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 241 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.