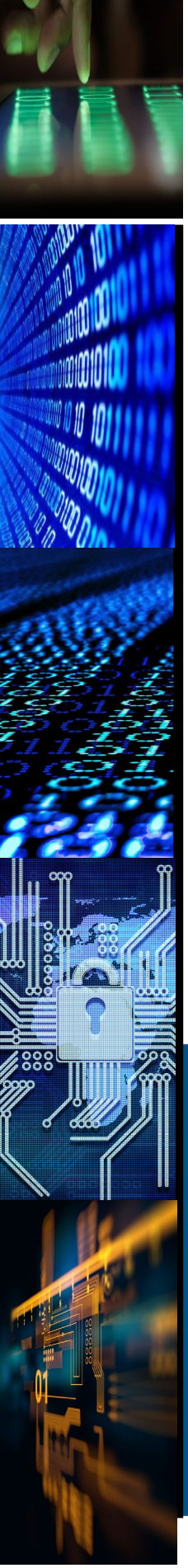
Agenda Item #8



STATE OF NEVADA

CYBERSECURITY PLAN

September 2022

Approved by the NEVADA CYBER SECURITY TASK FORCE on November xx, 2022
Version 1.0

DRAFT – INTERNAL WORKING DOCUMENT

THIS PAGE INTENTIONALLY LEFT BLANK

DRAFT

TABLE OF CONTENTS

DRAFT

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 2022 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, the Office of Cyber Defense Coordination, 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

DRAFT

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 Nevada's cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of 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 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[1], 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.

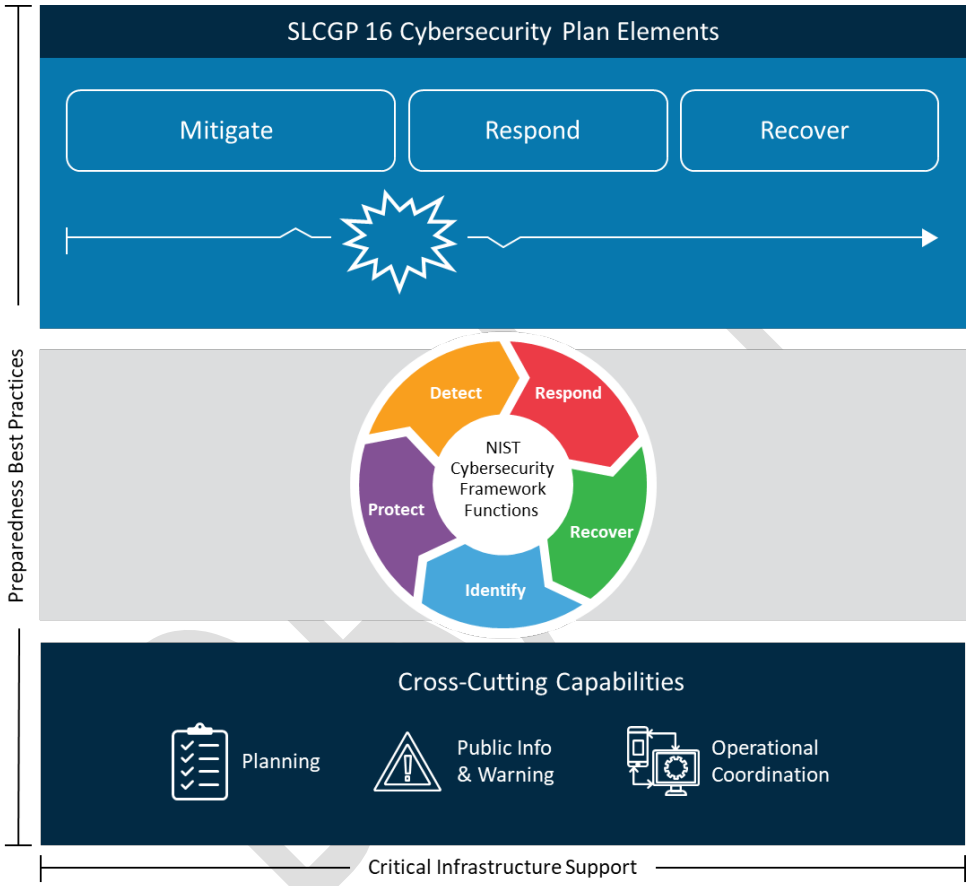


Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

[1] https://www.nist.gov/cyberframework/getting-started

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

Nevada Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. Statewide security information sharing, continuous monitoring, and incident response	1.1 Establish platform, infrastructure and governance for security information sharing between Nevada government entities
	1.2 Establish statewide Cybersecurity Incident Management capabilities to coordinate incidents between government entities
	1.3 Establish coordination process, governance, and parameters for statewide multi-entity incident response
2. Statewide security awareness training	2.1 Establish a statewide security awareness education program
3. Statewide cyber security response exercises	3.1 Establish cadence and parameters for statewide cyber security response exercises
	3.2 Establish process and governance for incorporating lessons learned into future cybersecurity program plans
4. Cybersecurity skills development	4.1 Establish program for cybersecurity skills development for both current and prospective cybersecurity professionals
5. Cybersecurity foundations	5.1 Establish baseline governance and standards for cybersecurity statewide

Commented [A1]: Instead of specifying SOC, how about "Cybersecurity Incident Management capabilities" to leave it more flexible but still indicating our goal?

Commented [A2R1]: Good call

DRAFT

Program Goal	Program Objectives
	5.2 Identify gaps and enable/assist entities in closing them
6. Statewide cybersecurity contracts	6.1 Establish statewide contracts and pricing for cybersecurity tools and services to leverage economies of scale for all entities
	6.2 Establish contract language for procurements statewide ensuring vendors are meeting cybersecurity requirements

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 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 the Office of Cyber Defense Coordination, 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 statewide programs for awareness and training regarding security risk. The Office is tasked with establishing partnerships with local governments in order 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 a widely acknowledged truth that you can’t protect what you don’t know about. An accurate inventory of hardware, software, and data, along with documented processes, work- and dataflows, and regulatory compliance requirements describe the environment to be protected and determines the appropriate defense to be put in place. An accurate inventory can also inform patching and replacement requirements, and incident response activities: knowing what hardware and software is in use, what version is in use, and where it’s being used can save time and effort in responding to widespread threats like the log4j software vulnerability. Inventories are currently performed in many entities throughout the state, but not to a consistent level, and the means to share inventory information are not currently available.

Monitor, Audit, and Track

A key aspect of any far-reaching cyber security program is the ability to identify and track anomalous traffic across the enterprise, correlate this behavior with identified vulnerabilities, and coordinate efforts to contain and mitigate any malicious attacks. Currently, these activities happen independently in most SLTT entities in Nevada; any coordination of findings or correlation of events happens ad hoc. As more malware is used that has the capability of moving sideways through an environment, the ability to track it across multiple entities becomes a vital part of the State’s ability to contain the malware, respond quickly and appropriately to threats, and protect the environment.

Enhance Preparedness

Exercises for Disaster Recovery (DR), Continuity of Operations (COOP), and Incident Response (IR) have taken place at various levels within the state. Nevada has participated in Cyber Storm exercises when they have been available, as well as CISA-led exercises and workshops. These have generally been ad hoc or "as available"; establishing a regular cadence of exercises at all levels of government would enhance DR, COOP and IR plan development and capabilities.

Assessment and Mitigation

Continuous monitoring, assessment, and mitigation of detected threats is performed in various ways by different entities throughout the state. Some of these activities are internal to the entity while others have been outsourced to managed security service providers. There is not currently a centralized state-wide function for collecting and assessing logs or traffic, correlating events across multiple entities, or coordinating mitigation efforts in multiple environments.

Best Practices and Methodologies

Nevada Revised Statute (NRS) 603A states that all government entities in Nevada that meet the definition of "data collector" as defined in NRS "shall, to the extent practicable …, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce." (NRS 603A.210.2, effective January 1, 2021)

All state agencies either have adopted or are in the process of adopting the appropriate standards from CIS or NIST Cyber Security Framework. In these efforts, the information being protected and resources available are dictating the level of protection, detection, response and recovery are being implemented. Additional guidance is being received from applicable Federal regulations and industry best practices.

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/. 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

DRAFT

Safe Online Services

Nevada entities are encouraged to use the .gov Top Level Domain for all online services, and is currently migrating off of other domains. Due to the federated nature of the state, no single body has the authority to mandate moving to that domain.

Nevada is also evaluating joining the StateRAMP program for purchasing cloud services.

Continuity of Operations

Continuity of Operations planning for cyber/IT operations is at different levels throughout the state. Many of the plans currently in place are holdovers from COVID and are focused on the specifics of pandemic operations. A broader effort in developing plans that are more robust, with regular testing, is needed.

Workforce

The ability to attract and retain qualified staff is as much a problem in Nevada as it is anywhere else. According to cyberseek.org, there are currently over 7,000 job openings in Nevada for cybersecurity professionals, with 514 of those in public sector positions. With this kind of competition, it is a far better strategy to focus on retaining existing talent, developing their skills through online or classroom course, on-the-job training, job shadowing, and mentoring. Nevada is also partnering with the Department of Veterans Affairs to assist separating veterans transition to civilian life by providing training, mentoring and government employment opportunities in cybersecurity, as well as other careers.

Beyond technical staff, security awareness training and testing has proven key to reducing entities' vulnerability to social engineering attacks, including phishing, and combined with broad use of MFA, has reduced the number of stolen credentials and ransomware incidents statewide.

Cyber Threat Indicator Information Sharing

All branches of State-level government, all counties, and several cities, school districts and other local entities are current members of MS-ISAC or EI-ISAC. Membership is encouraged at all levels of government. Open discussion and exchange of information is encouraged through committees and groups like the State Information Security Committee or the Southern Nevada Government Cybersecurity Group, and secure online resources like Signal and Discord. By fostering a secure, open and transparent environment, we can increase the communication, cooperation and coordination between entities at all levels of government. Additional tools like Anomali and other threat intel or integrated risk management platforms can be leveraged to facilitate sharing of threat and incident information.

Leverage CISA Services

Nevada currently participates in MS-ISAC's vulnerability scanning and web application scanning programs, as well as their Malicious Domain Blocking and Reporting service. We also have Albert sensors at the borders of the enterprise computing environment, as well as all county election offices. Entities are encouraged to consider MS-ISAC and CISA-provided tools and services when looking at new initiatives and programs.

Information Technology and Operational Technology Modernization Review

It is generally accepted that legacy or unsupported systems present a significant and tangible threat in any environment. Vendor End-Of-Life announcement are tracked, budgets adjusted, and staff notified to replace systems before they go out of support in most entities. However, budget approvals and entity

priorities may be challenges in the replacement and modernization efforts due to limited resources in government.

Cybersecurity Risk and Threat Strategies

The same communication channels and approaches mentioned above under Cyber Threat Indicator Information Sharing can be leveraged to provide communications and coordination on risk and threat strategies. With a federated environment like Nevada, these efforts are built primarily on partnership and trust, rather than discrete technical solutions.

Rural Communities

Rural communities are a particular challenge in Nevada, where counties larger than some states may have a population smaller than many towns. The Governor's Office of Science, Innovation & Technology is currently tasked with improving access to broadband in rural and underserved areas of Nevada, and are open to working with local and state government entities to include access to cybersecurity tools and services.

FUNDING & SERVICES

Our goal with this grant program is to increase the base level of preparedness for the state as a whole, across every entity. We will be systematically moving up the pyramid (pictured below) with each successive round of funding. Since this is the first year, we are focusing on the foundation of identifying what we have and knowing where we are. This will establish a baseline upon which we can perform a gap analysis of our strengths and weaknesses, which will help us identify both areas of greatest need, and resources that may be leveraged for wider impact and effect.

Distribution to Local Governments

In examining the grant guidance and requirements concerning distribution of funds, it becomes clear that the intent of this grant is that it be used to cover an many entities as possible. Parceling funds out to individual entity subgrantees is effective in some cases, but attempting to do this for the full grant amount would dilute the overall effectiveness of the grant program. As the saying goes, a rising tide raises all boats; finding effective and needed programs and services that can be purchased at the statewide level and provided to all entities will have the greatest effect for rural areas, and provide the largest economies of scale to the program and service pricing.

ASSESS CAPABILITIES

As noted previously, Nevada is a highly federated state, and capabilities vary widely between entities. At the county level, for example, we have entities with fully staffed and trained IT and cybersecurity departments, we have entities with one "IT guy" to do everything, and just about every possible situation in between. To date, no statewide assessment of capabilities has been performed, which is why in Year 1 we will be focusing on the foundation of identifying what we have and knowing where we are. This will establish a baseline upon which we can perform a gap analysis of our strengths and weaknesses, which will help us identify both areas of greatest need, and resources that may be leveraged for wider impact and effect.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

Nevada has a federated IT structure, with no central entity that has authority over all levels of government. The Office of Information Security and State Information Security Committee have responsibility for establishing policy and coordinating efforts within the Executive Branch. The Legislative and Judicial Branches have their own security policy and processes, as does the Nevada System of Higher Education. The Office of Cyber Defense Coordination is charged with coordinating efforts with the local government entities, between local and state entities, and between state government and private entities.

Coordination of effort between entities occurs through the establishment and support of the security community which encourages partnership and cooperation. There is a general understanding that we are all stronger if we stand together and support one another.

Appendix B: Project Summary Worksheet provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

METRICS

[describe the metrics the eligible entity will use to measure progress towards

- Implementing the Cybersecurity Plan
- Reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.]

- You may use the following table for reporting metrics. Please note: This table requests **PROGRAM OBJECTIVES NOT THE CYBERSECURITY PLAN OBJECTIVES**

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1. Statewide security information sharing, continuous monitoring, and incident response	1.1 Establish platform, infrastructure and governance for security information sharing between Nevada government entities		
	1.2 Establish statewide Cybersecurity Incident Management capabilities to coordinate incidents between government entities		
	1.3 Establish coordination process, governance, and parameters for statewide multi-entity incident response		
2. Statewide security awareness training	2.1 Establish a statewide security awareness education program		
3. Statewide cyber security response exercises	3.1 Establish cadence and parameters for statewide cyber security response exercises		
	3.2 Establish process and governance for incorporating lessons learned into future cybersecurity program plans		
4. Cybersecurity skills development **5. Cybersecurity foundations**	4.1 Establish program for cybersecurity skills development for both current and prospective cybersecurity professionals		
	5.1 Establish baseline governance and standards for cybersecurity statewide		
	5.2 Identify gaps and enable/assist entities in closing them		

Commented [A3]: Instead of specifying SOC, how about "Cybersecurity Incident Management capabilities" to leave it more flexible but still indicating our goal?

Commented [A4R3]: Good call

DRAFT

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
6. Statewide cybersecurity contracts	6.1 Establish statewide contracts and pricing for cybersecurity tools and services to leverage economies of scale for all entities		

DRAFT

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

[By taking the following actions, an entity will demonstrate that their cybersecurity plan incorporates the required assessment relating to the **Cybersecurity Plan Required Elements.** Ensure that the assessment incorporates an **entity-wide** perspective**.** It also links any line items from the **project summary worksheet** that will help to establish, strengthen, or further develop your cybersecurity capabilities**.**

Eligible entities can use the "EVAL" column as a self-assessment tool. Entities with newly initiated programs could use this spreadsheet to track the status of their cybersecurity planning efforts. Similarly, entities with advanced programs could use this worksheet to evaluate their current cybersecurity plan using "Yes, No, Partial, or N/A."]

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				
2. Monitor, audit, and track network traffic and activity				
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts				
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk				
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)				

a. Implement multi-factor authentication				
b. Implement enhanced logging				
c. Data encryption for data at rest and in transit				
d. End use of unsupported/end of life software and hardware that are accessible from the Internet				
e. Prohibit use of known/fixed/default passwords and credentials				
f. Ensure the ability to reconstitute systems (backups)				
g. Migration to the .gov internet domain				
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain				
7. Ensure continuity of operations including by conducting exercises				
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)				
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks				
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which				

DRAFT

may impact the performance of information systems within the jurisdiction of the eligible entity				
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department				
12. Leverage cybersecurity services offered by the Department				
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives				
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats				
15. Ensure rural communities have adequate access to, and participation in plan activities				
16. Distribute funds, items, services, capabilities, or activities to local governments				

DRAFT

APPENDIX B: PROJECT SUMMARY WORKSHEET

[The project worksheet should mirror all projects applied for in the Individual Justification (IJ) form.]

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**.

[Instructions: Completing the table below, including the following information in each column to expedite review and approval:

- **Column 1**. Project number assigned by the entity
- Column 2. Name the project
- Column 3. Brief (e.g., 1-line) Description of the purpose of the project
- Column 4. The number of the Required Element the project addresses
- Column 5. Estimated project cost
- **Column 6.** Status of project (future, ongoing, complete)
- **Column 7.** Project priority listing (high, medium, low)
- **Column 8.** Project Type (Plan, Organize, Equip, Train, Exercise)]

1.	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type

APPENDIX C: ENTITY METRICS

[Describe the metrics you will use to measure implementation and cybersecurity threat reduction (to be provided in your annual report to CISA), including:

1) progress toward implementing the cybersecurity plan; and
2) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to your information systems.

Consider the following when developing metrics:

- Metrics must be aligned to the Cybersecurity Plan and the established goals and objectives
- Review existing metrics that are already be used across the eligible entity
- The data for each metric must be available and reportable and should not create unnecessary bourdons to collect.

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

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
1. Statewide security information sharing, continuous monitoring, and incident response	1.1 Establish platform, infrastructure and governance for security information sharing between Nevada government entities		
	1.2 Establish statewide Cybersecurity Incident Management capabilities to coordinate incidents between government entities		
	1.3 Establish coordination process, governance, and parameters for statewide multi-entity incident response		
2. Statewide security awareness training	2.1 Establish a statewide security awareness education program		
3. Statewide cyber security response exercises	3.1 Establish cadence and parameters for statewide cyber security response exercises		
	3.2 Establish process and governance for incorporating lessons learned into future cybersecurity program plans		

Commented [A5]: Instead of specifying SOC, how about "Cybersecurity Incident Management capabilities" to leave it more flexible but still indicating our goal?

Commented [A6R5]: Good call

Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
4. Cybersecurity skills development	4.1 Establish program for cybersecurity skills development for both current and prospective cybersecurity professionals		
5. Cybersecurity foundations	5.1 Establish baseline governance and standards for cybersecurity statewide		
	5.2 Identify gaps and enable/assist entities in closing them		
6. Statewide cybersecurity contracts	6.1 Establish statewide contracts and pricing for cybersecurity tools and services to leverage economies of scale for all entities		
	6.2 Establish contract language for procurements statewide ensuring vendors are meeting cybersecurity requirements		

DRAFT

APPENDIX D: ACRONYMS

Acronym	Definition

DRAFT

UPDATE ALL ACRONYMS IN TABLE