Meeting Minutes
Nevada Commission on Homeland Security

Attendance	**DATE**	Friday, February 6, 2026
	TIME	2:00 PM
	METHOD	Zoom/Teleconference Conference line #: (669) 219-2599 Meeting ID# 202 331 8963
	RECORDER	Loren Borst

Appointed Voting Member Attendance					
Member Name	**Present**	**Member Name**	**Present**	**Member Name**	**Present**
Governor Joe Lombardo - Chair	ABS	Chief Fernando Grey	X	George Togliatti	ABS
Sheriff Kevin McMahill – Vice-Chair	X	Dr. Ikram Khan	ABS	James Chrisley	ABS
Sheriff Darin Balaam	ABS	Rick Edwards	X	Patricia Wade	X
Col. Kyle Cerfoglio	X	Richard Perkins	X	Bill Welch	X
Todd Fasulo	X	Harriett Vegas	X		
Mitchell Fox	X	Billy Samuels	X		
Appointed Non-Voting Member Attendance					
Karen Burke	X	Christopher Ipsen	ABS	Adam Miller	ABS
Christopher Delzotto	X	Brett Compston	X	Mike Matthews	ABS
Skip Daly	X	P.K. O'Neill	ABS		
Legal and Support Staff Attendance					
Samantha Ladich	X	Loren Borst	X		

1. CALL TO ORDER AND ROLL CALL

Vice-Chair Sheriff Kevin McMahill, Las Vegas Metropolitan Police Department (LVMPD) called the meeting to order. Roll call was performed by Loren Borst, Nevada Office of Emergency Management and Homeland Security (OEM/HS). Quorum was established for the meeting.

2. PUBLIC COMMENT

There was no public comment.

3. APPROVAL OF MINUTES

Mitch Fox, Nevada Broadcasters Association, motioned to approve the December 9, 2025, commission meeting minutes. Patty Wade, Wade Development, seconded.

No discussion was presented. There was no opposition, passed unanimously.

4. STATEWIDE NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS) COMPLIANCE REPORT

Brett Compston, OEM/HS, reported on courses for the latest quarter. He indicated there were 3,323 people trained, which was a significant reduction from historical, quarterly participation. This was predominately due to the federal government shutdown during the first quarter of federal FY ’26, which was approximately six weeks. During this period, no courses were run, including online courses.

There were no questions or comments from members.

5. LESSONS LEARNED FROM CYBERSECURITY INCIDENT

Tim Galluzi, Governor’s Technology Office, Chief Information Officer (CIO), shared lessons learned from the August 2025 ransomware cyberattack. He indicated to board members that there is a large, after-action report in their meeting packet if more detail was desired, and that he would just be providing a brief, overall, after-action on the incident and then focus on what is being done, beyond the event and focusing on what has been learned.

He then provided a bit of background on the incident, stating the initial compromise happened mid-May 2025, when a state employee downloaded a compromised tool that looked legitimate, hosted on a SEO-poisoned website. The payload then sat on the employee’s device for some time, recording keystrokes, credentials, and other critical information. Mr. Galluzzi stated this was an incredibly mature and complex attack, by a very sophisticated threat actor/threat actor group, one of the top, worldwide.

The payload sat on the device for over 100 days, from May 2025 to August 24, 2025, before it was finally launched in their main effort, when backup information was deleted and their encryption was launched onto the State of Nevada’s main virtual machine environment. When the encryption was launched, it triggered the State of Nevada Governor’s Technology Office (GTO), to begin trouble shooting, as the act initially appeared as a loss of network connectivity.

During that troubleshooting activity, it was found that the GTO could not see the machines within that environment. As the troubleshooting activity continued, the reason for the lack of visibility was discovered and the GTO immediately began isolating the environment and launching immediate action, as they had planned and practiced for in response to a cyber incident. Mr. Galluzzi believes that this immediate action is what kept this incident, despite the size that it was, isolated to where it was launched, which was just one, virtual machine environment.

Mr. Galluzzi did indicate that while it was a large environment impacted, typically, ransomware-type attacks like to spread out to endpoints and don’t typically stop in one space, moving laterally, effectively to anywhere they touch. Because the GTO team was able to see

exactly what it was, as quickly as they did, they were able to effectively drop the network down very quickly. They then notified the Governor's office, securing their help in prioritizing recovery steps. Mr. Galluzzi believes that immediate step helped begin recovery operations as quickly as possible. He stated this environment was only down for about a day and a half, as downtime is measured, as that was how long all network connectivity was effectively cut off.

Once the GTO team was able to rebuild network components outside of the quarantine environment, they started building up network connectivity, which was the official kickoff of the recovery process, which lasted about 28 days. As they were able to start bringing up those services, the recovery process was based off core infrastructure, which is the foundation of all other services. After that core infrastructure was re-established, GTO worked with the Governor's office for prioritization of which services should be restored and when.

Mr. Galluzzi then explained another reason the GTO was able to move really fast, was because they had excess cyber liability insurance available to them, which opened additional funding, used by utilizing a pre-approved vendor list for assistance with cyberattacks. The pre-approved vendors enabled the GTO to move relatively quickly in response to this attack, in an all-hands-on-deck fashion, bringing in these partners very quickly, including federal law enforcement, such as the FBI and CISA.

He stated there was a dire need for intelligence during the event, and that the GTO, vendor partners and federal partners all collaborated to help get through the investigative process more quickly. Devices could not start being cleared out of quarantine until they knew exactly what the threat actor touched and when, which was a large impediment. They needed to know exactly what the threat actor was doing in the environment, when they did it, and what was potentially impacted. The last thing they needed was to move a machine out of quarantine before it was absolutely clear if it had been impacted. It would have been devastating to start this entire process all over again, if one machine was not 100% clean.

There was also an issue of completely wiping a machine before critical evidence could be obtained from it, which would be critically important to either the investigative team from law enforcement or the vendor partners. If the machine had been wiped before that information was obtained, it would slow down the investigation process.

Mr. Galluzzi elaborated on the very time-consuming process of investigation, communication, and multi-team collaboration. He conveyed there was a clean group, standing up critical services, ensuring state employees got paid and critical life safety systems were stood up. Individuals were working 18-20 hour-plus days in the first two weeks, stating the first two days were viewed as incredibly dire, until the right partners were brought on to assist and determine what the recovery path was. He repeatedly showed his gratitude for the financial ability to bring on the pre-approved vendors as quickly as they did.

He then moved on to the topic of the State of Nevada paying a ransom. He stated that, in the public sector, paying a ransom is very difficult, as you are dealing with public funds and potentially paying criminals and effectively rewarding them for criminal activity. Paying a

ransom will continue to feed this criminal ecosystem and reward them, leading to continued victimization in the future. Mr. Galluzzi was then proud to vocalize that the State of Nevada did not pay any amount of money for ransom in this event.

Mr. Galluzzi then spoke to how, in an incident such as this, the public has a right to know what is happening, as this is their information and assets that officials are working with and controlling. They are concerned and scared. That being said, this was a delicate situation to navigate and not only does the public want and need to know this information, but the criminals are also wanting this information. He stated that every bit of information that was released, on every communication platform to the public, had to be filtered and monitored, ensuring that no critical information was conveyed to the bad actor, while at the same time informing the public of as much information as possible as developments unfolded.

He then spoke on restored defenses and how, with every release of information, the GTO would see a flurry of hits on their public-facing firewalls from countries of concern. These would be from the broader, threat-actor community, just trying to take advantage of the situation that the State of Nevada was currently in, looking for vulnerabilities and weak points. Again, Mr. Galluzzi stated that the GTO firewalls withstood all hits.

When word of the statewide password reset was released, the GTO immediately saw phishing attempts, trying to leverage fraudulent password reset attempts. The GTO really needed to make sure they were ready to contend with everything that was out there and they had a defense system to respond to it, which they were.

And so, what is the GTO doing now and what have they learned? Mr. Galluzzi stated they are stronger than they have ever been. He confidently stated that since he has been in this organization, significant changes were made, especially during this event, to the infrastructure and the way they manage identity infrastructure within the executive branch. He stated this makes them more resilient and stronger.

Mr. Galluzzi noted there was a special session shortly after the event, where Assembly Bill 1 was introduced, which received strong, unanimous, bipartisan support. He stated the GTO asked for help, and the legislature heard them and answered the call. He stated they received historic funding in cybersecurity, as well as some significant policy changes to aid in protecting the State of Nevada.

He stated a continued drive on projects supporting zero trust -- in network infrastructure, in server infrastructure, to reduce lateral movement by strengthening identity controls. He explained that historically, it used to be that, in network and systems infrastructure, you would just protect the perimeter with extremely strong firewalls, keeping out the bad actors, while maintaining a protected center. This isn’t possible anymore.

Everyone has mobile devices, accessing state infrastructure from several devices at home, bringing stuff in. Mr. Galluzzi stated identity is the new firewall, multi-factor authentication, and having physical tokens are incredibly important. He stated, like the Department of Defense, they are looking at PIV cards/ badges, for multi-factor authentication, segregating their tiered identity structure to better protect the most critical infrastructure.

Mr. Galluzzi then stated that this critical infrastructure is no longer remotely accessible. They are increasing policy and controls in governance so the central IT can gain visibility and control not only on physical department inventory, but software and other assets. The executive branch is now highly federated, with departments and divisions outside of the agency having a wide berth and flexibility. He stated, despite this, the GTO needs visibility of what is going on in those departments via strengthening controls there.

Assembly Bill 1 enabled the standup of a cybersecurity QRF. This means that, if the Governor declares a state of cybersecurity emergency, Mr. Galluzi, as the CIO, is empowered to have IT and cybersecurity professionals within the executive branch report directly to him. In practice, this would be done by Mr. Galluzzi maintaining a QRF made of the best of the best of agencies across the state.

He would be able to have an influx of trained and ready agencies, within the state's environment, that can be a force of readiness, so that if Mr. Galluzzi needs to surge support, any agency across the state could be given instruction by him. He stated they are moving towards practicing that, but hopefully, they will never have to apply it in a real situation. Having the capability and resources readily available, and almost at a moment's notice, is a true game changer.

Mr. Galluzzi then elaborated that, for additional governance and policy improvements, they are moving towards allow-list based governance. Currently, there is banned-list governance where departments can access resources as it suits the needs of their business operations, as long as it doesn't come from a list of the worst offenders. The move is towards allow-list based governance, which emphasizes that the GTO needs to know exactly what is on every single device, within every single agency in the executive branch. This enforces visibility in the central IT organization.

They are looking to work with govRAMP, which offers the ability to provide third-party verification of all cloud tools that are deployed within the executive branch, via ongoing security validation and verification of cloud tools. Mr. Galluzzi also indicated that the state data governance committee is working on launching a policy for data classification, similar to what the federal government has, with their unclassified/classified, secret/top secret approach, effectively doing the same thing with state-wide data. He stated there will be definitions, where agencies can have a better idea of what they have by being able to define it with common definitions and a common vernacular of that data. They will know the level of protection they need to provide on the data that they are creating and managing every day.

Lastly, Mr. Galluzzi provided a brief summary by telling the board that more practice is needed on policies put in place. Policies are only words, without any effect, unless people practice them, building relationships and trust amongst agencies. Combined forces matter, which enables faster recovery after damage and loss is incurred. He again spoke of the knowledgeable and skilled agencies and individuals that were brought in very quickly that enabled such quick recovery from this attack, emphasizing disciplined communications.

There were no questions from members.

6. PRELIMINARY UPDATE ON STATE OF NEVADA PARTICIPATION IN NATIONAL GUARD EXERCISE: VIGILANT GUARD 27-2

Brett Compston, OEM/HS, explained that Vigilant Guard 27-2 is a U.S. Northern Command-led exercise, stating the primary training audience is the Nevada National Guard, with secondary audiences of state, local, federal, and private partners. The focus will be on the National Guard joint force headquarters, and then laterally, to the state and federal government, including US North COM.

The dates of the exercise will be June 3-6, 2027. The kickoff of the information portion is called Foundation Day, which is tentatively scheduled for April 28-29, 2026. Information will be sent to partners that have been identified to participate next week.

This is the first multi-agency, multi-level -- classified and unclassified -- homeland defense exercise in Nevada. The National Guard role will predominately be at the secret level. The operation will provide a complex dynamic between both secret and unclassified events and information being shared and utilized by all players.

The concept is a Homeland Defense event, including military mobilization and deployment, potential consequences from nation-state threat actors to disrupt deployments and critical infrastructure. State of Nevada objectives are to focus on continuity of government, with three major objectives -- technical communications, public communications, and logistics and supply chain resilience.

State and local level participation and integration will be focused on key agencies, such as fusion centers, Nevada agencies and departments, critical counties, and utility stakeholders. Private sector participation will be the inclusion of a business emergency operation center, utilities, and key partner associations. There will also be an observer lane for non-participants, allowing learning of homeland defense threats, as we see it.

In addition to the exercise and preparation, the State of Nevada will have several events, including two communications exercises, a cabinet-level tabletop exercise, and quarterly emergency operations center exercises. He also stated Brigadier General Waters was present for questions, as well.

There were no questions from members.

7. NEVADA RESILIENCE ADVISORY COMMITTEE (NRAC) HOMELAND SECURITY GRANT RANKING PROCEDURE

Brett Compston, OEM/HS, stated that at the last NRAC meeting, the committee recommended a new process on raking of Homeland Security grants, moving into the 2026 cycle. All grants will now be competed every single year, with no more automatic renewals or categories, such as maintain, enhance, or new.

The Office of Emergency Management, with the Governor's concurrence, will provide enduring, focused investment areas in addition to FEMA's requirements for sustained capabilities for Homeland Security specific grant funds. Examples of this are fusion centers, bomb teams, cyber and hazmat teams. These will be released with the notice of funding opportunity. These investment areas will be Nevada specific, beyond the federally mandated, minimum spends that come from FEMA. A recurring request will require a detailed sustainment and funding plan.

Mr. Compston stated this was the most objective way they could find to give everyone a fair opportunity at money, every single year. He indicated that the commission would have to approve recommendations, once they're made by NRAC and the Homeland Security Finance Committee.

Chief Billy Samuels, Clark County Fire Department, stated that a challenge is trying to build out a program, relying on dollars for the next year, but not having enough time to actually show how well the project could be. He asked if that is taken into account in the new approach for voting, or will the committee be looking at such factors. He stated that projects that are 20 years old shouldn't be looked at, but ones that are a year old, and haven't had an opportunity to prove their worth, should be looked at with that lens, as well.

Mr. Compston indicated that, since every project will have to present every year, there will be discussion about being dollar based, capability based, etc. It was the NRAC's recommendation that this was the fairest way to give everyone an opportunity at funds. He explained that, in the example Chief Samuels just provided, if a sum of money has been invested, but hasn't quite had enough time to show its complete value yet, it would simply be another presentation asking for additional funds, as the project isn't quite complete yet and additional funding is needed to finish it.

Chief Samuels acknowledged that NRAC agreed to it but asked if the UAWG was in agreement. Mr. Compston stated that the UAWG has yet to review and agree to it, which will be done at their next meeting.

8. PUBLIC COMMENT

Vice-Chair Sheriff Kevin McMahill noted the great work by emergency response agencies in a biolab effort that occurred earlier in the week in Las Vegas.

There was no additional public comment.

9. ADJOURNMENT

Todd Fasulo, Security Crisis Management, Wynn Resorts, made a motion to adjourn Chief Bill Samuels, Clark County Fire Department, seconded. There was no opposition and the motion passed unanimously. The meeting was adjourned at 2:43 p.m.