STATE OF NEVADA
MEETING NOTICE AND AGENDA
GOVERNOR'S CYBER SECURITY TASK FORCE

Name of Organization:	Governor's Cyber Security Task Force
Date and Time of Meeting:	Friday, December 2, 2022 at 10:00 a.m.
Place of Meeting:	There will be no physical location for this meeting. The meeting can be listened to, or reviewed live, over the Internet through the Nevada Division of Emergency Management YouTube channel at: https://www.youtube.com/channel/UCFGa6exzrZdlgA6PP55kfqg
Conference Line Access:	Conference line #: 1-669-219-2599 Meeting ID# 686 738 8625 When prompted for Participant ID, please press #

This meeting will be video or teleconferenced as specified beginning at 10:00 a.m. The Governor's Cyber Security Task Force (CSTF) may act on items marked "For Possible Action." Items may be taken out of the order presented on the agenda at the discretion of the Chair. Items may be combined for consideration by the CSTF at the discretion of the Chair. Items may be pulled or removed from the agenda at any time.

Please Note: Witnesses wishing to have their complete testimony/handouts included in the permanent record of this meeting should provide a written or electronic copy to the CSTF administrative support staff. Minutes of the meeting are produced in a summary format and are not verbatim.

1. **CALL TO ORDER AND ROLL CALL** –Chair, Tim Robb.

2. **PUBLIC COMMENT**– (Discussion Only) – No action may be taken upon a matter raised under this item of the agenda until the matter itself has been specifically included on an agenda as an item upon which action may be taken. Public comments may be limited to three minutes per person at the discretion of the Chair. Comments will not be restricted based on viewpoint.

   To provide testimony during this period of public comment via telephone, please call in any time after 9:30 a.m. on the day of the meeting by dialing 1-669-219-2599. When prompted to provide the Meeting ID, please enter 686 738 8625 and then press #. When prompted for a Participant ID, please press #. When asked to provide public comment, please press *6 to unmute your phone and *6 again when your comments are complete.

   Please be advised that the YouTube stream will be between 60-90 seconds behind the live meeting. If you would like to present public comment, please call in using the above number to hear the meeting live.

3. **APPROVAL OF MINUTES** – (Discussion/For Possible Action) – Chair, Tim Robb. The CSTF will discuss and review the minutes of the November 7, 2022, the CSTF meeting. The CSTF will determine whether to approve the meeting minutes.

4. **DEVELOPMENT OF A STATEWIDE CYBER SECURITY STRATEGIC PLAN** – (Discussion/For Possible Action) – Chair, Tim Robb. The CSTF was presented with a draft cyber security plan at its last meeting. Members were asked to review, and be prepared to provide feedback, on the draft plan. Additionally, the plan is shared on the CSTF's website and with many partners on various listservs. The CSTF will review the draft plan and provide any potential revisions to ensure it meets everyone's statewide needs. The CSTF may provide input to the proposed plan and may adopt the plan.

5. **DISCUSSION ON THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM ADMINISTERED THROUGH THE DIVISION OF EMERGENCY MANAGEMENT AND HOMELAND SECURITY (DEM/HS)** - (Discussion Only) – David Fogerson, Chief of DEM/HS. The CSTF will be presented on the process used to solicit, vet, and rank projects for recommendations to the State Administrative Agent, the Chief of DEM/HS, for funding through the State and Local Cyber Security Grant Program.

6. **PUBLIC COMMENT** – (Discussion Only) – No action may be taken upon a matter raised under this item of the agenda until the matter itself has been specifically included on an agenda as an item upon which action may be taken. Public comments may be limited to 3 minutes per person at the discretion of the Chair. Comments will not be restricted based on viewpoint.

   To provide testimony during this period of public comment via telephone, please call in any time after 9:30 a.m. on the day of the meeting by dialing 1-669-219-2599. When prompted to provide the Meeting ID, please enter 686 738 8625 and then press #. When prompted for a Participant ID, please press #. When asked to provide public comment, please press *6 to unmute your phone and *6 again when your comments are complete.

   Please be advised that the YouTube stream will be between 60-90 seconds behind the live meeting. If you would like to present public comment, please call in using the above number to hear the meeting live.

7. **ADJOURNMENT** – (Discussion/For Possible Action)

This is a public meeting. In conformance with the Nevada Public Meeting Law, this agenda was posted or caused to be posted on or before 9:00 a.m. on November 29, 2022, at the following:

Nevada State Emergency Operations Center, 2478 Fairview Drive, Carson City, NV and

Posted to the following websites:

- Nevada Division of Emergency Management and Homeland Security Public Meeting Notifications/Information Website:

  https://dem.nv.gov/DEM/DEM_Public_Meeting_Information/

- Nevada Public Notice Website: www.notice.nv.gov

  To navigate to Division of Emergency Management and Homeland Security administered meetings, please do the following:

  - Within the Government Column, click **State.**
  - Within the Entity Column, click **Office of the Military – Division of Emergency Management.**
  - Within the Public Body column, click on the **Governor's Cyber Security Task Force**; results will populate on the page.

We are pleased to make reasonable accommodations for members of the public who are disabled. If special arrangements for the meeting are necessary, or if there is a need to obtain copies of any supporting meeting materials, please notify Sherrean K. Whipple, Division of Emergency Management and Homeland Security, at 1-775-687-0300. 24-hour advance notice is requested. Thank you.

Agenda Item #3
DRAFT MINUTES FOR REVIEW – DO NOT DISTRIBUTE

Meeting Minutes
Governor's Cyber Security Task Force

Attendance	**DATE:** November 7, 2022
	TIME: 10:00 AM
	METHOD: Zoom
	RECORDER: Sherrean Whipple

Member Name	Present	Member Name	Present
Tim Robb – Chair Office of the Governor – Director of Strategic Initiatives	X	Tim Horgan Chief IT Manager - Representative from the Secretary of State's Office	X
Bob Dehnhardt – Vice Chair Chief Information Security Officer of the State of Nevada	X	Aakin Patel Division Administrator - Office of Cyber Defense	X
Paul Embley Representative from the Judicial Branch	X	General Michael Peyerl Nevada National Guard - Office of the Military	X
David Fogerson Chief - Division of Emergency Management/Homeland Security (DEM/HS)	X	Sandie Ruybalid Chief IT Manager - Nevada Department of Health and Human Services (DHHS)	X
Sanford Graves IT Professional I - Representative from the Legislative Branch	X	James Wood Technology Project Coordinator - Washoe County Technology Services	X

Representative		
Samantha Ladich – Senior Deputy Attorney General	Office of the Nevada Attorney General	X
Sherrean K. Whipple – Administrative Assistant	Nevada Division of Emergency Management	X

1. Call to Order and Roll Call

Chair Tim Robb, Office of the Governor, Director of Strategic Initiatives, called the meeting to order. Roll call was performed by Sherrean Whipple. Quorum was established for the meeting.

2. Public Comment

Chair Tim Robb opened the first period of public comment for discussion.

There was no public comment.

3. Welcome and Introduction of Members

Chair Tim Robb asked each member of the task force for a quick introduction including the seat in which they are sitting and the organization for whom they work. Chair Tim Robb introduced himself, indicated that he works in the governor's office, and that he will serve as the chair of the Cyber Security Task Force.

Paul Embley, Nevada Supreme Court, introduced himself.

Dave Fogerson, Division of Emergency Management/Homeland Security, introduced himself.

Sanford Graves, ISO for the Legislature representing the LCB, introduced himself.

Tim Horgan, Chief IT Manager at the Secretary of State's Office, introduced himself.

Aakin Patel, Office of Cyber Defense Coordination (OCDC) Administrator, introduced himself.

General Mike Peyerl, Nevada National Guard and Director of the Joint Staff, introduced himself.

Sandie Ruybalid, Deputy Administrator and Chief IT Manager for Department of Health and Human Services (DHHS), introduced herself.

James Wood, Washoe County, introduced himself.

Bob Dehnhardt, State Chief Information Security Officer for the Department of Administration, introduced himself, indicating that he represents the Executive Branch.

4. Introduction to the Open Meeting Law

Samantha Ladich, Nevada Attorney General's Office, introduced herself and explained that her role at the task force meetings is to advice the Task Force on Nevada Open Meeting Law (OML). Ms. Ladich indicated that OML can be found in Chapter 341 of the Nevada Revised Statutes (NRS) and that the intent of the law is to ensure that public bodies conduct their business openly in the public view. Ms. Ladich further indicated that this business includes deliberations and any voting undertaken by the Task Force. Ms. Ladich explained that the Attorney General's Office promotes openness and transparency in government and assists public bodies in compliance with OML.

Samantha Ladich went through the components of OML with the Task Force, indicating that the first component is to ensure public notice, which refers to the need to post the agenda to public websites and at certain locations by 9:00 a.m. three business days in advance of a meeting. Ms. Ladich informed the Task Force that if the agenda is not posted by that time, cancellation of the meeting is required. Ms. Ladich further indicated that once the agenda has been posted, no items on that agenda can be changed, nor can new items be added. Ms. Ladich informed the Task Force that quorum must be met in order for the Task Force to act upon action items in a meeting. Ms. Ladich next discussed the requirement of multiple periods of public comment per NRS Chapter 241. Ms. Ladich further indicated that part of her job is to ensure that the Task Force sticks to the agenda during the meeting. Ms. Ladich explained that the Chair will take on a large role in ensuring that the discussions remain on track, as well, and reminded the Task Force that nothing can be discussed or voted upon that has not been agendized. Ms. Ladich indicated that voting as a Task Force must be done publicly and verbally. Ms. Ladich next discussed the importance of meeting accessibility and ensuring that there is adequate room for the public if in a physical location, and that the phone number and YouTube link provided are working for a virtual meeting. Ms. Ladich noted that if these criteria are not met, the meeting must be cancelled. Ms. Ladich concluded her discussion of OML by stressing the importance of members identifying themselves when speaking in order to ensure accurate minutes of the meeting.

5. Review and Approval of the Cyber Security Task Force's Charter

Chair Tim Robb discussed the background of the Cyber Security Task Force and the need for its establishment. Chair Robb indicated that the Task Force was established through an executive order and is thus eligible for Federal monies coming through the Infrastructure Investment and Jobs Act, which is what served as the foundation of the Task Force. Chair Robb explained that the goal of the Task Force is to include voices from cities, counties, and other state agencies in working through cybersecurity posture, and that the Task Force will serve as a piece of the public process in how cybersecurity will be addressed moving forward. Chair Robb reiterated that the Task Force is subject to OML.

Chair Tim Robb explained that the Cyber Security Task Force will bring a lot of the discussions about the IIJA funding and noted that the Task Force members are also included in the charter. Chair Robb explained that these are exactly from the executive order. Chair Robb indicated that he has been appointed Chairperson as he is the Governor's appointee to the Task Force. Chair Robb further indicated that the Chief of DEM/HS will act as the state's administrative agent and will be working directly with the Federal partners to ensure compliance with all of the grant requirements. Chair Robb indicated that the Task Force will be discussing the frequency of meetings needed in order to ensure priorities are being upheld and reporting is where it needs to be. Chair Robb next discussed the duties of the Task Force, which are based on the executive order and outlined in the charter. Chair Robb reiterated the importance of the Task Force holding open, collaborative conversations with the right voices at the table, as well as considering all of the aspects of cybersecurity preparedness, the ability to strategize when an active response is needed and ensuring that all resources are in place.

Paul Embley asked if an alternate or designated representative can be sent in the event of a meeting conflict.

Samantha Ladich indicated that proxies are no longer legally allowed under OML, so although this alternate representative cannot legally vote or count towards quorum, they can attend, listen, and take notes for the absent member.

Randy Robinson, City of Las Vegas, indicated that he was a member of the former State Cyber Security Task Force when employed in the private sector, and had done a lot of work on the issue statewide. Mr. Robison indicated his belief that the membership is one perspective short in terms of representation from the city level of local government. Mr. Robison noted that the city and county have different areas of responsibility and as such, this sometimes creates different perspectives not only in the services provided, but also in the risks that are encountered and mitigated. For all of these reasons, Mr. Robison recommended the inclusion of city representatives on the Task Force.

Bob Dehnhardt indicated his willingness to be included in Item F regarding receiving advice and recommendations for legislative action in the case that any is needed towards NRS 242.

Chair Tim Robb noted his desire to change the Co-Chair to Vice Chair.

Chair Tim Robb called for a motion to approve the charter. A motion to approve the charter was presented by Bob Dehnhardt, Chief Information Security Officer of the State of Nevada, and a second was provided by Sandie Ruybalid, Chief IT Manager, DHHS. All were in favor with no opposition. Motion carries.

6. Nomination and Selection of the Vice-Chair

Chair Tim Robb indicated that the Cyber Security Task Force needs to select a vice chair to preside over meetings in the absence of the Chair.

Chair Tim Robb called for a nomination for Vice Chair. David Fogerson nominated Chief Information Security Officer Bob Dehnhardt, and a second was provided by Sandie Ruybalid, Chief IT Manager DHHS. All were in favor with no opposition. Motion carries.

7. Discussion on the State and Local Cyber Security Grant Program Administered Through the Division of Emergency Management/Homeland Security (DEM/HS)

Jared Franco, DEM/HS, discussed the main points pertaining to the financial and administrative policies for the State and Local Cyber Security Grant Program. Mr. Franco explained that under the Infrastructure Investment and Job Act, $200 million has been obligated for FFY22, of which $185 million will be dispersed among the 56 states and territories specifically for the State and Local Cyber Security Grant Program with a cost share of 90 percent Federal and 10 percent local. Mr. Franco reported that the totality of the State and Local Cyber Security Grant Program is currently scheduled to end after the release and performance period of FFY25, and provided the yearly breakdown of funding, noting that the grant is designed to be scaled down towards the end of the grant cycle: FY22, 200 million; FY23, 400 million; FY24, 300 million; and FY25, 100 million. As such, Mr. Franco discussed the necessity of ensuring the existence of a plan for outside funding should the grant program be continued as the future of this is currently unknown. Mr. Franco noted that DEM/HS, as a state administrative agent, is still developing the grant program, and once the State Cyber Security Plan is finalized and all committee seats are filled, DEM/HS staff will then create the application for projects, at which time acceptance of applications for consideration of grant funding can begin. Mr. Franco further noted that the timetable of this is unknown, but DEM/HS's target date is before the start of FY23.

8. Development of a Statewide Cyber Security Strategic Plan

Chair Tim Robb explained that this plan was drafted between the Office of Cyber Defense and Coordination and the State Chief Information Security Officer.

Aakin Patel, Division Administrator, Office of Cyber Defense, explained that the philosophy with this plan is to start out with fundamentals and to work up from there. Mr. Patel noted that a diagram of the structure for cybersecurity foundations has been included, and within the diagram is a pyramid that shows the basics of what needs to happen in order to achieve a mature cybersecurity program. Mr. Patel further noted that the focus is to look at the fundamentals and look at what exists across every entity to determine where fundamentals are missing, and from there, bring each entity up to a solid foundational level to allow for the higher levels of cybersecurity functionality to function effectively.

Bob Dehnhardt, Chief Information Security Office, explained that the purpose of the plan is to look at cybersecurity at a statewide level which, to this date, has not yet been done. Mr. Dehnhardt indicated that when starting the process of looking at the requirements and the questions being asked, more unknowns than knowns were made apparent simply because of the federated nature of the state. As such, Mr. Dehnhardt noted that the plan was then written from the perspective of not having answers to the questions on a statewide level in hopes of getting an understanding of the various levels at different places in the state, the strengths and the resources available that might be leveraged statewide, as well as the common needs that may need to be purchased or contracted at a statewide level. Mr. Dehnhardt indicated the plan to exercise the economies of scale and get the best pricing in order to provide across the board, and then to identify the entities with special needs that do not necessarily translate statewide.

Chair Tim Robb opened the floor for discussion from the members of the Task Force.

David Fogerson added that the plan becomes very important because all grant funding and any projects that a city, county, or the state wants to do must fit within the cybersecurity plan developed. As such, part of the process includes ensuring that the plan is ironclad for the first year, a plan that will then be sent out to individuals wishing to submit a project for funding by the grant process in order for the individuals to be able to tie that project back into the plan.

James Wood further added that from a county perspective, the plan appears to be geared more toward the state as a whole and expressed his desire to see some verbiage changed in order to better adapt to a county's needs as well as a city's needs and requested that some more effort be included into the representation of non-state agencies.

9. Steps Moving Forward

Chair Tim Robb indicated that the discussion would include next steps for cybersecurity, including discussion of state agency roles and responsibilities. Chair Robb noted that this agenda item includes discussion from the Task Force regarding how often they wish to meet, topics of discussion, and the goals of the Task Force.

Cary Underwood, Southern Nevada Counterterrorism Center, noted his belief that different parts of the state will provide different responses as how a city is affected may be significantly different than how a rural county is affected and as such, indicated the importance of the Task Force being very flexible in working with the different dynamics.

Chair Tim Robb noted that this also addresses the Federal requirements within the grant regarding meeting the needs of many diverse types of cybersecurity environments across the state. The Chair asked if there are any considerations on timing of which the Task Force should be aware.

David Fogerson suggested that the Task Force meet again in the next few weeks in the hopes of getting the Cyber Security Plan adopted and then to subsequently release the grant application to provide applicants time to prepare for project building within that plan.

Aakin Patel concurred that every two weeks would be a good timeframe for the Task Force to meet until a permanent plan is developed.

10. Public Comment

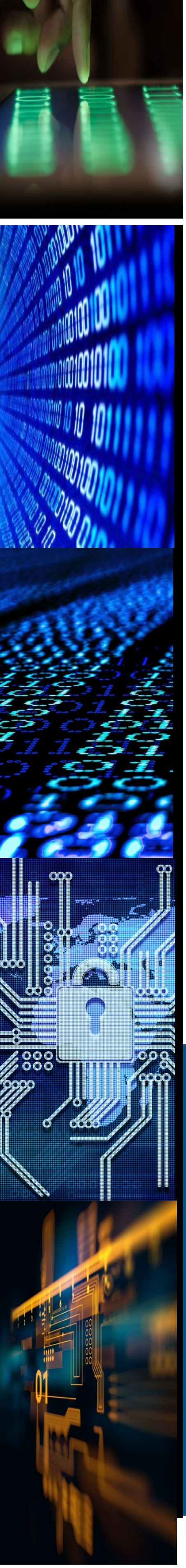
Chair Tim Robb opened the second period of public comment for discussion.

David Fogerson informed the Task Force that DEM/HS will be sending out the Homeland Security Lister to ensure that everyone has a chance to look at potentially hosting FEMA-funded cybersecurity training.

11. Adjournment

Chair Tim Robb called for a motion to adjourn. A motion to adjourn was presented by David Fogerson, Chief of DEM/HS, and second was provided by James Wood, Technology Project Coordinator for Washoe County Technology Service. All were in favor with no opposition. Meeting adjourned.

Agenda Item #4



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

TABLE OF CONTENTS

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

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.

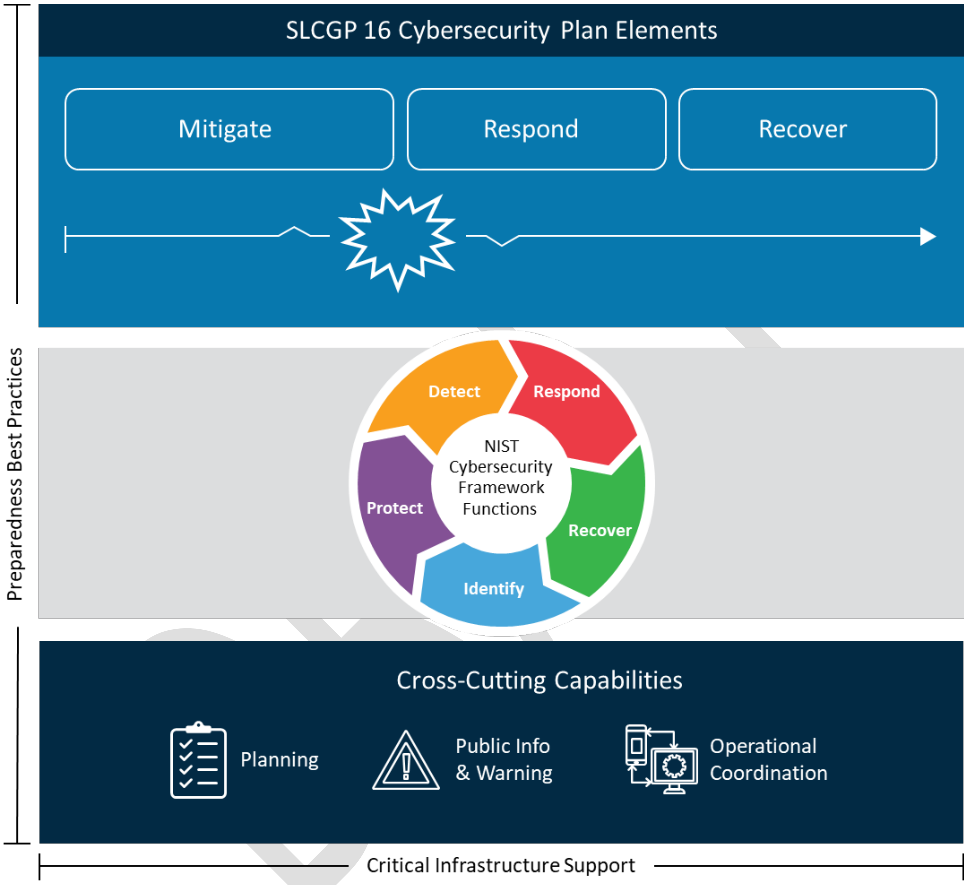

SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

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

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

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

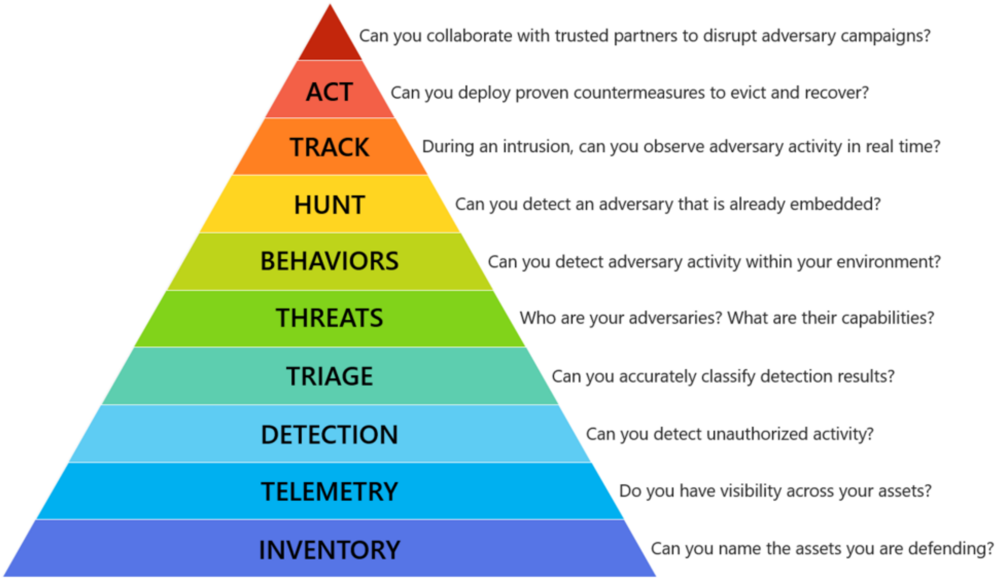
The same communication channels and approaches mentioned above under Cyber Threat Indicator Information Sharing can be leveraged to provide communications and coordination on risk and threat strategies. With a federated environment like Nevada, these efforts are built primarily on partnership and trust,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


Can you collaborate with trusted partners to disrupt adversary campaigns?
ACT
Can you deploy proven countermeasures to evict and recover?
TRACK
During an intrusion, can you observe adversary activity in real time?
HUNT
Can you detect an adversary that is already embedded?
BEHAVIORS
Can you detect adversary activity within your environment?
THREATS
Who are your adversaries? What are their capabilities?
TRIAGE
Can you accurately classify detection results?
DETECTION
Can you detect unauthorized activity?
TELEMETRY
Do you have visibility across your assets?
INVENTORY
Can you name the assets you are defending?

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

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		

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				🟥

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				🟥

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		

APPENDIX D: ACRONYMS

Acronym	Definition

UPDATE ALL ACRONYMS IN TABLE

Agenda Item #5

Nevada Division of Emergency Management / Homeland Security

Prevent • Protect • Mitigate • Respond • Recover

State and Local Cybersecurity Grant Program FFY 2022

Nevada's amount:	$2,488,375
Cost Share:	90% Federal, 10% local
Must Be Used By:	August 31, 2025
State Administrative Agent:	Division of Emergency Management and Homeland Security
Management Costs:	5% of the $2.4 million

Grant 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.
2. Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
3. Implement security protections commensurate with risk.
4. Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Grant Priorities:

1. Establish a Cybersecurity Planning Committee.
2. Develop a state-wide Cybersecurity Plan.
3. Conduct assessment and evaluations as the basis for individual projects throughout the life of the program.
4. Adopt key cybersecurity best practices.

Requirements on Spending:

1. State is the eligible applicant
2. State can subgrant to government entities
3. State must have an approved cybersecurity plan from a cybersecurity task force
4. Projects must align to the priorities within cybersecurity plan
5. Projects must be self-sustaining after grant period
6. State cannot add any additional requirements on use of funds that are not listed in Notice of Funding Opportunity
7. 80% must pass through to local governments or be spent by the state on local governments with their consent

Process to Apply:

1. State will announce application period once cybersecurity plan is developed
2. State entities and local governments will prepare a grant application in Zoom Grants with Division of Emergency Management and Homeland Security
3. Staff will review applications against Notice of Funding Opportunity
4. Projects will be taken to the Governor’s Cybersecurity Task Force for ranking
5. State Administrative Agent will determine final selection and submit projects through the federal grant portal
6. Successful applicants will attend a virtual grant training to ensure understanding of requirements
7. Quarterly reporting is required
8. Annual review of performance measures is required
    a. Implementing the Cybersecurity Plan.
    b. 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.

See the full Federal Notice of Funding Opportunity for further details at https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local