### Manage, Monitor, and Track

It is widely acknowledged that safeguarding the unknown remains a challenge. An exhaustive registry encompassing hardware, software, and data, well-documented processes, work- and dataflows, and adherence to regulatory compliance, is essential in delineating the protected environment and determining the appropriate defense measures—this comprehensive inventory further guides patching and replacement necessities, as well as incident response protocols. Being well-informed about the hardware and software in use and their respective versions and locations can prove invaluable in responding promptly and efficiently to pervasive threats such as the log4j software vulnerability. While certain entities within the State presently conduct inventories, the consistency of these efforts varies, and the means to share inventory information currently need to be made available.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #1:

Project Number	Project Name	Cost	Project Type
443741	Washoe County: Cortex XDR Host Insights	\$27,931.00 (FFY22 SLCGP)	Organization Equipment Training
444165	Douglas County: Firewall/Network Edge Refresh	\$86,915.00 (FFY22 SLCGP)	Equipment
444205	Governor’s Office of Cyber Defense: Nevada	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training

	Shared Cyber Threat Intelligence Platform		
--	---	--	--

**Monitor, Audit, and Track**

An integral facet of an extensive cybersecurity program involves the capacity to discern and monitor aberrant traffic traversing the entirety of the enterprise, subsequently correlating this behavior with identified vulnerabilities. Coordinated endeavors to contain and alleviate any malicious attacks are paramount. Such activities predominantly occur uncoordinatedly within most State, Local, Tribal, and Territorial (SLTT) entities in Nevada, needing more standardized coordination of findings or event correlation. As malware with lateral mobility capabilities becomes more prevalent, the State's capability to trace and manage it across multiple entities is critical in containing the malware, promptly and appropriately responding to threats, and safeguarding the overall environment.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #2:

Project Number	Project Name	Cost	Project Type
443335	Washoe County: Annual Penetration Testing	\$44,000.00 (FFY22 SLCGP)	Organization
443738	Washoe County: Incident Response Plan	\$35,000.00 (FFY22 SLCGP)	Organization
443741	Washoe County: Cortex XDR Host Insights	\$27,931.00 (FFY22 SLCGP)	Organization Equipment Training
443961	City of Sparks, Nevada Cybersecurity	\$109,050.00 (FFY22 SLCGP)	Organization
444165	Douglas County: Firewall/Network Edge Refresh	\$86,915.00 (FFY22 SLCGP)	Equipment
444205	Governor’s Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training

**Enhance Preparedness**

Exercises of Disaster Recovery (DR), Continuity of Operations Plan (COOP), and Incident Response (IR) have been conducted at diverse tiers throughout the State. Nevada has actively engaged in Cyber Storm exercises whenever accessible, in addition to participating in exercises and workshops led by CISA. However, the current approach has been ad hoc or contingent on availability. Implementing a structured and recurring schedule of exercises across all government levels would significantly bolster the development and efficacy of DR, COOP, and IR plans.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #3:

Project Number	Project Name	Cost	Project Type
443318	White Pine County SLCGP FY2022	\$39,740.75 (FFY22 SLCGP)	Organization Training
443738	Washoe County: Incident Response Plan	\$35,000.00 (FFY22 SLCGP)	Organization
443961	City of Sparks, Nevada Cybersecurity	\$109,050.00 (FFY22 SLCGP)	Organization
444167	Douglas County: Backup Datacenter Environment	\$119,292.08 (FFY22 SLCGP)	Equipment
444205	Governor's Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training

### Assessment and Mitigation

Diverse entities within the State undertake continuous monitoring, assessment, and mitigation of detected threats using various approaches. The entities conduct certain activities internally, while others are outsourced to managed security service providers. There is no centralized state-wide function for aggregating and evaluating logs or traffic, correlating events across multiple entities, or orchestrating mitigation efforts in numerous environments.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #4:

Project Number	Project Name	Cost	Project Type
443335	Washoe County: Annual Penetration Testing	\$44,000.00 (FFY22 SLCGP)	Organization
443741	Washoe County: Cortex XDR Host Insights	\$27,931.00 (FFY22 SLCGP)	Organization Equipment Training
443961	City of Sparks, Nevada Cybersecurity	\$109,050.00 (FFY22 SLCGP)	Organization

444205	Governor’s Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training
--------	--	----------------------------	---------------------------------

**Best Practices and Methodologies**

As per NRS 603A, all government entities in Nevada meeting the definition of "data collector" as outlined in NRS are required to make practicable efforts to adhere to the prevailing version of the CIS Controls published by the Center for Internet Security, Inc., or its successor organization, or the corresponding standards endorsed by the NIST of the United States Department of Commerce (NRS 603A.210.2, effective January 1, 2021).

All State agencies have adopted or are currently adopting the suitable standards from CIS or NIST Cyber Security Framework. These endeavors are influenced by the nature of the information being safeguarded and the available resources, thereby determining the level of protection, detection, response, and recovery measures to be implemented. Furthermore, guidance is being sought from relevant Federal regulations and industry best practices to reinforce the overall security posture.

Current security policy and standards for the Executive Branch of government are published at [https://it.nv.gov/Governance/Security/State\\_Security\\_Policies\\_Standards\\_Procedures/](https://it.nv.gov/Governance/Security/State_Security_Policies_Standards_Procedures/). These documents are freely available to all Nevada government entities, and can be used as templates for development of their own governance. These standards include provisions for:

- Implementing multi-factor authentication.
- Implementing enhanced logging.
- Requiring data encryption for data at rest and in transit.
- Retiring/replacing unsupported/end of life software and hardware, both internal and accessible from the Internet.
- Prohibiting use of known/fixed/default passwords and credentials.
- Ensuring the ability to reconstitute systems (backups).
- Reporting of incidents and coordination of response
- Discovery, tracking and mitigation of vulnerabilities
- Security awareness training for all employees

Furthermore, adopting cyber supply chain best practices is strongly recommended in alignment with NIST's guidance. Nevada will integrate NIST's cyber supply chain best practices into the ongoing efforts to update and revise the State's *Resource and Supply Chain Management Operational Plan*.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #5:

Project Number	Project Name	Cost	Project Type
444205	Governor’s Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training
444166	Douglas County: Multi-Factor Authentication for End-Users/Endpoints	\$4,772.00 (FFY22 SLCGP)	Equipment
444164	Douglas County: Physical Security - Badge/Card Reader System	\$101,204.17 (FFY22 SLCGP)	Equipment
444224	Pershing County: Multifactor Authentication	\$28,580.00 (FFY22 SLCGP)	Planning Organization Equipment

### Safe Online Services

Nevada entities are being strongly encouraged to adopt the (.gov) Top Level Domain (TLD) for all online services, and substantial efforts are underway to transition away from other domains. Given the federated nature of the State, the absence of a singular governing body with the authority to mandate such a domain shift is acknowledged.

Moreover, the Nevada Enterprise IT Services Division (EITS) has actively enrolled in the StateRAMP program to facilitate the procurement of cloud services, signifying the State's commitment to enhancing its cybersecurity posture and ensuring robust security measures are in place for cloud-based operations.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #6:

Project Number	Project Name	Cost	Project Type
443335	Washoe County: Annual Penetration Testing	\$44,000.00 (FFY22 SLCGP)	Organization
443738	Washoe County: Incident Response Plan	\$35,000.00 (FFY22 SLCGP)	Organization

### Continuity of Operations

Continuity of Operations planning for cyber/IT operations varies across different levels within the State. Numerous existing plans are remnants of the COVID-19 response and predominantly concentrate on

pandemic-specific operations. There is a pressing need for a more comprehensive endeavor to formulate resilient plans, augmented by regular testing, to effectively fortify cyber/IT operations against potential disruptions.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #7:

Project Number	Project Name	Cost	Project Type
443318	White Pine County SLCGP FY2022	\$39,740.75 (FFY22 SLCGP)	Organization Training
444164	Douglas County: Physical Security - Badge/Card Reader System	\$101,204.17 (FFY22 SLCGP)	Equipment
444167	Douglas County: Backup Datacenter Environment	\$119,292.08 (FFY22 SLCGP)	Equipment

### Workforce

The challenge of attracting and retaining qualified staff in Nevada is a shared concern faced by numerous regions. Cyberseek.org data reveals a substantial demand, with over 7,000 cybersecurity job openings in the State, encompassing 514 public sector positions. Given this intense competition, adopting a more prudent approach entails prioritizing current talent retention and fostering professional growth through diverse avenues, including online or classroom courses, on-the-job training, job shadowing, and mentoring.

Nevada is actively collaborating with the Department of Veterans Affairs to facilitate a smooth transition for separating veterans into civilian life by providing training, mentoring, and employment opportunities in cybersecurity alongside other career paths.

Beyond the technical staff, implementing security awareness training and testing has emerged as a crucial strategy in diminishing vulnerabilities to social engineering attacks, such as phishing. The widespread adoption of MFA has further reduced incidents involving stolen credentials and ransomware state-wide.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #8:

Project Number	Project Name	Cost	Project Type
443318	White Pine County SLCGP FY2022	\$39,740.75 (FFY22 SLCGP)	Organization Training

### Continuity of Communications and Data Networks

Entities within the State are strongly encouraged to prioritize establishing redundant communication networks and tools and comprehensive contingency and disaster recovery plans for these systems. Moreover, diligent efforts are underway to develop and maintain multiple data, communications, and intelligence pathways, enabling alternative means of conveying critical information during unforeseen outages and emergencies. This strategic approach ensures the continuity and reliability of essential communication channels in times of crisis.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #9:

Project Number	Project Name	Cost	Project Type
444205	Governor’s Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training
444165	Douglas County: Firewall/Network Edge Refresh	\$86,915.00 (FFY22 SLCGP)	Equipment

### Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

Nevada is actively promoting a comprehensive assessment process across all entities State-wide. To achieve this, we are exploring adopting assisted Assessment services provided by CISA wherever feasible. For cases where such services are currently not feasible, we are collaborating with other entities to ensure a thorough assessment.

Furthermore, the State is diligently working towards establishing a centralized repository to house risk assessment and disaster recovery plans. This initiative aims to enhance accessibility and facilitate effective planning and response efforts for potential risks and disruptions.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."



The following projects were selected to address SLCGP Required Element #10:

Project Number	Project Name	Cost	Project Type
443335	Washoe County: Annual Penetration Testing	\$44,000.00 (FFY22 SLCGP)	Organization
443468	Nevada Cybersecurity for the Judiciary	\$925,000.00 (FFY22 SLCGP)	Planning Organization
443738	Washoe County: Incident Response Plan	\$35,000.00 (FFY22 SLCGP)	Organization
443741	Washoe County: Cortex XDR Host Insights	\$27,931.00 (FFY22 SLCGP)	Organization Equipment Training
444224	Pershing County: Multifactor Authentication	\$28,580.00 (FFY22 SLCGP)	Planning Organization Equipment
444205	Governor's Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training
444165	Douglas County: Firewall/Network Edge Refresh	\$86,915.00 (FFY22 SLCGP)	Equipment
444166	Douglas County: Multi-Factor Authentication for End-Users/Endpoints	\$4,772.00 (FFY22 SLCGP)	Equipment

### Cyber Threat Indicator Information Sharing

All branches of State-level government, counties, and numerous cities, school districts, and local entities are active members of MS-ISAC or EI-ISAC. Encouragement for membership is extended to all levels of government. Open dialogue and information exchange are promoted through committees and groups such as the State Information Security Committee and the Southern Nevada Government Cybersecurity Group to foster a secure and collaborative atmosphere. Secure online resources, including Signal and Discord, are leveraged to facilitate communication among entities.

By cultivating a climate of security, openness, and transparency, we aim to enhance communication, cooperation, and coordination across all levels of government. Utilizing additional tools such as Anomali and other threat intel or integrated risk management platforms further enables the seamless sharing of threat and incident information among entities, contributing to a more resilient and united cybersecurity posture.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #11:

Project Number	Project Name	Cost	Project Type
444205	Governor’s Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training

**Leverage CISA Services**

Nevada actively participates in MS-ISAC's vulnerability scanning and web application scanning programs alongside their Malicious Domain Blocking and Reporting service. Furthermore, we have deployed Albert sensors at the perimeters of the enterprise computing environment and within all county election offices. Entities are strongly encouraged to deliberate on leveraging the tools and services provided by MS-ISAC and CISA when evaluating new initiatives and programs to bolster our cybersecurity capabilities. Such strategic adoption can enhance the overall security posture and resilience of our State's information technology landscape.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

Given current resource constraints, projects in this category have yet to be planned. However, they are receiving careful consideration for future initiatives during upcoming grant years, significantly as we strengthen our partnership with CISA representatives within the State.

**Information Technology and Operational Technology Modernization Review**

The prevailing consensus within the government sector acknowledges that legacy or unsupported systems pose a substantial and tangible threat in any operational environment. As part of proactive risk management, diligent tracking of Vendor End-Of-Life announcements is undertaken, accompanied by corresponding budget adjustments and timely notifications to staff for system replacements before they reach their end-of-support status.

Despite these proactive measures, challenges may arise in the replacement and modernization efforts due to budget approval processes and competing entity priorities. The constraints imposed by limited resources in the government sector necessitate careful deliberation and strategic allocation of funds to ensure successful and timely modernization initiatives.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #13:

Project Number	Project Name	Cost	Project Type
443741	Washoe County: Cortex XDR Host Insights	\$27,931.00 (FFY22 SLCGP)	Organization Equipment Training
444164	Douglas County: Physical Security - Badge/Card Reader System	\$101,204.17 (FFY22 SLCGP)	Equipment
444165	Douglas County: Firewall/Network Edge Refresh	\$86,915.00 (FFY22 SLCGP)	Equipment
444166	Douglas County: Multi-Factor Authentication for End-Users/Endpoints	\$4,772.00 (FFY22 SLCGP)	Equipment
444224	Pershing County: Multifactor Authentication	\$28,580.00 (FFY22 SLCGP)	Planning Organization Equipment

## Cybersecurity Risk and Threat Strategies

The communication channels and approaches highlighted earlier concerning Cyber Threat Indicator Information Sharing can be effectively utilized to facilitate communications and coordination concerning risk and threat strategies. Given Nevada's federated environment, the foundation of these endeavors primarily rests on collaborative partnerships and a framework of trust rather than relying solely on isolated technical solutions. Emphasizing this cooperative approach enables a more cohesive and synergistic response to risk and threat management across the State.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #14:

Project Number	Project Name	Cost	Project Type
443335	Washoe County: Annual Penetration Testing	\$44,000.00 (FFY22 SLCGP)	Organization
443468	Nevada Cybersecurity for the Judiciary	\$925,000.00 (FFY22 SLCGP)	Planning Organization
443738	Washoe County: Incident Response Plan	\$35,000.00 (FFY22 SLCGP)	Organization
444205	Governor's Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training

## Rural Communities

In this comprehensive three-year plan, three distinct Program Goals are outlined to advance and enhance cybersecurity practices throughout the State and its political subdivisions, including rural communities with populations of fewer than 50,000 residents. Addressing cybersecurity in rural communities poses a unique challenge in Nevada, where certain counties, more significant in size than some states, have populations smaller than many towns.

The Governor's Office of Science, Innovation & Technology is currently assigned with the task of improving broadband accessibility in rural and underserved regions of Nevada to tackle this challenge effectively. In this endeavor, the office is willing to collaborate with both local and State government entities to ensure the inclusion of access to essential cybersecurity tools and services in these areas. This collaborative approach aims to bolster the overall cybersecurity posture and resilience of rural communities and foster a more secure digital environment across the State.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #15:

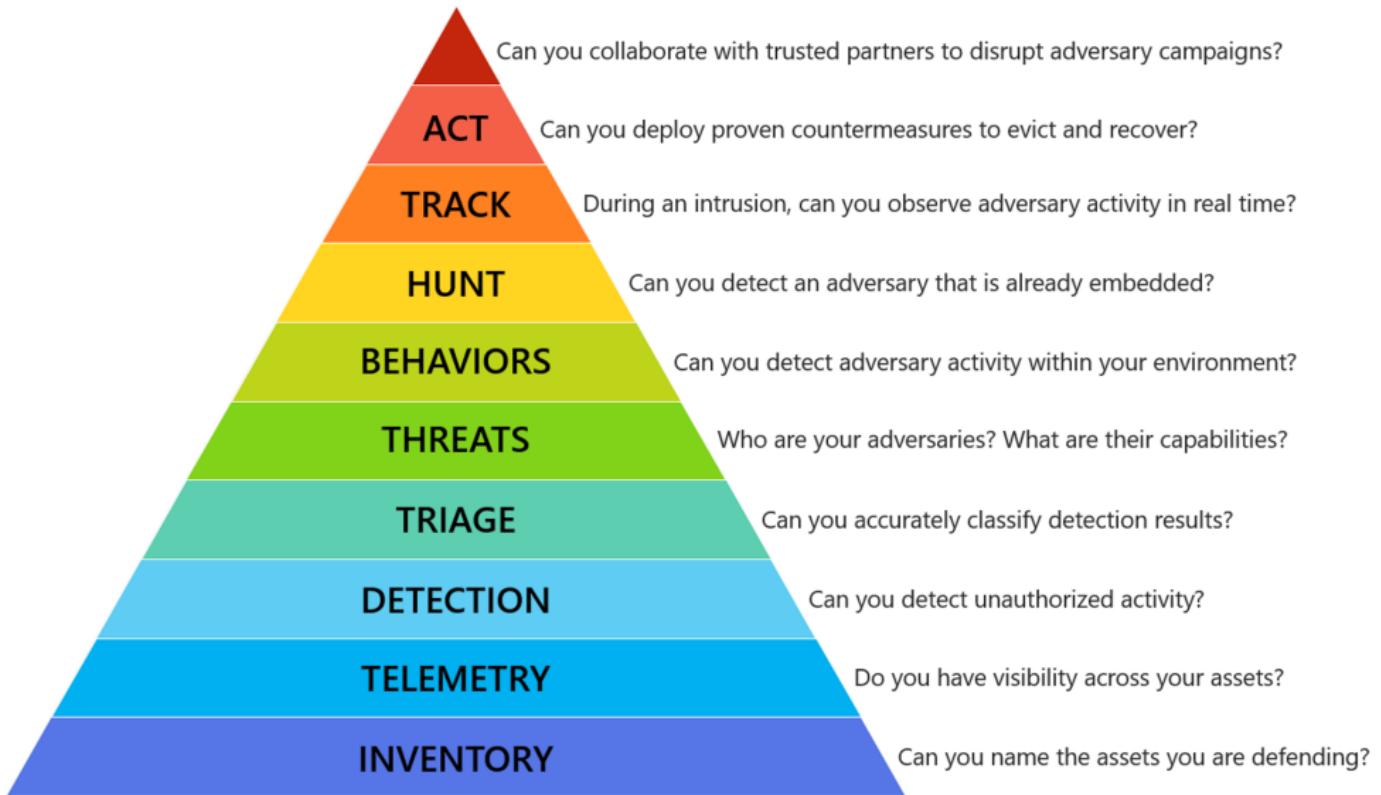
Project Number	Project Name	Cost	Project Type
443318	White Pine County SLCGP FY2022	\$39,740.75 100% to Rural Communities (FFY22 SLCGP)	Organization Training
443335	Washoe County: Annual Penetration Testing	\$44,000.00 36% to Rural Communities (FFY22 SLCGP)	Organization
443468	Nevada Cybersecurity for the Judiciary	\$925,000.00 25% to Rural Communities (FFY22 SLCGP)	Planning Organization
443738	Washoe County: Incident Response Plan	\$35,000.00 36% to Rural Communities (FFY22 SLCGP)	Organization
443741	Washoe County: Cortex XDR Host Insights	\$27,931.00 36% to Rural Communities	Organization Equipment

		(FFY22 SLCGP)	Training
444164	Douglas County: Physical Security - Badge/Card Reader System	\$101,204.17 100% to Rural Communities (FFY22 SLCGP)	Equipment
444165	Douglas County: Firewall/Network Edge Refresh	\$86,915.00 100% to Rural Communities (FFY22 SLCGP)	Equipment
444166	Douglas County: Multi-Factor Authentication for End-Users/Endpoints	\$4,772.00 100% to Rural Communities (FFY22 SLCGP)	Equipment
444167	Douglas County: Backup Datacenter Environment	\$119,292.08 100% to Rural Communities (FFY22 SLCGP)	Equipment
444205	Governor's Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	\$150,000.00 80% to Rural Communities (FFY22 SLCGP)	Organization Equipment Training
444224	Pershing County: Multifactor Authentication	\$28,580.00 100% to Rural Communities (FFY22 SLCGP)	Planning Organization Equipment

## FUNDING & SERVICES

The primary objective of the SLCGP is to enhance the overall preparedness level of the entire state, encompassing all entities. A systematic progression up the preparedness pyramid (illustrated below) will be executed in Nevada with each subsequent round of funding to achieve this. As this marks the program's inaugural year, our immediate focus is laying the groundwork for identifying our existing assets and determining our current position. This foundational step will establish a baseline from which we can conduct a comprehensive gap analysis, evaluating our strengths and weaknesses. The outcome of this analysis will aid us in pinpointing areas with the greatest needs and identifying resources that can be

strategically harnessed to have a broader and more impactful effect.



### Distribution to Local Governments

The State will employ multiple communication channels, including public meetings, bulletins disseminated through the Nevada Commission on Homeland Security (NCHS) Listserv, social media platforms, direct messaging, and the DEM Homeland Security Grant Resources Page ([https://dem.nv.gov/homeland\\_security/Grant\\_Resources/](https://dem.nv.gov/homeland_security/Grant_Resources/)), to inform local political subdivisions, including rural communities, about opportunities to participate in the SLCGP project proposal process. Additionally, collaboration with local government associations and organizations, including representatives on the CSTF and advisory roles, will be leveraged to promote the SLCGP opportunities.

Given the finite nature of SLCGP funds, approving all requests for project funding, equipment, services, or software may not be feasible. In the initial year of the SLCGP, Nevada will focus on cost-effective and scalable cybersecurity projects, aiming to provide services to all political subdivisions, including local and rural communities. These projects will adhere to established best practices for allocating funds, items, services, capabilities, or activities to local governments, with a 25% pass-through of grant funding to rural communities, as detailed in the table found in **Appendix B: Project Summary Worksheet**. This approach aligns with **State and Local Cybersecurity Improvement Act: e.2.B.xvi**.

An analysis of the SLCGP guidance and requirements underscores the intent to extend coverage to as many entities as possible. While parceling funds to individual entity subgrantees proves effective in some instances, applying this approach to the entire grant amount could dilute the program's overall effectiveness. To maximize impact and achieve economies of scale, the State seeks to identify effective and necessary programs and services that can be procured state-wide and extended to all entities. This

approach promises to yield the most significant benefits for rural areas while optimizing program effectiveness and service pricing.

An inaugural Cybersecurity Plan Capabilities Assessment was executed, encompassing a comprehensive entity-wide perspective by integrating the combined score of State- and local-level evaluations. Given that several State-level and local-level entities are presently in the nascent stages of establishing their cybersecurity programs, the interconnectivity of our environments rendered the capability level of this element as "Foundational."

The following projects were selected to address SLCGP Required Element #16:

Project Number	Project Name	Cost	Project Type
443318	White Pine County SLCGP FY2022	\$39,740.75 (FFY22 SLCGP)	Organization Training
443335	Washoe County: Annual Penetration Testing	\$44,000.00 (FFY22 SLCGP)	Organization
443738	Washoe County: Incident Response Plan	\$35,000.00 (FFY22 SLCGP)	Organization
443741	Washoe County: Cortex XDR Host Insights	\$27,931.00 (FFY22 SLCGP)	Organization Equipment Training
443961	City of Sparks, Nevada Cybersecurity	\$109,050.00 (FFY22 SLCGP)	Organization
444164	Douglas County: Physical Security - Badge/Card Reader System	\$101,204.17 (FFY22 SLCGP)	Equipment
444165	Douglas County: Firewall/Network Edge Refresh	\$86,915.00 (FFY22 SLCGP)	Equipment
444166	Douglas County: Multi- Factor Authentication for End- Users/Endpoints	\$4,772.00 (FFY22 SLCGP)	Equipment
444167	Douglas County: Backup Datacenter Environment	\$119,292.08 (FFY22 SLCGP)	Equipment
444224	Pershing County: Multifactor Authentication	\$28,580.00 (FFY22 SLCGP)	Planning Organization Equipment

## ASSESS CAPABILITIES

As previously highlighted, Nevada operates within a highly federated structure, resulting in diverse capabilities among its entities. At the county level, there exists a spectrum of IT and cybersecurity departments, ranging from fully staffed and trained teams to singular individuals handling all IT responsibilities. This varying landscape necessitates a comprehensive approach to assess the State's Cybersecurity Capabilities.

As part of the Federal Fiscal Year (FFY) 22 SLCGP application process, applicants and sub-applicants conducted an initial Cybersecurity Capabilities Assessment, laying the groundwork for identifying the existing landscape and understanding our current position. Appendix A: Cybersecurity Plan Capabilities Assessment outlines Nevada's baseline Cybersecurity Capabilities Assessment derived from the FFY 22 SLCGP Cybersecurity Plan development and project selection process. This foundational assessment facilitated a thorough gap analysis, allowing us to identify areas of greatest need and potential resources that can be harnessed for broader impact.

Building on this foundation, Nevada will collaborate with the DEM to conduct the Cybersecurity Capabilities Assessment annually with State Agencies, local political subdivisions, and tribal nations, beginning in the calendar year 2023. This iterative assessment approach will ensure continuous improvements and ongoing monitoring of the State's cybersecurity preparedness and resilience.

## IMPLEMENTATION PLAN

### Organization, Roles and Responsibilities

Nevada's IT structure is federated, without a central entity exercising authority over all levels of government. Within the Executive Branch, the Office of Information Security and State Information Security Committee is responsible for formulating policy and coordinating cybersecurity initiatives. The Legislative and Judicial Branches and the Nevada System of Higher Education maintain their distinct security policies and processes.

To foster effective coordination, the OCDC is pivotal in facilitating collaboration among local government entities, promoting synergies between local and State entities, and strengthening connections between State and private entities.

This coordination of effort is realized through establishing and supporting the security community, which actively encourages partnership and cooperation among all relevant stakeholders. A shared understanding exists that unity and mutual support enhance collective strength and resilience. As we stand together, united in purpose, we reinforce our cybersecurity defenses and collectively contribute to a more secure and safeguarded IT landscape.

#### *Governor's Cyber Security Task Force*

The Nevada CSTF was established via Executive Order 2022-11 by then-Governor Steve Sisolak. The purpose of the CSTF is to facilitate cooperation between federal, State, local, and tribal governments, as well as the private sector. The CSTF is responsible for:

1. Establishing itself as an eligible entity for SLCGP funding.
2. Developing, implementing, or revising the cyber plan required by SLCGP.
3. Identifying and providing advice and recommendations to Governor's Office, Department of Administration Chief Information Security Officer (CISO), OCDC Administrator, and Chief of DEM regarding future funding opportunities to support ongoing cybersecurity infrastructure.
4. Providing advice and recommendations to the OCDC Administrator pursuant to Nevada Revised Statute 480.900.
5. Providing advice and recommendations to the OCDC Administrator, Legislature, the Governor, regarding necessary legislative action to address cyber security challenges and needs.



The CSTF members do not receive compensation for their services. The CSTF performs its duties through established bylaws. The Governor's Office Liaison serves as the CSTF Chairman, and the Department of Administration CISO was elected Vice-Chairman. The CSTF meets at the discretion of its Chairman.

The following members are appointed to the CSTF by the Governor:

- The Governor or his or her designee
- The OCDC Administrator
- The Chief of DEM
- The Department of Administration CISO
- One representative from the State Judicial Branch who serves as an Information Security Advisor (ISO)
- One representative from the State Legislative Branch who serves as an ISO
- One representative from Secretary of State's Office who serves as an ISO
- One representative from the Nevada Department of Health and Human Services (DHHS) who serves as an ISO
- One representative from counties with a population less than 100,000 who serves as an ISO or Emergency Manager
- One representative from Clark County who serves as an ISO or Emergency Manager
- One representative from Washoe County who serves as an ISO or Emergency Manager
- A senior leader from the Nevada National Guard, Office of the Military
- One Tribal representative as recommended by the Nevada Indian Commission
- Two members who represent a business, organization, or association

At a public meeting, the CSTF will conduct hearings where representatives of SLCGP projects, who submitted FFY 2022 SLCGP project proposals and budgets, can present their proposals. Each presentation is limited to a maximum of five minutes.

Following the presentations, the CSTF will evaluate and rank the projects presented during the public meeting. This assessment will involve aggregating the combined rankings assigned to each project. Subsequently, the CSTF members will formally vote to determine the recommended rankings for the SLCGP project proposals.

The CSTF will then submit its endorsed SLCGP projects, along with their rankings, to the State Administrative Agent. The State Administrative Agent will comprehensively review the recommended projects before integrating them into the State's official SLCGP application to the Department of Homeland Security.

## **Resource Overview and Timeline Summary**

Each project approved by the CSTF is carefully aligned with a specific SLCGP Objective/Program Goal, corresponding to Program Objectives and one or more SLCGP required elements. These projects have a well-defined timeline featuring target start and completion dates. Additionally, they are assigned one or more responsible owners who will oversee and coordinate their execution. It is important to note that achieving these goals and objectives will necessitate the support and cooperation of numerous individuals, groups, or agencies.

Formal agenda items will be designated for reviewing the advancements of each project during CSTF meetings to facilitate effective progress tracking. **Appendix B: Project Summary Worksheet** outlines a comprehensive list of cybersecurity projects, with clear links to each SLCGP Objectives/State of Nevada Cyber Security Plan Program Goal and associated SLCGP required elements.

In compliance with the **State and Local Cybersecurity Improvement Act: e.2.E**, the Plan carefully documents the essential resources. It provides a projected timeline for each project, whenever feasible. This meticulous approach ensures that Nevada's Plan satisfies all requirements and aligns with the objectives set forth by the Act.

Project Number	Project Name	Related Required Element #	Cost	Project Type	Target Start Date	Target Completion Date
443318	White Pine County SLCGP FY2022	SLCGP Objective / Program Goal # 3  Elements 3, 7, 8, 15, & 16	\$39,740.75 (FFY22 SLCGP)	Organization Training	7/1/2023	3/31/2024
443335	Washoe County: Annual Penetration Testing	SLCGP Objective / Program Goal #2  Elements 2, 4, 6, 10, 14, 15, & 16	\$44,000.00 (FFY22 SLCGP)	Organization	6 months after FFY 22 SLCGP Funds are Received	6-7 months after FFY 22 SLCGP Funds are Received
443468	Nevada Cybersecurity for the Judiciary	SLCGP Objective / Program Goal #2  Elements 10, 14, & 15	\$925,000.00 (FFY22 SLCGP)	Planning Organization	2 months after FFY 22 SLCGP Funds are Received	12 months after FFY 22 SLCGP Funds are Received
443738	Washoe County: Incident Response Plan	SLCGP Objective / Program Goal #1  Elements 2, 3, 6, 10, 14, 15, & 16	\$35,000.00 (FFY22 SLCGP)	Organization	3 months after FFY 22 SLCGP Funds are Received	3-4 months after FFY 22 SLCGP Funds are Received
443741	Washoe County: Cortex XDR Host Insights	SLCGP Objective / Program Goal #3  Elements 1, 2, 4, 10, 13, 15, & 16	\$27,931.00 (FFY22 SLCGP)	Organization Equipment Training	1 week after funds are received	1 week after funds are received
443961	City of Sparks, Nevada Cybersecurity	SLCGP Objective / Program Goal #2  Elements 2, 3, 4, & 16	\$109,050.00 (FFY22 SLCGP)	Organization	1/10/2024	6/24/2024

444164	Douglas County: Physical Security - Badge/Card Reader System	SLCGP Objective / Program Goal #3  Element 5, 7, 13, 15, & 16	\$101,204.17 (FFY22 SLCGP)	Equipment	9/1/2023	11/1/2023
444165	Douglas County: Firewall/Network Edge Refresh	SLCGP Objective / Program Goal #3  Elements 1, 2, 9, 10, 13, 15, & 16	\$86,915.00 (FFY22 SLCGP)	Equipment	12/1/2024	4/20/2024
444166	Douglas County: Multi-Factor Authentication for End-Users/Endpoints	SLCGP Objective / Program Goal #3  Element 5, 10, 13, 15, & 16	\$4,772.00 (FFY22 SLCGP)	Equipment	12/1/2023	5/30/2024
444167	Douglas County: Backup Datacenter Environment	SLCGP Objective / Program Goal #3  Element 3, 7, 15, & 16	\$119,292.08 (FFY22 SLCGP)	Equipment	8/1/2023	3/16/2024
444205	Governor's Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	SLCGP Objective / Program Goal #1  Element 1, 2, 3, 4, 5, 9, 10, 11, 14, & 15	\$150,000.00 (FFY22 SLCGP)	Organization Equipment Training	Fall 2023	December 2024
444224	Pershing County: Multifactor Authentication	SLCGP Objective / Program Goal #3  Element 5, 10, 13, 15, & 16	\$28,580.00 (FFY22 SLCGP)	Planning Organization Equipment	9/30/2023	12/29/2023

## METRICS

During the entirety of the SLCGP implementation, the CSTF will diligently assess the progress made concerning the SLCGP Objectives/State of Nevada Cyber Security Plan Program Goal, Program Objectives, and the corresponding metrics outlined in this Plan. These metrics align with the required elements specified in the SLCGP NOFO and serve as comprehensive representations of the Plan's objectives.

While some initiatives within the Plan may have varying durations, spanning multiple years, or operating continuously, the CSTF will remain accountable for overseeing progress tracking. This responsibility entails using meaningful metrics and reporting mechanisms to evaluate the Plan's advancements and achievements accurately.

Nevada's Cybersecurity Plan Metrics			
Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
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.	1.1 Establish a structured outreach program targeting local government IT leaders and emergency managers, fostering communication and collaboration for consequence management and grants coordination.	Actively engage 100% of Nevada's counties	OCDC will initiate and track engagement with the counties throughout the next three years of this strategic plan and report the results of the engagement to the CSTF on an annual basis.
2. Understand Nevada's current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structure assessments.	1.2 Establish a state-wide cybersecurity capabilities assessment program with actionable results and improvement tracking.	Actively engage 100% of Nevada's counties	OCDC, in collaboration with DEM, will conduct a cybersecurity capabilities assessment annually and report the results to the CSTF on an annual basis.
	2.1 Enhance information and intelligence sharing between the OCDC and local government IT leaders and emergency managers.	Actively engage Government Cybersecurity Work Group	OCDC will conduct a biennial Government Cybersecurity Work Group meeting and will report the results to the CSTF on an annual basis.
3. Implement security protections commensurate with risk.	3.1 Ensure Multi-Factor Authentication (MFA) enabled where possible for devices with access to Nevada's sensitive information or critical systems	25% of State and local governments have MFA enabled for Nevada's information or critical systems	OCDC, through annual cybersecurity capabilities assessment, will identify and track implementation of MFA and report the results to the CSTF on an annual basis

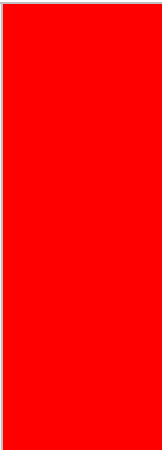
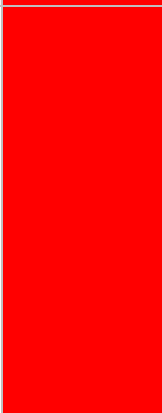
## APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

By taking the following actions, Nevada will demonstrate that its cybersecurity plan incorporates the required assessment relating to the **Cybersecurity Plan Required Elements**. The assessment incorporates an **entity-wide** perspective using a combined score of the State-level and local-level assessments. This assessment also links any line items from the **Appendix B: Project Summary Worksheet** that will help to establish, strengthen, or further develop Nevada’s cybersecurity capabilities.

COMPLETED BY NEVADA				FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) (If applicable – as provided in Appendix B)	Met
1. Manage, monitor, and track information systems, applications, and user accounts	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443741 444165 444205	
2. Monitor, audit, and track network traffic and activity	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443335 443738 443741 443961 444165 444205	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443318 443738 443961 444167 444205	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443335 443741 443961	

			444205	
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	444205 444166 444164 444224	
a. Implement multi-factor authentication	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational		
b. Implement enhanced logging	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational		
c. Data encryption for data at rest and in transit	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational		
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational		
e. Prohibit use of known/fixed/default passwords and credentials	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational		
f. Ensure the ability to reconstitute systems (backups)	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational		
g. Migration to the .gov internet domain	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational		
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443335 443738	
7. Ensure continuity of operations including by conducting exercises	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443318 444164 444167	
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443318	

abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)				
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	444205 444165	
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	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443335 443468 443738 443741 444224 444205 444165 444166	
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	444205	
12. Leverage cybersecurity services offered by the Department	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	N/A	
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443741 444164 444165 444166 444224	
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	No or incomplete implementation across the totality of Nevada State Agencies and local government entities.	Foundational	443335 443468 443738 444205	

<p>15. Ensure rural communities have adequate access to, and participation in plan activities</p>	<p>No or incomplete implementation across the totality of Nevada State Agencies and local government entities.</p>	<p>Foundational</p>	<p>443318 443335 443468 443738 443741 444164 444165 444166 444167 444205 444224</p>	
<p>16. Distribute funds, items, services, capabilities, or activities to local governments</p>	<p>No or incomplete implementation across the totality of Nevada State Agencies and local government entities.</p>	<p>Foundational</p>	<p>443318 443335 443738 443741 443961 444164 444165 444166 444167 444224</p>	



## APPENDIX B: PROJECT SUMMARY WORKSHEET

**Purpose:** The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment**.

1. Project Number	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
443318	White Pine County SLCGP FY2022	White Pine County is a rural county, home to less than 10,000 people. This project would provide security for all residents by ensuring 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.	SLCGP Objective / Program Goal # 3  Elements 3, 7, 8, 15, & 16	\$39,740.75 (FFY22 SLCGP)	Not Started	High	Organization Training
443335	Washoe County: Annual Penetration Testing	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.	SLCGP Objective / Program Goal #2  Elements 2, 4, 6, 10, 14, 15, & 16	\$44,000.00 (FFY22 SLCGP)	Not Started	High	Organization
443468	Nevada Cybersecurity for the Judiciary	"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	SLCGP Objective / Program Goal #2  Elements 10, 14, & 15	\$925,000.00 (FFY22 SLCGP)	Not Started	High	Planning Organization

		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.					
443738	Washoe County: Incident Response Plan	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.	SLCGP Objective / Program Goal #1  Elements 2, 3, 6, 10, 14, 15, & 16	\$35,000.00 (FFY22 SLCGP)	Not Started	High	Organization
443741	Washoe County: Cortex XDR Host Insights	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).	SLCGP Objective / Program Goal #3  Elements 1, 2, 4, 10, 13, 15, & 16	\$27,931.00 (FFY22 SLCGP)	Not Started	High	Organization Equipment Training
443961	City of Sparks, Nevada Cybersecurity	Project 1 The intent of the project is to assess all of City of Sparks’ 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-premises domain configuration. We are planning to	SLCGP Objective / Program Goal #2  Elements 2, 3, 4, & 16	\$109,050.00 (FFY22 SLCGP)	Not Started	High	Organization

		<p>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 assess 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.</p> <p>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.</p> <p>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.</p>					
444164	Douglas County: Physical Security - Badge/Card Reader System	<p>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 &amp; 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 Douglas County's environment which will allow us to track who enters each door and when if necessary. This will serve to significantly increase Douglas County's capacity as it pertains to physical security relative to cyber and elections security. Douglas County's 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</p>	<p>SLCGP Objective / Program Goal #3</p> <p>Element 5, 7, 13, 15, &amp; 16</p>	\$101,204.17 (FFY22 SLCGP)	Not Started	High	Equipment

		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 Douglas County's existing hardware can be migrated over into a new system. Some of Douglas County's older hardware needs to be replaced as it is not compatible with a new system. We will need to replace one of Douglas County's 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 Douglas County's badge access system by being able to tell who is access which doors and when.					
444165	Douglas County: Firewall/Network Edge Refresh	Existing firewalls have reached end of life and support will no longer be viable in Douglas County's environment as upgrade paths and features will not be in sync with the rest of Douglas County's firewall environment. This will secure Douglas County's edge and ensure content and feature releases to deal with new and ever-present threats are available to us. The new firewalls will increase Douglas County's resiliency to attacks and help to better monitor network traffic.	SLCGP Objective / Program Goal #3  Elements 1, 2, 9, 10, 13, 15, & 16	\$86,915.00 (FFY22 SLCGP)	Not Started	High	Equipment
444166	Douglas County: Multi-Factor Authentication for End-Users/Endpoints	"This project would implement MFA throughout Douglas County's 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 Douglas County's resilience of user accounts and protects us if a user credentials are compromised, and a computer is lost/stolen. Douglas County's 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 Douglas County's resilience of information systems and user accounts by forcing users to do MFA when logging onto computers. The adding of MFA to end point logins greatly reduces Douglas County's cybersecurity risks and threats.	SLCGP Objective / Program Goal #3  Element 5, 10, 13, 15, & 16	\$4,772.00 (FFY22 SLCGP)	Not Started	High	Equipment
444167	Douglas County: Backup Datacenter Environment	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 Douglas County's 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	SLCGP Objective / Program Goal #3  Element	\$119,292.08 (FFY22 SLCGP)	Not Started	High	Equipment

		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 Douglas County's preparation and shortens Douglas County's response time in case there is a cyber-attack.	3, 7, 15, & 16				
444205	Governor's Office of Cyber Defense: Nevada Shared Cyber Threat Intelligence Platform	<p>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.</p> <p>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.</p> <p>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.</p> <p>We are focusing our Office's 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 Office's 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 Office's products direction.</p>	<p>SLCGP Objective / Program Goal #1</p> <p>Element 1, 2, 3, 4, 5, 9, 10, 11, 14, &amp; 15</p>	\$150,000.00 (FFY22 SLCGP)	Not Started	High	Organization Equipment Training
444224	Pershing County: Multifactor Authentication	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.	<p>SLCGP Objective / Program Goal #3</p> <p>Element</p>	\$28,580.00 (FFY22 SLCGP)	Not Started	High	Planning Organization Equipment

		<p>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 civil service users.</p> <p>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.</p>	<p>5, 10, 13, 15, &amp; 16</p>				
--	--	--	--------------------------------	--	--	--	--

## APPENDIX C: ENTITY METRICS

The below table should reflect the goals and objectives the Cyber Security Task Force establishes.

Nevada's Cybersecurity Plan Metrics			
Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
4. 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.	1.1 Establish a structured outreach program targeting local government IT leaders and emergency managers, fostering communication and collaboration for consequence management and grants coordination.	Actively engage 100% of Nevada's counties	OCDC will initiate and track engagement with the counties throughout the next three years of this strategic plan and report the results of the engagement to the CSTF on an annual basis.
	5. Understand Nevada's current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structure assessments.	1.2 Establish a state-wide cybersecurity capabilities assessment program with actionable results and improvement tracking.	Actively engage 100% of Nevada's counties
	2.1 Enhance information and intelligence sharing between the OCDC and local government IT leaders and emergency managers.	Actively engage Government Cybersecurity Work Group	OCDC will conduct a biennial Government Cybersecurity Work Group meeting and will report the results to the CSTF on an annual basis.

Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
6. Implement security protections commensurate with risk.	3.1 Ensure Multi-Factor Authentication (MFA) enabled where possible for devices with access to Nevada’s sensitive information or critical systems	25% of State and local governments have MFA enabled for Nevada’s information or critical systems	OCDC, through annual cybersecurity capabilities assessment, will identify and track implementation of MFA and report the results to the CSTF on an annual basis



## APPENDIX D: ACRONYMS

Acronym	Definition
CISO	Chief Information Security Officer
COOp	Continuity of Operations Plan
DR	Disaster Recovery
DEM	Division of Emergency Management/Homeland Security
EITS	Enterprise IT Services Division
FFY	Federal Fiscal Year
IR	Incident Response
ISO	Information Security Advisor
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NCHS	Nevada Commission on Homeland Security
DHHS	Nevada Department of Health and Human Services
NRS	Nevada Revised Statute
NOFO	Notice of Funding Opportunity
OCDC	Office of Cyber Defense Coordination
SLCGP	State and Local Cybersecurity Grant Program
SLTT	State, Local, Tribal, and Territorial
TLD	Top Level Domain