MINUTES OF THE MEETING
OF THE
ASSEMBLY COMMITTEE ON GOVERNMENT AFFAIRS

Eighty-Third Session
March 24, 2025

The Committee on Government Affairs was called to order by Chair Venicia Considine at 8:02 a.m. on Monday, March 24, 2025, in Room 4100 of the Legislative Building, 401 South Carson Street, Carson City, Nevada. The meeting was videoconferenced to Room 1 of the Nevada Legislature Hearing Rooms, 7120 Amigo Street, Las Vegas, Nevada. Copies of the minutes, including the Agenda [Exhibit A], the Attendance Roster [Exhibit B], and other substantive exhibits, are available and on file in the Research Library of the Legislative Counsel Bureau and on the Nevada Legislature's website at www.leg.state.nv.us/App/NELIS/REL/83rd2025.

COMMITTEE MEMBERS PRESENT:

Assemblymember Venicia Considine, Chair
Assemblymember Duy Nguyen, Vice Chair
Assemblymember Max E. Carter II
Assemblymember Rich DeLong
Assemblymember Reuben D'Silva
Assemblymember Rebecca Edgeworth
Assemblymember Tanya P. Flanagan
Assemblymember Danielle Gallant
Assemblymember Heather Goulding
Assemblymember Bert K. Gurr
Assemblymember Linda F. Hunt
Assemblymember Jovan A. Jackson
Assemblymember Venise Karris
Assemblymember Heidi Kasama

COMMITTEE MEMBERS ABSENT:

None

GUEST LEGISLATORS PRESENT:

Assemblymember Toby Yurek, Assembly District No. 19
Assemblymember Selena Torres-Fossett, Assembly District No. 3

STAFF MEMBERS PRESENT:

Alex Drozdoff, Committee Policy Analyst
Sarah Delap, Committee Counsel
Judi Bishop, Committee Manager
Nikki Peterson, Committee Secretary
Mary Whalen, Committee Assistant

OTHERS PRESENT:

Timothy Galluzi, State Chief Information Officer, Office of the Governor
Adam Miller, Administrator, Office of Cyber Defense Coordination, Office of the Chief Information Officer, Office of the Governor
Ashley Garza Kennedy, Principal Management Analyst, Government Affairs, Department of Administrative Services, Clark County
Nick Schneider, Director, Government Affairs, Vegas Chamber
Randy Robison, Director, Government and Community Affairs, City of Las Vegas
Alejandro Rodriguez, Director, Government Relations, Nevada System of Higher Education
Austin Daly, Manager, Government Affairs, Government and Community Engagement, University of Nevada, Reno
Kivanc Oner, Vice President for Digital Transformation and Chief Information Officer, Office of Information Technology, University of Nevada, Las Vegas
Clara Thomas, Private Citizen, North Las Vegas, Nevada
Al Rojas, Private Citizen, Las Vegas, Nevada
James Tenney, Director, Wellness Bureau, Las Vegas Metropolitan Police Department
Nic Ciccone, Manager, Government Affairs, Office of the City Manager, City of Reno
Ryan Beaman, District Vice President, Professional Fire Fighters of Nevada
John Abel, Director of Governmental Affairs, Las Vegas Police Protective Association; and representing Public Safety Alliance of Nevada
Mike Cathcart, Business Operations Manager, Finance Department, City of Henderson
Dan Gordon, President, Nevada Police Union
Berry Johnston, Private Citizen, Las Vegas, Nevada

Chair Considine:
[Roll was taken. Committee protocol and rules were explained.] Good morning. Welcome to today's meeting of the Assembly Committee on Government Affairs for the 2025 Legislative Session. Today we will hear two bills. First, we will hear Assembly Bill 432, which revises provisions relating to governmental administration, followed by Assembly Bill 433, which revises provisions relating to peace officers. I will open the hearing on Assembly Bill 432.

Assembly Bill 432: Revises provisions relating to governmental administration. (BDR 19-551)

Assemblymember Toby Yurek, Assembly District No. 19:
Today, I am here with our state's Chief Information Officer (CIO), Tim Galluzi, and the Administrator of the Office of Cyber Defense Coordination, Mr. Adam Miller.

Chair and Committee members, I want to make sure there was a conceptual amendment [Exhibit C]. It seems like most of our bills this session have been presented with conceptual amendments. This one corrects a drafting error that came out of the Legislative Counsel Bureau that specifically takes item (l) under subsection 2 and crosses it out. To be clear, this bill aims to direct Executive Branch state agencies to be part of this Security Operations Center (SOC); everybody else has opt-in. Somehow it came out, and it said the state agencies can opt in. No, we want state agencies to be mandated to participate in this SOC. That conceptual amendment should be before Committee members; it was uploaded to the Nevada Electronic Legislative Information System (NELIS).

Additionally, I just want to put on the record, I have been contacted by the Nevada Supreme Court assistant administrator indicating some possible concerns with the way this is worded, that it might be a stretch, forcing our Judicial Branch to participate and mandate them. For the record, I want to make clear—and I will continue to work with the administrator, Mr. McCormick—to clarify that. I am an ardent supporter of *Nevada Constitution* Article 3, Section 1, separation of powers, and we will clarify any language that might be needed to address that concern as well.

Before we begin to dive into threat matrices and network logs, let me ask the Committee members something a little more familiar: Has your email ever been hacked? Has your credit card number ever been stolen? Maybe one day your phone lit up with a charge from a gas station in Ohio saying you charged fuel there when you were literally sitting in this building. Or here is my recent favorite: maybe you got one of those suspicious text messages telling you that you owe money for using a toll road. Well, I happen to sit on our Growth and Infrastructure Committee, and I can guarantee you, we do not have any toll roads in Nevada. Likely that would be a scam. Unfortunately, it is a very effective one.

Cybercrime is not some abstract threat anymore. It is very personal; it is pervasive; and it is hitting closer to home than ever. Just like we would not leave the front doors to our homes wide open, we should not leave our state's digital front door unlocked either. So let us talk Nevada for a moment. Make no mistake: we are a high-value target. Between our tourism, gaming, financial institutions, government databases, and critical infrastructure, we are not just a neon oasis in the desert. We are a blinking bullseye for bad actors across the globe.

Let us not forget, every January Las Vegas becomes the global epicenter for innovation during our consumer electronics show (CES), one of the largest and most influential tech trade shows in the world. Alongside CES, Nevada hosts a steady stream of conventions and conferences centered around cutting-edge technologies, smart infrastructure, AI (artificial

intelligence), and data. These events put us under an international spotlight. While they certainly help to drive economic growth, they also attract attention from cybercriminals looking to exploit new vulnerabilities or make a high-profile statement. You might even remember the MGM ransomware attack last year; one compromised password shut down gaming floors, canceled reservations, and reportedly cost more than $100 million. That was not just a disruption; it was a heist, a public relations nightmare, and a statewide wake-up call. The truth is, that was just one of many.

Right now, Nevada's cybersecurity posture is patchworked: different agencies, different systems, and different levels of defense. When cybercriminals exploit these gaps, it is not just agencies that suffer. It is schoolkids whose data is leaked; it is seniors who lose their retirement savings; it is veterans, patients, voters, and taxpayers. It is your constituents. That is why I have brought this bill forward after nearly a year of collaboration with various stakeholders and our state CIO officer. That is why we brought this bill.

In short, here is what Assembly Bill 432 does: it establishes a statewide Security Operations Center (SOC) under the Office of the Chief Information Officer (OCIO), providing 24/7 cyber threat monitoring and response; it authorizes federal grant funding to support the Center's operation and growth; it requires annual reporting to ensure transparency, performance tracking, and accountability; it creates a cybersecurity talent pipeline program to train and recruit Nevada's students into this growing field; it extends SOC services to school districts and local governments, helping smaller entities improve their cybersecurity with state-level resources; and finally, it empowers the SOC to enforce compliance, mitigate risks, and coordinate across agencies in the event of a cyber incident.

It is a smart, scalable, and collaborative solution, and frankly, it is long overdue. Now to explain how it all works, with your permission, Chair, I would like to hand the presentation over to Mr. Tim Galluzi, our state CIO, who will walk you through the vision, mechanics, and strategy behind this bill. We are also joined by Adam Miller, a technical expert from the Office of Cyber Defense Coordination, who is on deck to answer any questions the Committee may have.

Timothy Galluzi, State Chief Information Officer, Office of the Governor:
Thank you for the opportunity to provide insight and analysis on A.B. 432. I would also like to thank Assemblymember Yurek for his efforts in elevating the conversation on cybersecurity.

To fully understand what this legislation is endeavoring to accomplish, we must first contemplate the situation that our cybersecurity professionals in Nevada are facing every day. Modern government is interconnected government. From over 485,000 students across 761 schools and 23 school districts all sending reports, emails, communications, all at some point reaching the Department of Education and into the Executive and Legislative Branches [page 2, Exhibit D].

Nevada's information technology (IT) environment is vast. We are talking over 3.3 million residents, 28 federally recognized tribes, 17 counties, hundreds of boards and commissions, and over 40 million visitors a year. These are all stakeholders who interact with state and local systems every day. Every voter record, every tax form, every school network, every email sent, every transaction is an opportunity for a threat actor to move from a Nevadan or a visitor to a local entity and beyond. This is what we are being asked to defend.

We have made real progress through partnerships, particularly between the Office of Information Security (OIS) and the Office of Cyber Defense Coordination [page 3]. But let me be clear: collaboration is not a substitute for structure. Nevada lacks a centralized backbone for cybersecurity [page 4]. Cyber threats are becoming more frequent and more sophisticated. Many of our agencies are running on aging infrastructure and tight budgets. But what is our biggest risk? They are also our biggest asset—our people. One bad click, one missed update—that is all it takes. Both OIS and the Office of Cyber Defense Coordination take a proactive approach to cybersecurity awareness to address the human element and to help turn those risks into defenders. As you can probably assume, Nevada is not alone.

I am going to go through some case studies. In 2018, the Colorado Department of Transportation was brought to a standstill by ransomware [page 5]; $1.7 million in recovery costs and it all started with an unsecured temporary server. That is why centralized visibility and oversight are not nice-to-haves, they are essential. Quincy, Illinois, spent over six months recovering from a 2022 attack [page 6]. City files were encrypted, and entire departments were frozen. The absence of backups and coordinated response plans turned a breach into a full-blown shutdown. In Fort Lauderdale, $1.2 million was lost to fake invoices due to a business email compromise [page 7]. It was not a technical failure; it was a training and policy failure. Investment in awareness and governance can help mitigate events like this.

In 2023, Atlanta's ransomware recovery costs topped $17 million [page 8]. That number is not just financial, it is reputational. Public confidence, essential services, and internal operations were all disrupted. That is exactly what we are trying to avoid. In Texas, one attacker took down 22 municipalities [page 9]. Statewide disruption: that is the danger of a fragmented approach to cybersecurity. The inverse would be a unified response: capability, one team, one mission, shared intelligence, and response capability.

In Oakland, they declared a state of emergency after a ransomware breach in 2023 [page 10]. They lost over 600 gigabytes worth of data. They are now facing lawsuits from citizens and even their own police union. Cybersecurity failures do not just hurt systems, they undermine institutions. In Bernalillo County—this one is especially sobering—ransomware knocked out jail security systems—doors could not lock, cameras were disabled; schools were closed; and mortgage applications were frozen [page 11].

Real-world impacts of these threats are why this bill matters [page 12]. The common thread across all of these events is, cybercriminals will continue to try to exploit our vulnerabilities. The consistent lesson is this: if you do not have a central structure in place before the attack, it is already too late; you cannot build the plane in flight. We have seen patterns of

reputational harm, service disruption, and massive recovery costs [page 13]. We have also seen what works: centralized proactive cybersecurity backed by policy resources and accountability.

The good news is we are not starting from zero [page 14]. Our Office of Information Security within the Office of the Governor is already doing the work—threat hunting, training, and monitoring. This bill allows us to scale that work statewide and serve more partners effectively. In fiscal year (FY) 2024, we analyzed over 298 billion network logs—billion, with a "B" [page 15]. We reviewed over 241,000 incidents and validated 17,304 of them as legitimate threats. That is a scale of the threat landscape that we are seeing just in the Executive Branch, and we are keeping up, but we see there is an opportunity to sustain and grow those efforts. We received 12 critical emergency notifications last year [page 16]; we resolved all 12. That is 100 percent resolution on the most serious incidents. That is a standard we want to set across all state and local entities.

The number of incidents is increasing [page 17]. It is not speculation; it is data. That is not a wave we can just ride out. We cannot continue to practice security through obscurity; they are after us. We have to scale up; we have to stay ahead; and we have to keep moving. With emerging technologies such as agentic AI, that create agents that act autonomously, we will only expect to see this number grow exponentially. The Office of Cyber Defense Coordination is key here [page 18]. They are the bridge to local, tribal, and private sector partners. They are currently how we reach outside the Executive Branch.

Assembly Bill 432 does four big things [page 19]: creates a Security Operations Center (SOC) underneath the Office of the Chief Information Officer; allows us to apply for and use federal grant funding; requires annual performance reporting; and brings schools into our cybersecurity coverage. That is a strategic package. The SOC will not just watch for threats [page 20], it will mitigate them and hopefully prevent them from happening in the first place. It will develop policy, enforce standards, and coordinate response. It will serve as the center for excellence and an accountability mechanism all at once. We are shifting from scattered approaches to unified, scalable defense [page 21]. We are optimizing for cost, talent, and threat intelligence. This is about sustainability and strategy. Nevada's higher education institutions are building the next generation of cyber talent [page 22]. Our Public Sector Cybersecurity Summit convenes leaders to collaborate. We have seen that this works. Assembly Bill 432 aligns those investments and helps turn training into action.

Here is the truth: trying to run 30 different security teams is expensive and ineffective [page 23]. Centralizing under a SOC gives us economies of scale and better return on investment. Local governments are some of the most targeted and least resourced. Assembly Bill 432 opens the door for them to access state tools, staff, and expertise. This is how we protect everyone, not just the big agencies [page 24]. Our K-12 systems house sensitive data and are increasingly digital [page 25], and cybercriminals know that. Assembly Bill 432 gives schools access to state-level monitoring and response [page 26], so our students and teachers are protected as well.

This is about resilience, and with one SOC [page 26], we can share intel, coordinate response, and raise the bar across the board. It is not just smarter; it is faster, cheaper, and better. The costs of a breach are enormous [page 27]; millions in recovery, [unintelligible] costs, and reputational damage. A centralized SOC helps us avoid these costs, keeps services online, and demonstrates to citizens that their data is in good hands.

Finally, this bill is the kind of long-term thinking we need in government [page 28]. It is not about a quick fix; it is about building durable modern infrastructure that protects our state's digital backbone. The timing could not be even more critical with recent federal cuts to the Cybersecurity and Infrastructure Security Agency, the announcement of the withdrawal of federal support for the Multi-State Information Sharing and Analysis Center, and just last week's Executive Order signaling the federal policy shift toward cybersecurity preparedness and responsiveness at the state and local levels. It is time we send a clear message to all of our municipal and governmental partners here in the Silver State that you are not alone. Nevadans take care of Nevadans. It is time we ensure that if we have an agency that needs our support, regardless of what level of government they sit, if they pick up the phone, they have someone to call.

A lot of you might not know a lot about my story. Before I joined the State, I had the honor of serving our country in the Marine Corps. I know a lot of movies get a lot of things wrong, but when they talk about one thing in particular—that we do not leave anybody behind—that is true. If we have the opportunity, even in the world of cybersecurity, if we see an agency hurting, if we see an agency struggling or being attacked, we cannot sit back and watch that happen. If we have the resources to help them, we have an obligation to do so. This gives us the ability to do just that. One of the biggest frustrations I have had since joining state service is that we have arbitrary rules—and I call them arbitrary—but there are rules in place for funding reasons, for policy reasons, that we have restrictions on what we can and cannot do, when the answer seems obvious. If someone is hurting, if someone needs support, we provide that support. This bill will allow us to do just that.

Right now is the time that I can walk through, very quickly, a section-by-section review of the bill. Section 1 allows for the amending of *Nevada Revised Statutes* (NRS) Chapter 242. Section 2 requires the SOC to establish policies and procedures for combating threats, protecting data, response, and reporting requirements, as well as training requirements. Section 3 discusses potential remedies for noncompliance with SOC policies and procedures and using agencies. Section 4 allows the CIO to apply for grants to support SOC activity. Section 5 mandates collaboration with the Office of Cyber Defense Coordination. Section 6 outlines mandatory reporting requirements to state stakeholders. Section 7 defines the requirements to partner with the Nevada System of Higher Education on a talent pipeline program. Section 8 adds SOC services, the definition of "information services," and NRS 242.055.

Section 9 expands the definition of "local governmental agencies" to include the board of trustees of a school district. Section 10 defines a "using agency" as either an agency that is required to use OCIO services, or one that may negotiate. Section 11 adds the word "secure"

to emphasize security as OCIO's purpose and broadens the scope to all using agencies. Section 12 adds SOC as an entity within the OCIO. Section 13 adds details from cybersecurity incidents, specifically to the items that may be protected from public disclosure if that disclosure would further place an agency or the State at risk of further compromise. Section 14, again, broadens the definition of "using agencies." Section 15 defines what services would be provided to using agencies and allows any governmental agency to negotiate for OCIO services. Of note, section 15 is where OCIO and the bill sponsor have worked on a friendly amendment that would remove item (l) from the list of subsection 2 to prevent an exception loop.

Sections 16 through 18 further simplified language leveraging the word "using agency." Section 19 adds the requirement to report security incidents to the SOC for using agency. Section 20 requires OIS to work with the SOC to investigate and resolve breaches of using agency systems. Section 21 authorizes the CIO to set a rate for SOC. Section 22 makes clarifying updates. Section 23, NRS 218D.380, does not apply. Section 24 repeals NRS 242.141 as it is made redundant through this bill.

That concludes the overview of this bill. We stand ready for any questions.

Assemblymember Yurek:
I was watching all of your faces, and this can be a confusing topic. While we appreciate the opportunity to present kind of an overview, we would love to entertain any specific questions the Committee may have.

Chair Considine:
We do have some questions. I am requesting everyone on the Committee who has questions, please limit it to two questions, and we will go around. If we have additional time, we will go back for any additional questions.

Assemblymember Flanagan:
A lot of agencies fall into this, so one of my biggest curiosities is how you link all of these different agencies by state, county, city, unincorporated, or incorporated. This bill references five standing organizations that address information technology intelligence; what is the sixth one? How is it going to function to actually corral this? I do not see how that works in this bill.

Timothy Galluzi:
Right now, the Office of the Chief Information Officer is an internal service organization that provides services to governmental agencies. What this bill will allow us to do is really broaden our user base. With the SOC, we would be able to provide those services to non-Executive Branch agencies directly. What this bill envisions is that all non-Executive Branch agencies would be able to opt in to those services. If we are talking county governments, city governments, K-12 school districts, any non-Executive Branch governmental organization who would see the value in investing in a statewide Security Operations Center, it would be opt-in, and I think that is a clear distinction in this bill.

We are not mandating that any non-Executive Branch organization would be required to use these services. For the Executive Branch agencies, they are already leveraging these services through the Office of Information Security, so we would just shift those over to the Security Operations Center. For non-Executive Branch organizations, this would be opt-in. We are already working with them through the Office of Cyber Defense Coordination, but this would be an opportunity for us to provide more direct services to them, which, after this biennium, we would be developing a rate and then give them the opportunity to actually provide direct investment into that. Hopefully that provides a little bit of clarification. If not, I can dive more into that.

Assemblymember Goulding:
I think that, as you stated, most of us have seen, either in smaller or larger scales, this very real threat. I think three months ago I would have responded to this bill differently than I am today. Given the current data breach at the federal level by the Department of Government Efficiency that has crept through citizens' data that should have remained secure, how can Nevadans be assured the plan outlined in Assembly Bill 432 would not leave our state more vulnerable by having everything tied up in one system? You mentioned that A.B. 432 opens the door to security services, but my concern is, seeing what has happened at the federal level, it opens the door to everything.

Timothy Galluzi:
The only data at this point that would be transmitted to the Security Operations Center would be security logs and data specifically for securing the infrastructure of the participating agencies. We would not be taking over infrastructure; we are not taking data from municipal governments and moving it over to state entities. The municipal data infrastructure belongs to the municipal data infrastructure, and that is not what this bill is envisioning whatsoever. This bill is really looking for opportunities to leverage economies of scale, to be able to provide resources out to our municipal partners, resources that unfortunately a lot of our municipal partners just really cannot afford to provide at a level of maturity that we can provide statewide in a whole-of-state approach.

This does not give the envisioned Security Operations Center access to servers, data, equipment that would be in the municipal protection. That is not what this bill is envisioning whatsoever, but I definitely appreciate the concern of data security and in ensuring that what belongs to municipal governments or other subdivisions of government stays in those subdivisions.

Assemblymember Goulding:
So, you can assure us that this is not a master key to all government data systems? If it is not a master key, then what is the analogy? Is it the key creator? I want assurance, as I would imagine all Nevadans do, that there is no master key.

Timothy Galluzi:
The standard practice, and the practice we would promote through this, is that data at rest is encrypted. The Security Operations Center would not have that encryption for those agencies

it is providing services for. That would belong to those agencies. Agencies would control that encryption. That is not within the purview of a Security Operations Center.

What is within the purview of a SOC would be disaster recovery plans, threat mitigation, intelligence sharing, the actual logs that have nothing to do with the data that is involved. In our world, we practice least privilege. The last thing we would want to do is have folks who are involved with cybersecurity to have access to data because that violates one of the core principles of cybersecurity; and that is the principle of least privilege. We do not believe in master keys. As the State's Chief Information Officer, as the leader of IT, and the one who advises in cybersecurity and IT matters in the highest levels of Executive Branch, I have zero administrative privileges and that is intentional. With me being one of the largest targets for spear phishing attacks or directed attacks towards me, if they get me, then they cannot do anything with my accounts. We definitely practice least privilege and data privacy, and the SOC would be no different there.

Adam Miller, Administrator, Office of Cyber Defense Coordination, Office of the Chief Information Officer, Office of the Governor:
I think a helpful analogy is thinking of this like a post office. If I send you a letter, unless I physically walk up and put it in your mailbox, it goes to the United States Postal Service (USPS). The USPS scans that mail; they will swab it; they will X-ray it for nefarious reasons, but they will not actually physically open the mail and read the letter inside. That is the data we are talking about here. They will look at the packet you are receiving, they will scan it for malicious intent, but they will not actually physically open that letter and read the writing in the letter.

Assemblymember DeLong:
I have two questions, one general, one very specific as it relates to section 15, but not necessarily the amendment. The general question, is the intent of this bill basically a reorganization of an existing system using existing staff and responsibilities, or are we creating a new program that needs new staff with new responsibilities?

Timothy Galluzi:
I would like to move away from the word reorganization. It is definitely a realignment, and that might be synonymous, but this is an authorization. That is the way I look at it. This authorizes the Office of the Chief Information Officer to stand up this program. This program, in the very early stages, can begin as more of a virtual program where I do not necessarily need boots on the ground on Day One. This allows me to extend services that already exist within the Executive Branch out to municipal entities at, hopefully, a lower cost than if they were going out individually to get those services on their own.

The vehicle that has been designed to do that is this Security Operations Center. Our intent is to leverage the federal grant funding that has already been made available and additional grant funding we hope to go out and secure to eventually bring the boots-on-the-ground piece to build this out as a program. That is our intent to do this upcoming biennium; then we would be back next biennium to have further conversations on what that is growing into. To

answer your question, this is not a reorganization of resources that we already have within the Executive Branch. This is more of an authorization to be able to extend the tools and abilities we have in the Executive Branch out to our municipal partners.

Assemblymember DeLong:
My second question, as it relates to section 15, you have got subpart 1 and then subpart 2. I am just trying to understand, how did you divide up the various state agencies and say, OK, this group of state agencies, you are required to do this; this other group of state agencies, you can opt in. What was your litmus test to say who falls in which group?

Timothy Galluzi:
The list of agencies that are currently in subsection 2 have historically been in subsection 2 for quite some time. Those are carryover from previous legislation.

Assemblymember Jackson:
My only concern is, if schools opt into this—children often say stuff they do not mean. There are real threats and then there are some things that are just said on impulse. Could this tool be used to target and criminalize children?

Timothy Galluzi:
I do not believe that would be in the scope of this bill. I think what we are really looking at for this legislation are network scans, scans of infrastructure; we are not looking at content of communications. I do not see how this bill would divert from any standard course of action that is currently being conducted within K-12.

Assemblymember Karris:
How many states have enacted an Executive Branch-driven, centralized cybersecurity system? Are we the first or are there others?

Adam Miller:
As far as a specific number, I can definitely come back to you with that. I think one [unintelligible] example of this would be North Dakota. Four years ago, North Dakota had a very disparate cybersecurity patchwork organization throughout their state. In the last four years, they have increased their cybersecurity operation 50 full-time equivalents and approximately $30 million. They stood up their own SOC. I think for me personally, that is kind of the shining light we would move toward, is a North Dakota operation. As far as the specific number of states that have a centralized SOC, we can definitely get back to you with that answer.

Assemblymember D'Silva:
You said briefly there were issues accessing federal grant funding for programs like this. I was wondering if you could discuss some of those issues. Also, what specific types of grants would you be applying for? I see section 4 expressly gives powers to the Office to apply for these sorts of grants, so what kind of grant funding would you be looking for?

Adam Miller:
I am sure many of you are familiar, the federal grant situation is currently fluid. The Office of Cyber Defense Coordination in particular has, I think, five or six grants from FY 2023 through FY 2024. Two, in particular, are for a Security Operations Center; two, in particular, for an incident response team; and one is for a cyber threat intelligence program. This money can be used to leverage and bolster a state-driven Security Operations Center, whether that is through training programs—so to Assemblymember Jackson's point, we are not going to be monitoring communication from students—but we can provide that training to K-12 and say, These are ways you can avoid malicious links; these are ways you can ethically hack within the classroom environment; not going out and trying to be a renegade and do it that way.

The grants we have already procured—and we are just waiting for the money to come in and the authority to go spend—will be used as a kind of pillar in how we reach out to the community, provide them licenses, provide them training, and bring them into the SOC circle.

Assemblymember Carter:
My question has to do more with alignment. We have seen the Executive Branch of this state align themselves with the illegal seizing of personal data at a national level, and letting independent contractors and nongovernment agencies come in and attack and have access to personal private data, with our Executive Branch not only cheering that, but perfectly aligning themselves with that effort to tread all over Americans' rights. What kind of confidence can we have that this is not that same action being extended down to state level to create a way to attack Nevada citizens for the benefit of political means?

Timothy Galluzi:
Like I mentioned before, the municipal governments are still in control of what data is given to the SOC. The only data the SOC would be given access to is the data that is required to conduct scanning of network infrastructure, logs, and security events. It is not the private personal data that would be of concern. That is wholly owned by the municipal entities, by the owners of that data. This would not give the Executive Branch of state government access to that in any means necessary.

Assemblymember Carter:
We still have not had the answer because early January, we did not think this could happen at a national level. We were assured; we thought we were secure in our constitutional rights, and that evaporated overnight. Now our rights are being trampled all over. How can we possibly trust this type of an effort?

Adam Miller:
Assemblymember, I think I share your concerns with making sure that data is protected. Going back to Assemblymember Goulding's question, it is less about getting into that letter, it is a means of just making sure that letter, in and of itself, is safe. For the data you are speaking to, we are not looking to go into that specific line and find that specific person and target them. That is not at all the data we are looking after. We are making sure the data flow

is safe. If there is malicious intent with any of the packets that are being sent, that is what we are looking at.

When we talk logs, a log is very vast, and that is a matter of, I am logging onto my computer in the morning, or I am opening a PDF [portable document format] file. These are all considered logs. The nefarious intent of the 298 billion logs that the CIO mentioned in his presentation from last fiscal year; it is so vast. We are not looking to target specific data sets for voters or constituents or anything like that. It is strictly managing the network traffic, protecting the network infrastructure, and making sure there are no nefarious purposes.

Assemblymember Hunt:
I just want a clarification. You want to create a new department, Security Operations Center, which oversees lots of other departments. It also tells other departments what to do and would have the ability to punish. What I want to know is, what entity will be above the Security Operations Center?

Timothy Galluzi:
What this bill envisions is, the Security Operations Center would reside within the Office of the Chief Information Officer. With everything we have done since our office has moved into the Office of the Governor, we embrace the tenets of shared governance. Every policy that has come out of my office, we put it in front of our state Technology Governance Committee, and this is made up of representatives from across the Executive Branch.

Our vision for this is that the Security Operations Center would have a committee just like that. Any decision, every policy, and every product that would be supporting the Security Operations Center would be selected through a governance committee of all of the represented entities that are supported by the Security Operations Center. We want our stakeholders that have invested in the success of the Security Operations Center to have a voice, and that is what has made our agency successful in supporting our agency partners throughout the Executive Branch. We want to extend that down to the Security Operations Center.

The way this bill envisions the Security Operations Center today is, it would sit within the Office of the Chief Information Officer, and then it would be directly supported by the Office of Cyber Defense Coordination and the Office of Information Security. It is not a brand-new department. Like I mentioned before in a previous question, it really just gives us the authorization to provide these services through this vehicle.

Assemblymember Yurek:
Also to address your question, I am hearing kind of a theme of questions that are going on here, and I really want to reiterate that this, again, is not just trying to create this new megadepartment that can oversee and control our entire state. What it is trying to do is really pull together what I think every member on this Committee will agree is the threat and mitigate the cybersecurity threats that exist out there.

If I use the weakest link in a chain analogy, it is a hodgepodge right now of security defense mechanisms that our various state agencies have in place, and access through one can gain access to the other. What we are trying to do through this is mitigate any of those weak links and ensure we have one strong cyber defense system in place that our state agencies will use. The idea of threatening or punishing or doing—really, what it is designing is ensuring that any body that is part of our state's infrastructure, and to mitigate against these threats, meets certain minimum thresholds, minimum standards to ensure we can accomplish the SOC's goal, which is to prevent our state against these types of attacks.

Assemblymember Gallant:
First of all, I want to say thank you for bringing this bill forward. I also want to apologize. I think some of the line of questioning is kind of way out there. I do not think you guys deserve that. To me, what this sounds like—and I just want to reiterate a little bit—last night, I watched *300* on the flight up here and he used the analogy that all the shields, everybody has to be able to hold them up together in order to have a strong wall, same as the weakest link. This sounds to me like you guys are looking to offer an upgraded software that, really, these local government agencies would not be able to have access to, would not be able to afford, so they can have the most protection. It is not the National Security Agency—that is not what you are looking to do—but offering the greatest protection for Nevadans, for our kids, and for our constituents so we can ensure that our data is protected. Is that correct?

Timothy Galluzi:
Absolutely. Our intent with this bill is, and why we are supportive of it, it does raise the tide. We understand, and I think we tried to highlight during our presentation, that Nevada is so interconnected. All levels of government in Nevada are so interconnected that no matter what level you begin your interaction with, eventually it will lead to the Executive Branch and to the Legislative Branch through our communication systems, through SilverNet.

Our intent is to provide at least the opportunity to set a baseline level of security across all entities, to offer that as a service, and to offer that as an opt-in. If municipal governments, if K-12, as any other governmental organization across Nevada, if they find value in that service offering we are putting out there, then they can invest in it. If they do not, then they do not have to. I think that is the clear distinction in this, that it is opt-in. If they do not like what we are selling, they do not have to buy. I think we are incredibly confident that the numbers are there. Once they see what we can provide, the value we can provide; the community we are standing up; the intelligence we can push out there; the value of economies of scale in licensing, in support, in communication; then they will see it and they will be there for us. I think that is what we are really trying to provide.

Assemblymember Nguyen:
I think tough questions are part of the presentation, so I am glad you are all prepared. The existing infrastructure of the OCIO already has somebody doing this; that is Mr. Miller. Your role is already administrator for the Office of Cyber Defense Coordination, right? Why do we need to create something extra when the existence of your role and the definition of what you do is already in here?

Adam Miller:
Vice Chair Nguyen, there is a bit of a distinction. My role is everything outside of the Executive Branch. The OIS that currently sits under the OCIO, actually runs the SOC service for the Executive Branch. Currently, I do not touch the SOC service that the state provides. What this bill is looking to entertain is, I will be playing a key role in bringing in our community partners to that SOC service. I do not, myself through my office; I do not touch the current SOC service that the state provides; that is done through the Office of Information Security.

Assemblymember Nguyen:
It would make sense for you, who has the experience to coordinate and bring everybody together, versus creating something completely separate. Is that not kind of redundant to the process?

Timothy Galluzi:
What this bill really does is, it gives the Office of the Chief Information Officer the authorization to provide those direct services to those municipal entities via the SOC. The bill codifies that direct link between Office of Cyber Defense Coordination, in being that key partner and bringing those municipal partners in. We do not currently have that operational mechanism to be able to provide those direct services to municipal partners or to non-Executive Branch stakeholders.

That is why we needed this legislation, because we do not currently have a vehicle to do that. Right now, Office of Information Security can provide those services directly to Executive Branch entities, and we do so, and they do a dang good job doing it, but we needed a vehicle through this legislation to extend those services out to municipal, to non-Executive Branch entities.

Chair Considine:
I have a couple of questions. When you first started talking, you were using examples of what happened at the MGM, what happened in Colorado, and those sorts of end users—and I do not know if I am using that properly—the flaw in that being, it is the person who opens the email. In both of my roles, I have IT departments that say, this email may be suspicious; but it is still up to me if I want to click on it. My question is, how does a centralized structure stop a single user from clicking that button?

My second piece, going to my colleague from Assembly District 23's *300* reference, that does work. But if you are allowing people to opt in, then you are allowing entities to not, therefore that blows the whole idea that everybody has got their shield up if there are people who do not have shields.

Timothy Galluzi:
You are absolutely right. The human element is still, like I said in the presentation, that one piece that there is no system, there is no absolute control, that is a hundred percent preventative of that last piece. What we do, and what we do quite well here in the Executive

Branch, is we educate, we train. We have a platform here in the Executive Branch called KnowBe4, and we send out simulated phishing attempts and whatnot, so they get real practical training on what email is suspicious and what is not. If they click on one of our training emails, they get some remedial training—no one likes remedial training—and then their supervisor is notified, and it is a lot of fun.

That is one of the ways we mitigate that process, and we have the numbers; we can back that up that it works. It is never going to be 100 percent, so one of the service offerings we are envisioning is to be able to extend a service like that, a similar service, out to all partners in the SOC [Security Operations Center]. We can at least raise that tide across the entirety of Nevada.

Then to the second part of your question, how do we make sure that shield wall is as strong as possible, with as many shields as possible, and that is on us to go out there, hit the streets, and prove the value of this, to do that stakeholder engagement. We are not starting from ground zero. Administrator Miller and I, we have already been having those conversations with a lot of the key stakeholders across Nevada. Are we going to be at 100 percent on Day One? Probably not, I can almost guarantee no. But we had to leave it as opt-in because municipal governments are their own governments, and we had to respect the fact that they can determine their own fate and their own direction.

We would love for them all to say, Hey, this is a great idea. We all want to invest in cybersecurity, and this is the path we want to go on. We wanted to put it out there and bet on ourselves. If this is worthwhile, we would build this in a way that we have to go out there and prove the value of this to the point where they have to put this in their budgets moving forward into next biennium. If we are not out there proving enough value, then we are not doing our part.

Assemblymember Yurek:
I have had numerous conversations with local governments, counties, municipalities, all of whom have acknowledged and recognized the threat and the need for cybersecurity. There are some entities that are ramping up their own. They have invested in products and services to mitigate this threat that is out there, and, quite frankly, have expressed some interest in the idea that our state might be able to offer those services at some point through economies of scale. Where they see not only in the long term that this is not costing more money, it could save money just by leveraging these resources and making these offerings statewide across all of our agencies. There are also smaller entities out there—smaller governments, counties—that do not have big budgets. Because we have put this package together in a scalable way, we would be able to offer these services and provide it to people who do not have the ability to really fend off these types of attacks now.

Addressing the first part of your question, we will certainly never escape the human element. Through training, I think most of the members of the dais have learned to recognize, Oh, this thing looks a little fishy, there are no toll roads in Nevada—these sorts of things. Training and stuff will certainly help, but that human element will always be there.

In terms of getting everybody on board, as Mr. Galluzi said, I think through time we will demonstrate the efficiency of this statewide SOC in offering these services and the money savings that can be had as a result of that. I think in the long term; this can be something we will get large-scale buy-in to.

Chair Considine:
Then my second question is for those entities that opt in. They opt in and there are trainings, equipment, and services. On page 4, section 3, there is also, if the entity opts in and does not comply with the cybersecurity policies and protocols developed by the SOC, the Chief may impose additional oversight, audit requirements, restrict the agency's access to the equipment of the office. Or they could charge the agency an additional amount for using the agency's continued use of equipment and services. Also, once they opt in, the user agency, whether they are a small entity or a large entity, they are paying out of their own budgets for services and equipment, and that equipment is installed on their systems, and there is a charge for that. There are also penalties if they do not follow. Am I reading that correctly?

Timothy Galluzi:
Yes, that is the correct interpretation. I believe the intent of that section was to ensure compliance with the policies. It is one thing to sign up for a service and say one will follow the policies, but then if there is noncompliance and there is no enforcement mechanism, it could create a situation where you are putting the larger entity at risk. I think that would be taken very judiciously and at a step-up type mechanism. We are, obviously, incredibly open to conversations on that section. As with everything in this, being that it is opt-in and all of these services would be negotiated for, even that provision could be handled during the negotiation process with the agencies that are leveraging these services.

Assemblymember Kasama:
Cybersecurity is a real threat. We have it now, and it will only continue to get worse. I do think as a state we have an obligation to look at the most efficient ways we can protect our state and the information that we do have. I am in real estate, and we are constantly under attack with insurance companies, real estate. We have people losing large amounts of money because of cybersecurity. It is something we have to constantly work at and be vigilant with. Thank you again for looking to try to bring economies of scale to the state.

I just wanted to understand, this is authorizing language, so at this point, there is no fiscal note or need for any additional staff because you can handle it with your current infrastructure. Along with that, in the future, agencies would be paying for it, so you do not need to increase the budget with this new Security Operations Center.

Timothy Galluzi:
Your interpretation is absolutely correct. Because this legislation is just authorizing legislation, we are not attaching a fiscal note to this. Just like was previously mentioned, we plan on scoping this up as the need increases. As municipal partners or non-Executive Branch partners sign onto this service, we would then extend out those services to them. We could set a rate at that point if we do not have grant funding. It would be effectively

cost-neutral as we roll it out initially. Then we would talk about future funding in future biennia for sustainment moving forward. At that point, we would be able to set a rate. We already have the authorization in NRS Chapter 242; it is already existing for the Chief Information Officer to set a rate for services. This would be a self-sustaining program moving forward.

Chair Considine:
Everyone on the Committee who has not asked a question had the opportunities, so there are a couple of second-chance questions here.

Assemblymember Goulding:
Just a point of clarification, because the examples you have given us are all related to email. Is this really email security? Would it be appropriate to think of this as a beefed-up Microsoft Office email security? Or is there something beyond that? I think that some of us have expressed some concern about access to data that is not email. I am wondering if you can just clarify what you are proposing to secure.

Timothy Galluzi:
We use email just as a very tangible and comprehensible example. I think the vast majority of the logs and what the Security Operations Center would be seeing would honestly be very boring logs to this Committee. It would be network traffic logs. It would be log-in attempts; it would not be very exciting stuff for the general public to see. It would not necessarily be an email security platform. It would be more of a holistic security approach where we talk about security logs from different sensors that might be embedded in infrastructure—not at the data level; we are talking the infrastructure level. We are talking about network logs. We are talking logs from servers, not the data, but the actual equipment itself.

That is what a lot of the work that the Security Operations Center would be doing; it would be monitoring that network traffic to look for any anomalous activity. If we see any activity that is coming from a country of concern or going to a country of concern, that would obviously be an immediate flag for us and that would trigger immediate action. A Security Operations Center would provide us that opportunity, that real-time monitoring opportunity, to be able to act. Instead of waiting for an event to happen, we would be able to respond in real time. Email is a very convenient example to use, because we all use email in our daily lives, but that is only one small piece of what the SOC would be doing.

Assemblymember Goulding:
Thank you for that clarification. It is helpful.

Assemblymember Flanagan:
I thought I would save my second question until I heard a bit more of your presentation. We have not even really begun to get into the weeds of what the equipment itself consists of. It is curious to me how it would roll out across counties, given that you have clerk's offices, recorder's offices, assessors, treasurers, and hospitals that have within them already intricate programs they use to interface and interact with their customers. If an agency were to

consider opting in when most of them already have very sophisticated systems in place under their chief information officers, and they spend quite a bit in their budgets, what type of manpower to actually watch this broad of a data tracking are we talking about hoping they will pay for?

Timothy Galluzi:
What we are looking at in the very initial phases of this is to leverage what is coined as a managed security operations center. And so that is primarily vendor-supported. If it is services that are beyond what my Office of Information Security can provide, it would be vendor-supported, and a lot of that is virtual. It would be synonymous with a platform as a service or a software as a service. As far as actual physical equipment, I do not foresee, in the initial rollout, us having to show up with a truck's worth of equipment out to Elko or Ely to drop off and set up physical infrastructure. It would be more along the lines of installing software, rolling out digital sensors to support those communities, and signing them up for a subscription service is more likely the response in at least the initial rollout as we scale this up.

Adam Miller:
I think this kind of touches a bit on Assemblymember D'Silva's original question, too, about where some of the grant funding can come from. The grant funding will provide a beautiful on-ramp for the state SOC. What I mean by that is, the grant funding I have received for my office comes from the State and Local Cybersecurity Grant Program (SLCGP). Within that, my office has to act as the rural pass-through. As we look at Clark County, Washoe County, they have most likely got the budget resources to pay for the SOC outright from Day One. When we look at our smaller municipalities, smaller counties, I am able to use that grant funding to purchase the licenses and the training materials they need so they are not fronting the cost on Day One. I think that provides that on-ramp to get them in the door; then as we talk about next biennium, the biennium after that, building that into their budgets. In the meantime, I can provide those licenses they need to get on board through grant funding.

Assemblymember Flanagan:
Are you saying you have done an assessment of which counties have this need, or you just assume that this is such a great product, they will all want to get on board if you can stand it up nicely?

Adam Miller:
Yes. We are currently in the middle of a feasibility study with the University of Nevada, Las Vegas (UNLV) on what a statewide SOC would look like, target areas, and who to bring on board first. Because I have the SLCGP grant money, I have to spend a majority of that in rural areas. Otherwise, the State of Nevada loses the entirety of the $5 million grant. Whether we highlight certain municipalities or certain counties that need that service, that money has to go to those areas. That will be the primary focus of where we onboard those folks. Again, it is opt-in, so they do not have to take that service, but that is who we will be engaging with at the forefront to make sure we can look at bringing those folks in.

Chair Considine:
I do not think there are any additional questions from the Committee. This is an important topic. It is important that we flesh out as much as we can from our end so that we can explain everything that is going on. I really appreciate your time on this.

We would now like to move on to testimony on this bill. We will begin with testimony in support of Assembly Bill 432.

Ashley Garza Kennedy, Principal Management Analyst, Government Affairs, Department of Administrative Services, Clark County:
Our Clark County Chief Information Officer (CIO) has been in conversations with the State CIO, and we believe this moves us towards a single model of cybersecurity and easier to participate in statewide efforts. I do appreciate that this is an opt-in system because it gives us the ability to plan, collaborate, and budget for these services.

Nick Schneider, Director, Government Affairs, Vegas Chamber:
We are here in support of A.B. 432 as well, as it creates a centralized source for developing stronger and faster responses to cybersecurity breaches. We appreciate this is a comprehensive approach that creates both a cybersecurity talent pipeline, as outlined in section 7, as well as gives some economic scalability to state and local agencies that are looking at strengthening their systems, as contemplated in section 15. Cybersecurity is essential to keeping our state thriving as well as protecting the data of all Nevadans. We ask for your support.

Randy Robison, Director, Government and Community Affairs, City of Las Vegas:
For the record, in support of A.B. 432. We ventured down this path a few years ago at the City of Las Vegas. We are aware of some of the challenges and issues that come up that you have all raised here this morning. I really appreciate you giving it so much time because this is a critical issue for all of us. We might have the strongest fortress we can possibly muster, and we spend all of our time protecting our own fortress. If another piece of the network is not as strong, that creates a vulnerability for all of us.

Several years ago, I spent many years with one of the largest telecoms in the world and got a little nerded out about cybersecurity. One of the examples I remember is of a threat that occurred, an attack that was successful, in a very rural area of a very rural state that ended up affecting institutions across the western United States. They do not care how they get in; they just want to get in. The more we can share intelligence and help each other protect each other, the better off we will be.

Alejandro Rodriguez, Director, Government Relations, Nevada System of Higher Education:
Nevada System of Higher Education (NSHE) plays an important role in cybersecurity enhancement, and the provisions of this bill help address the growing threats that impact all sectors, including higher education. We especially look forward to collaborating on the scope and structure of the development of the cybersecurity talent pipeline program, as this will

provide valuable hands-on opportunities for students to develop the skills needed to fill critical workforce gaps in this high-demand industry. By leveraging NSHE's expertise and educational resources, A.B. 432 helps Nevada have a well-trained, highly skilled cybersecurity workforce, prepared to meet the challenges of the future. We appreciate Assemblymember Yurek bringing forward this bill and we urge your support.

Austin Daly, Manager, Government Affairs, Government and Community Engagement, University of Nevada, Reno:
We are in support of A.B. 432, and especially in support of the cybersecurity talent pipeline program for our students as well.

Kivanc Oner, Vice President for Digital Transformation and Chief Information Officer, Office of Information Technology, University of Nevada, Las Vegas:
[Read from written testimony, Exhibit E.] I am here today to express UNLV's strong support for A.B. 432. This legislation speaks directly to an urgent and growing need: the ability to safeguard Nevada's public agencies, institutions, and infrastructure against increasingly sophisticated cyber threats. A centralized SOC would significantly enhance our statewide cyber readiness by improving visibility, coordination, and response across jurisdictions.

I want to acknowledge our Chief Information Security Officer, Vito Rocco, who has been instrumental in advancing this vision. We have been working closely with State CIO Tim Galluzi for over a year. What makes A.B. 432 particularly forward thinking is its integration of workforce development to the cybersecurity talent pipeline program.

At UNLV, we see firsthand how much interest and demand there is from students for practical, hands-on cybersecurity experience. This initiative would allow them to work inside a real SOC, learning directly from seasoned professionals and gaining the kind of experience that leads to meaningful, high-impact careers. We recognize that continued dialogue and thoughtful planning will be needed to ensure this workforce pipeline is supported sustainably, including discussions around resources, grants, and funding as the program scales.

This is also a moment of strategic alignment. Our current Officer in Charge, Heavey, has been deeply supportive of this effort. He has helped ensure this initiative is embraced across the university. We have also been working with our academic partners, including faculty in business and computer science, to align curriculum and research opportunities with this emerging infrastructure.

Assembly Bill 432 is more than a cybersecurity measure. It is an investment in Nevada's digital resilience, workforce development, and economic competitiveness. It helps position UNLV, and our sister institutions across NSHE, as national leaders in cybersecurity education and innovation. I respectfully urge your support and thank you for the opportunity to speak today.

Clara Thomas, Private Citizen, North Las Vegas, Nevada:
I am in full support of A.B. 432, as this is something that our state will need in the future. I am looking at it as being relative to the Iron Dome. It is not an individual entity; it is for the whole scope of Nevada. I think this would be something that not only myself as a constituent, but other constituents, especially when we have breach of security in any small entity. This way, the bigger picture is that before it happens, this could be alleviated. I want to thank Assemblymember Yurek for sponsoring A.B. 432 and I am in full support.

Chair Considine:
We will now hear testimony in opposition to A.B. 432. Is there anyone wishing to oppose A.B. 432?

Al Rojas, Private Citizen, Las Vegas, Nevada:
I am testifying in strong opposition against A.B. 432. I live in Assembly District 12. The Committee has asked some very specific questions regarding cybersecurity. I am a retired electronics and software engineer, and I have expertise in designing many softwares. This weekend, I was on social media and I got into a dispute. Somebody determined that I downloaded videos to fix my android phone and to repair my cyber wall, I mean, put up sheet rock on my wall. How come I did not know how to do that? They ridiculed me. I wanted to know how did they figure that out? I wanted to have maybe a software security detective determine that.

The problem here is, this is the worst explanation of a software product I have ever seen because you are supposed to have a spec. The person who presented the software should be ashamed of themselves. When they were asked these questions, he should have pulled out a software spec and said, In our specification, it says this, and these people will be held accountable. There should be clear boundaries. I have designed both hardware and software. I have designed a lot of stuff. Any engineer, when asked a specific question, will bring out a specification and tell you this is a product that I am using; this is our procedure. I heard nothing from the presenter of this that our software spec specifically states that the boundary is here, and everybody crosses this boundary will get arrested.

I am part of a neighborhood watch program, and there are a lot of times when we got to trespass people, and the police have to follow the rules. Our rules for the law are very well laid out and we should be taking that path also for software security laws. I am totally against this bill, and I am sorry, I am disgusted for the discussion of the person who presented this—

Chair Considine:
Thank you, Mr. Rojas, that is your two minutes. We will now move on to neutral testimony. Is there anyone wishing to testify in neutral on A.B. 432? [There was no one.] Would the presenter like to make some final remarks?

Assemblymember Yurek:
I want to tell you that I love the way this hearing went. I love the robust debate and the difficult questions. Truly, it is fun to see a Committee that engages like that.

What I want to do, as I close, is offer assurances that there is nothing in A.B. 432 that is going to extend our state, its agencies, anybody, increased access to the data, quite frankly, that this bill is designed and is attempting to protect. We all agree. I have seen that as a theme as we just continue to advance down this digital age of wanting to protect our data. That is exactly what this bill does. It does not give us access to the content of this information. It is all designed to help elevate, coordinate, the defense systems we can have in place to fight off attacks that people would otherwise get access to the data we are all trying to protect. I appreciate everybody's questions and participation, and I encourage your support of A.B. 432.

Chair Considine:
I will now close the hearing on Assembly Bill 432, and I will open the hearing on Assembly Bill 433. We have the former Chair of Government Affairs, Assemblymember Torres-Fossett.

Assembly Bill 433: Revises provisions relating to peace officers. (BDR S-399)

Assemblymember Selena Torres-Fossett, Assembly District No. 3:
Today, I will be presenting Assembly Bill 433, which was a Joint Interim Standing Committee on Government Affairs piece of legislation, which revises provisions relating to peace officers. I am also joined by Dr. Tenney in Las Vegas, who will share a little bit about why this is so important for our peace officers now. I am going to pass this to Dr. Tenney first, then I will go ahead and talk a little bit more about what the specific piece of legislation does, do a section-by-section breakdown, and discuss some of the amendments.

James Tenney, Director, Wellness Bureau, Las Vegas Metropolitan Police Department:
My name is Dr. James Tenney, a licensed psychologist in Nevada. I am the designer and director of the Las Vegas Metropolitan Police Department (LVMPD) Wellness Bureau. I am representing LVMPD in strong support of Assembly Bill 433.

This is a general comment: I believe the question has been answered: compared to the rest of us, police officers encounter a significantly higher degree of PTSD [post-traumatic stress disorder], depression, anxiety, family disruption, and suicide. This task force is well-positioned to review existing policies on law enforcement wellness. I think the actual gem might be that this task force can provide a wireframe for avoiding the pitfalls and missed opportunities of well-meaning wellness bureaus across the country, and guide toward the most effective and most impactful mental health response at the state level.

Assemblymember Torres-Fossett:
During the interim, we heard from many of the law enforcement agencies throughout the state of Nevada. One of the items each agency mentioned was the need for us to create a consolidated and more strategic plan in regard to mental health for peace officers here in the state of Nevada. This bill is driven off of the recommendation from the committee. There were a lot of recommendations, different projects we could have funded, and different ways

to do things that we are doing. It became clear, too, we needed to have an initial conversation.

Due to the demanding nature of their work, peace officers face different and often greater health and wellness risks than the general public. Multiple studies have examined this issue. One such study reports that peace officers are at risk of mental health conditions including PTSD, depression, anxiety, suicidal ideation, or self-harm. Furthermore, studies report that police officers are often seen as a high-risk group for developing mental health disorders, and the challenging and stressful nature of police duties has negative outcomes on mental health.

Due to these concerns, it is necessary to consider different mental health techniques and plans to address them, including programs like screening, long-term monitoring, mindfulness practices, stress management tactics, or counseling services. Each department in the state of Nevada is doing something differently in regard to providing support and services for our peace officers. This is an opportunity for us to have a conversation and really figure out what it is that we as a legislative body can be doing to support these efforts and make sure mental health and wellness standards for one department look similar to what other departments have. That is simply not the case right now.

These health risks are also extended to physical health. A workplace health and safety report highlights the bodily stresses the officers undertake, including demanding work schedules that leave little time for recovery, physical strain, and chronic pain as a result of work duties and various operational risks.

These realities are reflected in the state as well. During the interim, we heard from multiple law enforcement agencies that health and wellness are key issues under their consideration, including the work to combat mental health stigma and to implement programs needed to support officers. To best accomplish this, the interim committee voted unanimously to create a task force to address these concerns. Specifically, this bill creates a Blue Ribbon Task Force on Peace Officer Wellness to review existing state policies concerning personal wellness initiatives that account for mental and physical health of peace officers and other law enforcement personnel.

During the interim, the firefighters had reached out to me early on to address how they are seeing similar issues with the firefighter community and how they continue to need mental health supports as well. With that, I have accepted an amendment that includes them as participants in this task force, recognizing they have similar issues, and they are responding to similar situations and view similar trauma. It is also known that 37 percent of firefighters have contemplated suicide, which is nearly ten times the rate of the general population. I think it is essential that this body works to create solutions that can support our first responders, which is inclusive, obviously, of firefighters. This piece of legislation ultimately creates that committee.

At this time, I am going to be open to any questions. I think the legislation is straightforward on who the nominating agencies are. A couple of different groups had reached out to me as

well and said, Hey, can we have this specific agency on the committee? Obviously, there are a number of counties and local governments and cities that would all like to participate in this task force. However, at that point, you could have a task force of 50 different agencies, which would not be productive. I have just enabled and empowered the leaders who are elected by the community and our state; and by ourselves as well, as they are the leaders and representatives of our individual caucuses here to make the appointments. Just to make it clear, they should be one of those four. At this time, I am ready for any questions.

Chair Considine:
Are there any questions? [There were none.] You have done an amazing job—we have no questions. We will move on to testimony. Is there anyone wishing to testify in support of Assembly Bill 433?

Nic Ciccone, Manager, Government Affairs, Office of the City Manager, City of Reno:
Just want to say thank you to the bill sponsor for including us in that working group, and we are excited to work on the task force.

Ryan Beaman, District Vice President, Professional Fire Fighters of Nevada:
I am a firefighter, serving our community for the last 29 years, with strong commitment to the public safety. I am here today to express my support for this important piece of legislation, which proposes to create a task force on first responder wellness and concerning personal wellness initiatives that account for mental and physical first responders.

I am here today to talk about a group of people who serve our communities with courage, strength, and selflessness—our firefighters and police officers. But behind the uniform, behind the badge, are human beings; people who carry the weight of every tragedy they respond to; people who wake up every day not knowing the danger they face; and who often carry the emotional scars long after the sirens stop. Nearly one in three first responders will develop a behavioral health condition. Firefighters, as mentioned, are ten times more likely to contemplate suicide than the average American. In some years, more police officers have died by suicide than in the line of duty.

These are not just statistics; they are warnings. They are telling us the stress, the trauma, and the pressure the individuals face, day after day, is taking a toll, and often they are not getting the help they need. When mental health goes unaddressed, the costs are profound for first responders, their families, and the public they serve. We see burnouts, we see strained relationships, and ultimately, we lose good people; not because of what they saw on the job, but because they felt they had to face it alone. The barriers are real, but they are not immovable.

Many first responders do not seek help because of stigma—they are afraid of being seen as weak or they simply do not have the access to trusted confidential resources. We must change that, and we can do that with this task force. Because we take care of the people who protect us, they are better equipped to serve with compassion, professionalism, and strength. Let us send a clear message to our firefighters and police officers: we see you, we hear you,

and we have got your back. Let us invest in mental wellness, not just because it is the right thing to do, but because it makes our community stronger, safer, and more united. Please support A.B. 433.

[Exhibit F was submitted and made part of the record.]

John Abel, Director of Governmental Affairs, Las Vegas Police Protective Association; and representing Public Safety Alliance of Nevada:
I was excited to come in here and see Dr. James Tenney here for Metro. I want to give a shout-out to Sheriff McMahill for establishing the Wellness Bureau. Last year was the first time in several years LVMPD has not lost an officer to suicide. That has a lot to do with the work that Dr. James Tenney, the Wellness Bureau, and the sheriff of LVMPD have done. For that reason—thank you so much—we support this Committee.

Mike Cathcart, Business Operations Manager, Finance Department, City of Henderson:
The City has invested considerably in public safety wellness, and we look forward to sharing our story and what we have learned with the task force and learning from others. We are in full support of the bill.

Randy Robison, Director, Government and Community Affairs, City of Las Vegas:
I think Mr. Beaman said it well, so I would just echo his testimony in support of this bill.

Dan Gordon, President, Nevada Police Union:
I am just going to reiterate what everybody before me said. We are in full support of A.B. 433.

Chair Considine:
Is there anyone else wishing to testify in support of A.B. 433?

Al Rojas, Private Citizen, Las Vegas, Nevada:
Our mental wellness, mental health for our first for responders, is very crucial. I also want to bring to the attention that some of our people who are callers at 311 and 911 are also. I am [unintelligible] wellness and maybe more [unintelligible] access to that. My neighborhood watch group had a meeting with the captain of the call center, and we were talking about this. This is another company that does security, they are a security company, they do video, and they said, Hey, sometimes, what are you guys doing? You have a weird call and it kind of affects the caller; do you guys give them a break? They said, Yeah, well, we kind of give them a break. Then I asked if they also had access to the wellness center. They said yes, but it appeared to me that they did not really have a ready access, where you have to drive down. They said something like the policeman can drive down there.

We also want to include our callers, make it easier for them to get some support. When you call in, believe me, as a neighborhood watch, a lot of weird stuff happened, and you want to

get a quick response. Sometimes it gets very, very, very heated. I do want to call that attention, and I am in total support of that.

Berry Johnston, Private Citizen, Las Vegas, Nevada:
I am here today, not just as a concerned citizen, but as someone who has watched my friends, who are cops, suffer—good cops. Some were forced to leave the state they love because of what this Legislature has done. Let me be clear: the mental health decline in our communities and in our police force is not a mystery; it is the result of your woke, soft-on-crime policies. You socialists were screaming, Defund the police, and fought for it. It is the constant demonization of our police officers who are sworn to protect and serve. You did not reform the system, you sabotaged it.

Good officers are leaving. They are moving to counties with constitutional sheriffs who respect liberty, transparency, and the rule of law. Why? Because in places like Metro, they do not trust leadership. McMahill has failed to build trust as he hides behind PR statements while morale crumbles. This bill you are proposing is another Band-Aid that looks good on paper, but it does not treat the infection. The root cause is political rot, local nightmares, like socialist Selena and her allies, who care more about ideology than public safety. It is actually funny she is the one presenting it.

A good sheriff is transparent. A good department protects constitutional officers, not pedophile sergeants who are sitting in jail right now. Our good officers are tired of corruption and cover-ups of the silence. They know it is wrong, so they leave. Until we address the real cause—your own destructive policies—Nevada will continue to suffer, and we will not be silent. We must protect the good constitutional officers, and you guys are the ones who made their lives hard.

Chair Considine:
We will now move on to testimony in opposition. Is there anyone wishing to testify in opposition to Assembly Bill 433? [There was no one.] We will move on to neutral testimony. Is there anyone wishing to testify in neutral on A.B. 433? [There was no one.]

Would the sponsor like to make any final remarks? [Assemblymember Torres-Fossett indicated in the negative.] I will now close the hearing on A.B. 433.

Before we go to public comment, we have two BDRs [bill draft requests] to introduce this morning. First, we will introduce BDR 15-394.

BDR 15-394—Revises provisions relating to utility wire. (Later introduced as Assembly Bill 503.)

I will entertain a motion to introduce BDR 15-394.

ASSEMBLYMEMBER NGUYEN MADE A MOTION TO INTRODUCE BILL DRAFT REQUEST 15-394.

ASSEMBLYMEMBER HUNT SECONDED THE MOTION.

THE MOTION PASSED UNANIMOUSLY.

Next, we will introduce BDR 28-401.

BDR 28-401—Revises provisions relating to public works. (Later introduced as Assembly Bill 502.)

I will entertain a motion to introduce BDR 28-401.

ASSEMBLYMEMBER NGUYEN MADE A MOTION TO INTRODUCE BILL DRAFT REQUEST 28-401.

ASSEMBLYMEMBER KARRIS SECONDED THE MOTION.

THE MOTION PASSED UNANIMOUSLY.

We will now move on to the last item today, which is public comment. Is there anyone wishing to provide public comment?

Al Rojas, Private Citizen, Las Vegas, Nevada:
I want to comment that I have been very successful with the neighborhood watch group; I have got a lot of volunteers. I want to bring an issue that I think might be important to help us with our security in our community. As you know, we have a lot of HOAs [homeowner's association] and I was surprised, when I came to shop for a residence here in Nevada, that many detached homes are part of an HOA. What I am saying is, one of the boundaries that is making it difficult for us to sometimes start a neighborhood watch group, because in these HOAs you have to have special permission to trespass somebody from community property. Okay? We are getting home invasions, even in HOAs with attached properties. It is hard when a person comes into our restricted HOAs and getting them out.

I am proposing that possibly we add that it is mandatory for HOAs here in the state of Nevada to have a security committee. If you have a security committee, they will grant you a document which will allow you to trespass people. It would be voluntary for anybody who wants to volunteer. You would not have to be that the HOA mandatorily has to create such a committee, if somebody wants to step up in the community and at least have some kind of jurisdiction on getting somebody out, having them trespass only on community property; a very restrictive type of committee. Every HOA would have to give that opportunity to the residents, and it would be very, very helpful.

We have a lot of HOAs coming up, we have a lot of existing; and HOAs are a big part of our development, especially down here in Clark County. Homelessness is growing. We need to start taking action and I do believe that we can do it.

Chair Considine:
We are now going into a recess so we can reconvene if any additional work comes before us today.

[The Committee recessed at 9:50 a.m. and adjourned on the Assembly floor at 1:08 p.m.]

RESPECTFULLY SUBMITTED:

_____
Nikki Peterson
Committee Secretary

APPROVED BY:

_____
Assemblymember Venicia Considine, Chair

DATE: _____

EXHIBITS

Bill	Exhibit	Witness / Agency	Description
	A		Agenda
	B		Attendance Roster
A.B. 432	C	Assemblymember Toby Yurek, Assembly District No. 19	Conceptual amendment
A.B. 432	D	Timothy Galluzi, State Chief Information Officer, Office of the Governor	PowerPoint presentation titled "Enhancing Nevada's Cybersecurity Posture: An Analysis of Assembly Bill 432"
A.B. 432	E	Kivanc Oner, Vice President for Digital Transformation and Chief Information Officer, Office of Information Technology, University of Nevada, Las Vegas	Written testimony
A.B. 433	F	Ryan Beaman, District Vice President; and Todd Ingalsbee, President, Professional Fire Fighters of Nevada	Proposed conceptual amendment