Meeting Minutes
Governor's Cyber Security Task Force

Attendance	DATE: January 9, 2023
	TIME: 1:00 PM
	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	
Representative			
Samantha Ladich – Senior Deputy Attorney General			
Sherrean Whipple – Administrative Assistant			

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.

David Fogerson, Chief of Nevada Division of Emergency Management/Homeland Security (DEM/HS), just heard back from the Department of Homeland Security (DHS) on the Cyber Security State Local Tribal Territorial Grant process. The grant, though accepted, is on hold as they review the draft and some other technical details that we are working with them. Critical Infrastructure and Cyber Security Administration (CISA) and DHS should get back to DEM/HS in about a month for the approval.

There were no other additional public comment.

3. Approval of December 2, 2022 CSTF Meeting Minutes

Chair Tim Robb called for a motion to amend or approve the draft minutes of the December 2, 2022, Cyber Security Task Force meeting.

Tim Horgan, Chief IT Manager at the Secretary of the State's Office, motioned to approve the minutes.

David Fogerson, Chief of Nevada Division of Emergency Management, seconded the motion to approve the minutes.

All others were in favor with no opposition. Motion passed.

4. Reactive and Preventative Postures for Cyber Security within Nevada

David Fogerson, DEM/HS, advised that the CSTF was created to unify the different cyber security components throughout the state, local, and private sectors, which is required for the grant. Mr. Fogerson explained the cyber security plan has two sides, the prevention side and the reaction side. The prevention side is all the cyber security professionals include Enterprise Information Technology Services (EITS) - Chief Information Security Officer (CISO) at the local government, Office of Cyber Defense and Coordination (OCDC), the Fusions Centers, CISA, DEM/HS grants, and all the local and state information security officers in each of the departments, who work everyday to make sure that our computer systems and cyber programs are safe. The CSTF acts as the balance beam between the Prevent and React postures. The Reaction side is the consequence management, something bad has occurred and we need to be able to fix. Mr. Fogerson gave the example of if someone took control of all the traffic lights and made them green in the state of Nevada. The Cyber specialist would work on that, but then law enforcement would need to be deployed to work on traffic control, the Department of Transportation would be deployed to help with road signs, along with Public Works to support the local hospitals because of the multiple traffic accidents that will occur, working on all those other conflicts management pieces, to work together. The Reaction side is composed of DEM/HS, which has a Policy Group, and they report to the Governor. The Policy Group is composed of those Directors of the agencies that are activated. The Reaction side continues with the Operations Center, and Emergency Support Functions (ESF), such as Communications, Cross Sector Business and Infrastructure, the Nevada National Guard, Cyber Security, and the Local Emergency Operation Centers. Mr. Fogerson saw this in another plan and felt this keeps groups in their proper lanes and that this allows it to be a collaborative and cooperative process, because we are all in this together.

Billy Samuels, Deputy Fire Chief Clark County Fire Department, asked what ESF Cyber Security will be in. David Fogerson advised that at the state level, it will be in ESF17.

5. Office of Cyber Defense and Coordination (OCDC)

Aakin Patel, Administrator of OCDC, described the OCDC for the task force, indicating that the official mission is to serve as the focal point for cyber security strategy, policy planning, and coordination for the entities that exist within the state of Nevada. Mr. Patel explained that the scope is very broad, based on the statutes, but differs from all other entities in that it is not a group with an operational cyber security responsibility for any one specific entity's cyber security plan. Rather, Mr. Patel indicated, the OCDC is focused on coordinating cyber security in a way that every entity can take advantage of. Mr. Patel described the projects that currently exist

within the office such as: a biweekly cybersecurity threat briefing; focusing the intelligence on items that are relevant to the entities in Nevada, including state-specific threats and threats for technologies and items used within the state; continued work on the incident response plan repository as mandated by NRS 480.935; working with the Governor's Office and the National Guard on incident response coordination. Mr. Patel further indicated that the OCDC has future plans on how to improve what it can be doing to help other groups as well as a plan to start up programs and services based on budget and staffing. Mr. Patel noted that there are not yet any specifics to report as no program has yet been approved or started. Mr. Patel encouraged the members of the task force to contact him directly with any ideas or ways that can help as the programs are being built.

6. Critical Infrastructure and Cyber Security Administration (CISA) State Cyber Security Advisor

Dr. Rick Hays, Cybersecurity State Coordinator, indicated that he is the Region IX Coordinator, which includes Nevada, California, Arizona, Hawaii, Guam, and American Samoa, and that his role is the cybersecurity coordinator and acting CSA to support the state of Nevada, a role which he began in August of 2021. Dr. Hays explained that he is assisting with the development of the ESF 17 program, particularly as it faces cyber risk management and incident response for cyber. Dr. Hays next indicated that his primary focus for 2023 will be on assessments, using the five stages of the mid-cybersecurity (phonetic) framework used to understand the identify-and-protect portion in the assessment. Dr. Hays explained that this will enable continuance with the detect, respond, and recover phases of incident response. Dr. Hays relayed his plan to continue with the Incident Response Plan development with all of the government and critical infrastructure across the state to ensure that a plan exists and if not, to help develop one. Dr. Hays next discussed his focus on assisting with the adherence to NRS 603(a), specifically the 210 portion, which deals with security measures and the importance of looking at how those security controls are being managed via CIS or NIST RMF and helping them to understand the big picture as they work through their processes for that. Dr. Hays indicated that he is uncertain whether or not there is a consolidated base where all the information is being reported but further indicated his belief that if not, this consolidated repository will come to fruition within the next year. Dr. Hays next discussed tabletop exercises, noting that the Protecting Critical Infrastructure Information (PCII) requirements go on these assessments and as such, the information is not shared outside of the organization being assessed.

7. Nevada Enterprise Information Technology, Chief Information Security Officer (CISO)

Robert Dehnhardt, State CISO, indicated that the Office of Information Security is responsible for coordination of governance and processes for security within the executive branch and has a fairly tightly defined scope of responsibility and area where it can be active. Mr. Dehnhardt noted that the office does try to work beyond that scope as much as legally possible with the focus that security is a team sport and more players provide strength. Mr. Dehnhardt indicated that while the office has this responsibility as a standard in government, it actually has nearly no authority and is not able to compel anyone to do anything or to issues orders and instead works through cooperation. Mr. Dehnhardt explained that the mission is centered on collaboration and partnerships with the other executive branch agencies, but noted that the office also has an operational element in that it provides some enterprise-level tools and services to the other executive branch agencies wherever it makes sense to leverage the economies of scale and get the best tools possible within the provided budget. Mr. Dehnhardt described the values, noting that everything begins with integrity as relationships are built on trust, honesty, and accountability. Mr. Dehnhardt further indicated the importance of continually looking at the tools to see where they can be upgraded or what new functions or features might

be needed, given that everything is subject to change at a moment's notice. Mr. Dehnhardt added that it is important to work beyond silos, understand everyone's goals, and work together to push things forward. Mr. Dehnhardt next listed some of the responsibilities of the Office of Information Security, including: provide management of the state security program policy standards and procedures for the executive branch; publish this information on a public website in the interest of transparency; providing an integrated risk management platform that will have a number of functions all working together, chief of which are incident response, coordination, and threat intelligence. Mr. Dehnhardt indicated that the office provides security awareness training and assistance in continuity of operations and planning, as well as doing vulnerability scanning and penetration testing on various assets within the state. Mr. Dehnhardt further indicated that the office manages the physical security access card system (NCAS) and establishes and maintains the vision and strategy for the statewide security program. Mr. Dehnhardt discussed the importance of chairing the State Information Security Committee, which was established in 2001 and consists of information security officers from every executive branch agency. Mr. Dehnhardt explained that this committee establishes the security policy and standards for the state, which is an ongoing process. Mr. Dehnhardt further indicated that although the committee originally began with the executive branch, recently invitations have been extended to members of the legislative and judicial branches, the National Guard, and NSHE.

8. Nevada Office of the Military, Nevada National Guard Cyber Security Joint Task Force

General Michael Peyerl, Director of the Joint Staff for the Nevada National Guard, discussed the design of the joint task force team and how it will support partners and governors, noting that this provides additional capacity and capability for the state in response to emergencies. General Peyerl further indicated that the Joint Task Force embeds and works with and for incident commanders. General Peyerl discussed the hazards response playbook, noting that in the last year it was discovered that there was not a team that would be responsive to a cyber emergency or incident, thus the creation of the JTF Cyber, whose main goal is to provide additional capability capacity when communities need it. General Peyerl next described the two primary actors: nation state actors and transnational cyber criminals, noting that the most likely course an organized criminal actor would take is via ransomware and other techniques, with the most dangerous course of action potentially being nation state actors targeting critical infrastructure. General Peyerl explained the building out of the team by overlaying the cyber kill chain from a threat-based aspect with the NIS framework. General Peyerl indicated that requests will come through emergency managers to DEM and then will be vetted by the JTF. General Peyerl discussed the two case studies used in the building of the JTF, one from Texas an one from Louisiana, noting that there were two findings: the necessity of assessments in locating threat actors within the network; following the shutdown of networks by cyber criminals, the National Guard was limited in its ability to then defend those networks as they had already been compromised. As a result, the two states studied had rebuilt their networks, which General Peyerl indicated Nevada now has the capacity to do. General Peyerl reiterated that the purpose of the JTF Cyber task force is to provide additional support and an all-hazardous response in partnership with all of the agencies that it supports with an end goal of decreasing the attack surface for all of Nevada. General Peyerl next discussed the approach being taken and the lines of effort, including: the Air and Army National Guards providing members to the JTF for a specialized team who are organized to be able to assess and respond; the defense team, which will be built out over the next two years and will report directly to him; and coordination of effort through the office of the military, through DEM, and through all partners to ensure trust and transparency across all agencies. General Peyerl discussed upcoming cyber defense training called Cyber Shield, the intent of which is to build out experts that can be integrated into assessment or response/recovery missions. General Peyerl next discussed new initiatives, citing the use by other states of a state active duty full-time force that augments the cyber team. General Peyerl indicated that the JTF is

requesting four positions to help lay the framework and build a better partnership. General Peyerl concluded his presentation by explaining how the JTF cyber team integrates across the state through the Department of Emergency Management, with the Office of Military under General Barry, across all the different agencies to support them, integrate, and work together as partners so as to build capacity and capability to reduce the attack surface as well as to address any cyber emergencies with minimal damage to lives and infrastructure. General Barry indicated that the partnership with OCDC, AKIM, and CISA has already started and the first cyber warrior has already been certified with the intent of certifying more members of the team.

9. Nevada Division of Emergency Management and Homeland Security (DEM/HS)

Jon Bakkedahl, DEM/HS, provided a quick breakdown on consequence management versus crisis management so as to clarify DEM's role. Mr. Bakkedahl indicate that DEM utilizes a particular diagram called Lifelines, which is used for situation awareness in order to help identify which particular sector may be impacted. Mr. Bakkedahl explained that the cyber experts are those that would be dealing with the technical aspects with whomever is impacted in order to assist in dealing with the actual cyber threat and that DEM would be focused on the consequences. Mr. Bakkedahl reiterated the idea that cyber touches a multitude of the Emergency Support Functions (ESFs). Mr. Bakkedahl explained that in the case of an incident DEM would try to coordinate efforts across all the jurisdictions, as well as with state partners with the hopes of reducing impacts further down the line. Mr. Bakkedahl indicated that DEM's responsibility is to help plan for and use preparedness efforts to respond to incidents, help support the different groups recover from the incidents, with the hope of mitigating those events from occurring again. Mr. Bakkedahl pointed the group to the attached document, noting that all 17 ESFs are spelled out with the different approaches taken by emergency management.

10. Public Comment

Chair Tim Robb called for any public comment.

There was no public comment.

11. Adjournment

Chair Tim Robb called for a motion to adjourn. A motion to adjourn was presented, and second was provided by Frank Abella. All were in favor with no opposition. Meeting adjourned.