MINUTES OF THE MEETING
OF THE
ASSEMBLY COMMITTEE ON EDUCATION

Seventy-Seventh Session
March 11, 2013

The Committee on Education was called to order by Chairman Elliot T. Anderson at 3:23 p.m. on Monday, March 11, 2013, in Room 3142 of the Legislative Building, 401 South Carson Street, Carson City, Nevada. The meeting was videoconferenced to Room 4406 of the Grant Sawyer State Office Building, 555 East Washington Avenue, 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 nelis.leg.state.nv.us/77th2013. In addition, copies of the audio record may be purchased through the Legislative Counsel Bureau's Publications Office (email: publications@lcb.state.nv.us; telephone: 775-684-6835).

COMMITTEE MEMBERS PRESENT:

Assemblyman Elliot T. Anderson, Chairman
Assemblywoman Marilyn Dondero Loop, Vice Chairwoman
Assemblyman Paul Aizley
Assemblywoman Lesley E. Cohen
Assemblywoman Olivia Diaz
Assemblyman Wesley Duncan
Assemblyman Andy Eisen
Assemblywoman Michele Fiore
Assemblyman Randy Kirner
Assemblyman Harvey J. Munford
Assemblyman Lynn D. Stewart
Assemblywoman Heidi Swank
Assemblywoman Melissa Woodbury

COMMITTEE MEMBERS ABSENT:

Assemblywoman Dina Neal (excused)

GUEST LEGISLATORS PRESENT:

None

STAFF MEMBERS PRESENT:

Todd Butterworth, Committee Policy Analyst
Andrew Diss, Committee Manager
Sharon McCallen, Committee Secretary
Steven Sisneros, Committee Assistant.

OTHERS PRESENT:

Lucas Foletta, General Counsel and Policy Director, Office of the Governor
Chris Ipsen, Chief Information Security Officer, Office of Information Security, Division of Enterprise Information Technology Services, Department of Administration and member, Technological Crime Advisory Board, Office of the Attorney General
James R. Elste, representing Nevada Cyber Initiatives
Ira Victor, President, InfraGard, Sierra Nevada Members Alliance, Las Vegas, Nevada
Greg Bortolin, representing Desert Research Institute, Reno, Nevada
Tom Piechota, Vice President for Research and Dean of the Graduate College, University of Nevada, Las Vegas
Joseph Lombardo, Executive Director, National Supercomputing Center for Energy and the Environment, University of Nevada, Las Vegas

Chairman Elliot Anderson:
[Roll was called. Protocol explained.] We will begin with a subcommittee and will note, for the record, when we get a quorum. I will open the hearing on Assembly Bill 42, which establishes the Nevada Cyber Institute within the Nevada System of Higher Education (NSHE). Presenting the bill will be Lucas Folletta with the Governor's office and Mr. Christopher Ipsen.

Assembly Bill 42: Establishes the Nevada Cyber Institute within the Nevada System of Higher Education. (BDR 34-286)

Lucas Foletta, General Counsel and Policy Director, Office of the Governor:
The Governor and the Administration appreciate this opportunity to talk about, in our view, one of the most significant policy concerns confronting not only the state, but also the country. As many of you may have noticed, the issue of cybersecurity is growing in national prominence, particularly over the last several years. The federal government has begun to deal aggressively with several aspects of the problem, including workforce development, securing the nation's critical infrastructure, and the integrity of the information that flows

through not only the federal government, but also through our marketplaces in general.

The presentation you are going to hear today really reflects what the Governor views as his vision for going forward and dealing with this problem in Nevada.

Next to me is Christopher Ipsen, who is the state's Chief Information Security Officer. He has been integral in developing a vision for going forward for our state in working with, not only our office, but with the Nevada System of Higher Education (NSHE) which has been a great partner in our efforts to date.

Before we get to the elements of the bill, we will present a little background on what cybersecurity is and why we view it as an important issue. We will talk about what steps we, as a state, have taken to date under the Governor's leadership with respect to this problem. We will then lay out what we feel is a compelling vision.

Chris Ipsen, Chief Information Security Officer, Office of Information Security, Division of Enterprise Information Technology Services, Department of Administration and member, Technological Crime Advisory Board, Office of the Attorney General:

I want to say what an honor it is to be here with the Governor's office, presenting before you, and in front of the NSHE. As a cybersecurity professional, it does not get any better than this. Many days are very challenging. Oftentimes you are having to explain exactly what the challenges are. To have a venue like this is truly an honor.

I welcome the opportunity to discuss with you some of the challenges we are facing. It was not just the other day that we sat down and thought about cybersecurity. This bill is a culmination of a couple of years of effort. Before you is a general overview of what cybersecurity is. [Read from PowerPoint presentation (Exhibit C).] As we move forward through the presentation, it will be very important to note a couple of points of demarcation. First, the definition we have before you did not exist prior to 1994. It is a relatively new phenomenon. As we move further into this presentation, I hope to bring a level set as to how important technology is, and how important cybersecurity is as a subset of that innovative technology revolution we are experiencing.

A couple of examples of things that are happening right now that would have seemed implausible a year ago include smart refrigerators that can tell how much power is being used, and in some cases even monitor what is inside. There are smart scales. The Japanese have developed systems where people can stand on scales and it will assess relative health. We have smart cars that rest on smart transportation systems. Nevada was the first state to have the autonomous vehicle. It is truly a landmark, self-driving vehicle. When I first heard about it, I was tremendously concerned because things like autonomous vehicles can be managed to do something other than their intended purpose. The ramifications could be quite great. If you combine that with smart transportation systems, your first instinct is to recognize this is an opportunity, but also a challenge moving forward.

We also have major projects within the state like the health information exchange. Recently, Nevada became one of the few states to have legalized online gaming, which I believe, is absolutely critical to the economic survival of the state.

"Access to Information" [(Exhibit C), page 6] is more a discussion around what technology means to a society. The up-and-down bars are the level of penetration of high-band width connections per capita into communities and countries around the world. The dark up and down line is the socio-economic status of individuals within those communities. Taking a step back you realize that there appears to be a direct correlation, in both the impact and the pervasiveness of technologies in communities.

What is important about this slide is not what you see, but what you do not see. If you look at who is not on this scale, you will realize that technology in the Internet is more important to some societies than others. As we rely on technology more heavily, as it becomes imbedded in creating online scales and what diets we have, how we drive our vehicles, pay our bills, and game online, you realize it is becoming a fundamental component of our society. This has become so ingrained that any disruption of these services is magnified. A healthy way to look at this is to say the more a society relies on technology, the greater the reliability of that technology needs to be. What do I mean by that? If we have a technology like autonomous vehicles and 90 percent of our people drive them, it is really important the vehicles drive correctly, are safe, and do the things that we intend them to do. If the vehicle can be circumvented somehow, then that becomes a tremendous liability to society.

If you have seen a teenager lately, you know how important technology is to the generations coming up. One of the challenges we face is that kids sleep with their smart phones. This is how they communicate. This is how they do their jobs and live their lives.

A couple of the most recent incidents that really highlight the attack vectors or the significance cybersecurity can play are Flame, Stuxnet, and Duqu [(Exhibit C), page 6]. Maybe most of you have heard about Stuxnet, which is cyber warfare personified, in that it eliminated a small portion of the Iranian nuclear refinement facility. It was done through a very sophisticated attack with systems not even connected to the Internet. A year ago, that would probably not have been the case, and two or three years ago, definitely not. Targeted attacks on critical infrastructure using very specific code is the wave of the future. As we look at Duqu, we also realize some of the controllers that power the electrical grid, the water systems, and the critical infrastructure of the United States were developed prior to the understanding that they would eventually be connected or interconnected with each other. As a result, many of those systems were created with software that was relatively archaic but effective for the purpose. Now, with those systems exposed to virtually anyone in the world, over multiple communications links, the attack vector has increased, but the threat posture has remained the same. We have very vulnerable systems exposed to people in every country of the world.

In security statistics in Nevada [(Exhibit C), page 7], the numbers speak for themselves. When we are looking at firewalls in the state, we are able to assess how many connections are rejected as a result of malicious attacks or inappropriate attempts at contact internal to our network.

The perimeter firewalls to our Internet prevent or reject between 235,000 and 1 million attempts an hour. If you could have seen our presentation, "Enterprise IT Services," that we gave to the Committee on Ways and Means, you would have seen virtually a matrix display of rejects going in front of you. That number is startling, and it is growing every day.

The second statistic we are presenting is that, of those trusted partners we have, like counties and cities, we have an enterprise network that has firewalls facing them as well. We have more trusted connections with those entities. For example, if someone is receiving welfare benefits in a community, those connections usually are established through the state network and then propagate up to the federal network, so they pass through our network. We provide connectivity for them, but they are eventually passing on information to federal networks. In the months that we have been working, we have identified up to 11 million known virus attacks on our network from trusted partners.

Lastly, and this should be very alarming to you, in the last legislative session, the Attorney General proposed, the Legislature approved unanimously, and the Governor's office signed Senate Bill No. 82 of the 76th Session. That legislation required state agencies to report security incidents to the Office of Information, for which I am responsible. Approximately two years ago, the statistics were even lower than the five incidents per month. Now, with increased security capabilities and reporting, we are reporting to them, through some very sophisticated monitoring that we have and some probes on our network, a twenty-fold increase in the number of known virus attacks that have been successful internal to our network. This is over 100 per month. What that represents to us is we consume two full-time employees just to catalogue and to remediate the end points associated with those attacks. What started with five incidents a month is now 100. If we extrapolate this, it becomes completely unmanageable in about six months. Why is that significant? I believe the state network is more secure today than it was a year ago. That statistic represents the threats facing us. If you juxtapose that statistic with some of the most recent breaches, primarily in South Carolina and Utah, there have been three major breaches in just those two states alone in the last year. Those compromises are believed to have cost those two states more than $100 million. That is not soft money. That is hard money out of state coffers.

Another important consideration is that if anyone within the state is compromised, especially to a degree of $50 million, $60 million, or $100 million dollars, those costs generally are not incurred by the agency that deploys the system. Those costs are incurred by state risk management. That means the General Fund. If there is a breach, if there is a cost, we all pay for it. That is a significant factor. Couple that with the fact the state, for good reason, requires citizens to provide sometimes very personal information about their families, such as blood tests done at birth along with personal information. However, if we collect that information, then beyond the fiduciary component, there is also an ethical responsibility for us to keep that information secure and safe. Now, if we interject the health information exchange, and we look at health insurance systems, you can see that the challenge is becoming greater.

"Implications of Cybersecurity" [(Exhibit C), pages 8-9] speaks for itself. This is President Obama's most recent Executive Order that took place about a week ago. I had the honor to speak with Michael Daniel, the new cybersecurity advisor to the president, about what cybersecurity is. He wrote this particular Executive Order on behalf of the President. It is a reflection of the president's understanding that this is a priority.

General Keith Alexander, Head of the National Security Agency (NSA) and U.S. Army Cyber Command (USCYBERCOM) said, the "greatest transfer of wealth in history" has occurred as a result of cybersecurity intrusions and crime. One trillion dollars is believed to have been stolen, as well as the intellectual property of the United States. One of the things we have in our freedom of democracy is the right to invent, to create things, and to prosper as a society and civilization based upon our ideas.

In some countries, North Korea in particular, citizens are not allowed access to information. As a society, they lag behind industrialized nations. The most significant way they can catch up to us is not to invent, but to steal, information. If we make it available to them, or if we have vulnerabilities in our systems, which we clearly do, those trade secrets, fighter jet plans, weapons systems, confidential conversations and negotiations between business interests, patents, and new ideas that power our Internet society so profoundly can all be stolen and used surreptitiously. Unfortunately, they can be stolen without being seen. What we have to face is that those losses may not be apparent for years to come. We are under a very significant challenge in our society.

"Dimensions of the Problem" [(Exhibit C), page 10] focuses on the additional challenges of security and workforce development. One reason we are sitting here is that in addition to the challenges becoming greater, the workforce is insufficient. Currently, it is believed that there is a deficit of up to 40,000 in cybersecurity analysts in the United States alone—10,000 required for government and 30,000 for the private sector. What type of people are these analysts? They are sophisticated, technical cybersecurity professionals. We do not need are people who can talk about cybersecurity. We need people who can do cybersecurity. There is opportunity for our young people, both to do good things, to be intellectually challenged, and to get a job doing the things that are necessary to protect our critical infrastructure.

We also have a challenge in our state in that our systems are at risk. That should give you pause. We are at risk, and we need to apply the appropriate resources in these fiscally constrained times to make sure we maintain the survivability of our infrastructure. I am not here to alarm everyone. I have some positive things going forward, but I think it is important to understand the problem. If we ignore it, it does not go away. It gets worse. As our society uses more technology, it is going to get more challenging, and we need to do both security and workforce development as part of our discussion on homeland security and the security of our state's political infrastructure and that cybersecurity could be one of our greatest threats moving forward. I believe it is our greatest threat.

In public statements before the Nevada Homeland Security Commission, the Governor agrees that this is a unique challenge before us. To his credit, as well as yours and the university's, we want to do something about it. It is not enough to sit here and talk about it. If we talk about it we fail. If we do something about it then we have a fighting chance. That is all I am asking for.

Where has the "Prioritization of Cyber" occurred [(Exhibit C), page 11])? Prioritization has occurred by President Obama through an Executive Order, by the Department of Homeland Security and, to our credit, Mark Weatherford has come here and presented. In your packet is testimony he provided to the Nevada Technological Crime Advisory Board, [September 9, 2011, (Exhibit D), page 7]. I recommend that you read his testimony. Not only was he the deputy undersecretary, responsible for cybersecurity, he was also the chief information security officer for the North American Electric Reliability Corporation (NERC). If you are not aware of it, the power grid stretches from Mexico to Canada. We are all interconnected as a result of our power being interconnected. Prior to being the chief information security officer for NERC, he was the chief information security officer to California, and prior to that, to Colorado. Mark has a unique perspective. He came to Nevada because he believes we have a unique position in terms of our collaboration and our capabilities.

In returning to (Exhibit C), we also see prioritization by the United States Department of Defense. According to General Keith Alexander, "The loss of industrial information and intellectual property through cyber espionage constitutes the greatest transfer of wealth in history." United States companies lose about $250 billion per year through intellectual property theft, with another $114 billion lost due to cyber crime, a number that rises to $338 billion when the costs of down time due to crime are taken into account.

This year, the Department of Defense is looking to hire 3,000 cybersecurity analysts for USCYBERCOM alone. That is a significant number. They are hoping to get enough people to meet that demand. If we look at the NSA, one of the individuals we have had the opportunity to talk with is Tony Sager, the former leader of the NSA Red Teams. He concurs with this and is working closely with us on what controls matter in our computer systems infrastructure, to make sure we are deploying the important controls that lead to maximum benefit.

Hopefully that is a theme you are going to hear throughout the presentation [(Exhibit C), page 12]. Not only do we have to defend ourselves, we also have to come up with a strategy that is efficient. We cannot do all things for all people, so we have to pick and choose our battles effectively. Prioritization has occurred by the Office of the Director of National Intelligence (ODNI), and another important conversation we had was with Jim Richberg. When he worked for the Central Intelligence Agency (CIA), he chased war criminals in previous conflicts, but more importantly for the cybersecurity initiative, he was the author of the Comprehensive National Cybersecurity Initiative that President George W. Bush and President Barack Obama have carried forward. This is a comprehensive strategy that talks about what we need to be doing. Not only is he a friend of Nevada, but he has come here and met specifically with the Governor's office and also the chiefs of police within our state. He is one of the cybersecurity leads for the ODNI which is the umbrella agency for all of the intelligence organizations in the United States. It was developed after 9/11 as a way for us to communicate more effectively. As their lead, Jim came here to look at how effectively we are using our infrastructure. Some very important and profound observations on his part have become part of our initiative.

On a number of occasions we have had an opportunity to reach out to the private sector, and I have been overwhelmed by the response. People know their critical infrastructure is at risk. I can tell you without equivocation, that every proactive engagement we have had with the private sector has been met warmly and appreciatively, because they understand the risk they face. As a cybersecurity professional, I cannot tell you how heartwarming it is to have people like yourselves and the Governor listen and set priorities for cybersecurity, and also to get the same from NSHE. In recent discussions with NSHE we are beginning to see that things like the NSA Center of Academic Excellence at the University of Nevada, Las Vegas (UNLV), will be retained. These are the many entities we have worked with that have listed cybersecurity as a priority. We have also worked with Howard Schmidt, and Senator Harry Reid's office. Howard was the author of the national cybersecurity bill. We have had opportunities to influence that legislation. The ways we have actually had to leverage that are very important. We have been able to talk with federal legislators and explain to them why individuals such as returning war veterans who are nontraditional students can utilize this type of education and might not be in a conventional program, but we need to apply appropriate training resources for them to help fill the gap. We have also had presentations from Mark Weatherford, James Richberg, and Tom Kellerman, who is at the World Bank. Alan Paller, who is affiliated with the SANS Institute and is the head of the largest training organization in the world, has also presented. He came to the Technological Crime Advisory Board [December 16, 2011] [(Exhibit E), page 14] where he talked specifically about cyber education and gaming in Nevada and how we can develop training capabilities using the military, and entities like Defcon, Blackhat, Switch Communications Group, LLC, and all of the other partners we have in this state to solidify our unique position in the world.

We have also spoken with Robert Brese who is the chief information officer of the U.S. Department of Energy (DOE). Energy plays a big role in this state. When it was a nuclear test site and when it was a nuclear repository, it clearly had a role. As a conduit to other states and as part of a partnering program, UNLV is the home for a DOE supercomputing facility. Joe Lombardo and I have worked collaboratively to come up with ways to communicate.

Lucas Foletta:
I would like to point out what the Governor has done specifically to move this issue forward in our state. The implications of the cybersecurity problem are very significant and the Governor takes this as a very serious responsibility, in part for the protection of critical infrastructure in the state such as utilities and water systems. He chairs the Nevada Commission on Homeland Security, which has some operational responsibility. It also has the responsibility to oversee the work of the information technology (IT) professionals within state government to ensure the integrity of the information that citizens give us, whether it be through the Department of Health and Human Services or through the Employment Security Division or any other of the ways we receive and are responsible for citizens' information.

On a national scale, the Governor has advocated for and worked on this issue through his recent appointment to the Council of Governors, which is a ten-governor council that advises the President on national security issues as they affect state governments. He is also the vice chair of the National Governors' Association Health and Homeland Security Committee. The chair of that committee is Governor Martin O'Malley of Maryland. Maryland is a state that is very engaged on the cybersecurity front. Our Governor has worked with Governor O'Malley to help come up with best practices that states can roll out on a state-by-state basis to ensure the integrity of the information they hold.

On a more local level, the Governor has made this a priority in his chairmanship of the Nevada Commission on Homeland Security. It is his number one priority. That affects the distribution of federal Department of Homeland Security dollars and the appropriation of that money to various projects.

The Governor has also directed the state's IT organization to undertake at least a partial consolidation of the state's IT infrastructure, which is an effort to make intrusions less likely with respect to those elements that are consolidated. It makes monitoring of the state's network easier. He has also directed Mr. Ipsen and his staff to implement, to the extent possible, something called the four controls. Essentially, these are controls put into place to ensure that our internal systems are as safe as they can possibly be from intrusions and viruses.

The Governor has also made development of cybersecurity professionals an important part of his economic development plan. When the state changed its economic development apparatus a couple of years ago, we looked at a number of studies to identify green patches of potential development. One of the areas within the technology space was cybersecurity. That was identified as a place the state could grow for economic development purposes by the Brookings

Institution/SRI ["Unify, Regionalize, Diversify: An Economic Development Agenda for Nevada," Metropolitan Policy Program at Brookings, Brookings Mountain West, and SRI International, November 14, 2011]. It was followed up on and endorsed by the Governor's Office of Economic Development. That has led to a number of engagements that people from economic development can tell you more about. It really is a reflection of what the Governor views as probably the greatest opportunity for the state in this area. There are obviously a number of things we have to do to make sure the people in our state are safe. There are other things we can do to benefit from helping to solve this problem, from an economic development perspective.

Chris Ipsen:
On pages 16-17 (Exhibit C) we have several quotes regarding cybersecurity employment. Quoting Alan Paller, "We do not need people who can talk about security, we need people who can do security." That is an important distinction. There are plenty of people who can check boxes and evaluate environments objectively. Very few people can look at what is happening and make intelligent decisions about how to rectify it. It is a highly technical field. Some of those people are unstructured learners.

Secondly, Mark Weatherford, "I presented workforce development and had never found one entity that could find all of the technical cybersecurity personnel that they need." In all of the presentations he has done as deputy undersecretary, he will go to a room and ask in a room of 200 people, "How many of you have all of the people you need?" Not one person has ever raised their hand and said they had enough and were okay.

Last, Tom Kellerman said, "The Government needs to hire at least 10,000 experts in the near future, and the private sector needs four times that number." That was just a couple of days ago in *The Washington Post*.

How do we do this efficiently (page 18)? In technology it is very frustrating when I see things developed in silos, where one person does it one way and another person does another way. There is only so much money to go around. The concept of united we stand, divided we fall really holds true for two reasons. One is limited resources. Two, there are not enough people to go around. Even if we wanted to hire people in all of these silos, we could not find them. It is important for us to think globally and look at all of the partners and leverage the needs of all of the interactive entities to make sure the global needs of the state are met. Efficient use of state resources is critical.

To that end, we have seen a strong interest from education, and that is encouraging. When we say education we mean higher education, the community colleges, and also kindergarten through twelfth grade (K-12). As with the education committee, I have spoken with Clark County and representatives within Washoe County about their strong interest in training students in ethical ways to use cybersecurity as a means.

The NSA Center of Academic Excellence has done a full program around cybersecurity excellence, and UNLV is one of the few entities in the United States that retains current certification. As we proceed forward with online gaming, it is imperative that we do it with assurance. If people can "game" the system, for lack of a better word, then they can ruin the reputation of the system, and they can steal money. Nevada has a tight regulatory regime and very strict requirements, and there is huge play for online gaming.

Nellis Air Force Base in the southern part of the state is home to some of the Air Force Red Teams. In the northern part of the state, autonomous vehicles are flown from Fallon, as well as from Creech Air Force Base in the south. Also, there are training programs in the National Guard. If there is an emergency or a large event, we are going to need effective coordination of all of the resources to make sure that if the electricity or water services are interrupted, we have all resources identified and engaged.

We also have conferences in the state. This is one of those interesting things about Nevada. There is a sensibility about risks. The two largest hacker conferences in the world are held in Las Vegas. One is Blackhat and the other is Defcon, and they sprang from a grassroots engagement. Last year I attended both of their executive forums, and I can assure you more than 15,000 people attended them, and probably half were from law enforcement and the other half were people law enforcement was looking at. There were very interesting, cutting-edge discussions regarding the risks of all of the technologies we have. They are here in Nevada. Why do we not utilize them?

Also we have bandwidth, and if you are familiar with Switch Communications Group, LLC, you know it is significant. As entities use the Internet to move forward, then we have an opportunity to position ourselves in the secure platform.

We have talked about autonomous vehicles, and we were the first state to legalize them. Why not leverage that?

If you go to Las Vegas, there are weekly IBM, Oracle, Symantec, McAfee, and other technical trade conferences. All of them are bringing people to the state. We can effectively leverage that. Alan Paller's presentation [(Exhibit E), page 14] talks about that. We should utilize that as a teaching opportunity as we cycle people through the state; leverage their training toward training of our people.

It is an important concept to engage nontraditional students. You realize some of the best people in cybersecurity do not specialize in building things, they specialize in breaking things. They are not all malicious individuals. If they are really good at breaking things, then we can use that to find the flaws in our systems. Why do we not use that? We actually used a person from this area named Teague Newman, who was on the cover of *Wired* magazine. He found a vulnerability in logic controllers in jails. How many of you think it would be a really bad idea if a criminal organization could inject a virus into a prison and release all of the prisoners at one time? Mr. Newman found a vulnerability that if delivered appropriately, could do that. He trains all over the world and he has offered to train in Nevada. These are the nontraditional people we need to capture.

"Who Should be Involved?" [(Exhibit E), page 20] brings together the private sector, gaming, communications, energy and utility providers, and businesses of all sizes. When we present legislation, oftentimes the people who speak up the most are the small business owners. They say they have no idea what we are talking about and ask how they can do this, and what are the ramifications to them? If we can build the capability for them, they can prosper in our state and become medium businesses, then large businesses.

In the public sector—state, county, and municipal governments—there are the haves and the have-nots in government. The citizens expect the same level of service at all levels. We have a responsibility to help share the expertise with our rural counties and our smaller communities, as well as some of our large communities.

Education has the capability to deliver the message and develop systems of education. Either through conventional or nonconventional means, there is a discrete position for the universities, the community colleges, and K-12. There are very fun programs being developed, one of which I just heard about from Facebook, a competition called "Hacktoberfest." It is described as the gamification of security awareness. They dress up in costumes, run around the company, and see if they can find ways to compromise their cohorts. This is what you would expect from Facebook, a whole mindset around cybersecurity and making it more palatable. I discussed this with folks from the Department of Transportation (NDOT) the other day. They were excited, and I was excited that they were excited about it.

Last, but not least on the list are military and federal partners. We are the conduit to the federal government, and the military sees this as a critical strategy. We need to be able to partner effectively with them.

Lucas Foletta:
That brings us to the bill itself. We have just heard the fast and furious ride through the issue of cybersecurity. This gives you a feel for why the administration thinks it is an important issue that we grapple with as a state. The bill in front of you is an effort to reflect one approach to going forward in terms of embracing the opportunity we have as a state to not only solve an important problem for the state and the country, but also to benefit through the contribution to the development of a very high-end set of professionals. They are clearly in high demand.

The bill, section by section, is not that intriguing, and in some ways a lot of this work is already being done in various parts of the higher education system. I know we have representatives here from the Desert Research Institute (DRI), and UNLV, and NSHE who can tell you in more detail what they are doing through various programs. It is our understanding and hope that we are going to continue the conversation with them on a parallel track about how we can perhaps bring some of those programs together to put together a potentially very compelling proposal for the Knowledge Fund. The type of work the higher education system is doing in this area really reflects part of the reason why we have the Knowledge Fund and although this is not the subject of this hearing, it is relevant.

We can go through the bill section by section or simply take questions on the background as it relates to all of this.

Chairman Elliot Anderson:
We will just talk about the overall alignment of our educational system with key growth potential. This being, obviously as Mr. Ipsen discussed, a key area where we need to develop a workforce.

Does the Committee have any questions about what the state is doing to diversify the economy and align our educational programs with our workforce?

Assemblyman Stewart:
Will the actual institute be housed at UNLV? Will staff be hired there? How is UNLV to carry this out, or will it be dispersed among the DRI and other institutions as well?

Lucas Foletta:
The bill does reflect the Institute that is associated with the higher education system, not dissimilar to the way that the DRI is associated with the system. That said, there are a number of programs that are being developed and have been developed in the higher education system over the last couple of years that may render the need to formalize the approach through legislation unnecessary. But the bill does reflect a DRI-like institution being associated with the system as a whole.

Assemblyman Stewart:
Do you envision a separate facility like DRI has, or offices at UNLV where they would hire staff to come in to coordinate all of this cyberspace activity that is going on?

Lucas Foletta:
If the bill were to move forward, I would think there would be an investment of facilities and a coherent approach to looking at these issues from a research and practical perspective.

Assemblyman Aizley:
I agree with the need for the cybersecurity personnel and the workforce development, but I do not agree with any of the process in this bill for creating the programs through higher education. If you are suggesting that we have another campus of NSHE, with a president and others, more faculty, and grant writing, it is a pretty large issue to bring up. I would not do it this way in the bill. It should be given to the campuses. Somewhere, the courses, the program, and the degree have to be defined. You have the Board of Regents defining courses. The Regents do not define courses, they approve them. This has to be done through faculty development and not through a legislative bill.

Chairman Elliot Anderson:
The question I have is regarding our workforce needs. We are talking about getting into online gaming and a number of other things, and certainly our lives go more online all the time with things like iPhones. How big a need is there in our workforce? How many positions do you think we could develop in this sector?

Lucas Foletta:
I think the numbers referred to earlier are pretty compelling. There is another statistic that says there is one qualified cybersecurity professional for every five cybersecurity jobs. We would have difficulty saturating this market. Whatever extent we invest in producing workers in the area, the sky is the limit.

There is no indication that the need for cybersecurity professionals is plateauing by any means, and all indications are that the need for cybersecurity professionals is only going to grow exponentially over the next several decades. It is difficult to quantify exactly what we can achieve, but I am confident that to whatever extent we invest in this area, we will see returns.

Christopher Ipsen:
I echo Mr. Foletta's comments. First of all, I would like to applaud the university's work in this area. That is important. One of the constraints is how do we do it well? If we train the wrong kind of people, it does not work. If we train the right kind of people, it will work. I think using the university is dead on. There are also opportunities for virtual outreach to other people throughout the United States, and we can use other means in the private sector to bring those individuals in who have expertise. For example, at Switch Communications in one of our meetings at UNLV, the chief technology officer talked about an intercloud exchange. Having a cybersecurity instructor in cloud technologies is really valuable. Partnering with an entity to bring someone in to work and also teach is a really innovative approach. I do not know how that works within the university system if they do not have Ph.D. or a master's degree, but I think there is an opportunity there.

Assemblyman Kirner:
I agree with my colleague's comment about how you get a program started at UNLV or the university system. My question is, are we in the embryo stage, or is work already being done in this area at the university? Are we just now trying to formalize and expand on it?

Lucas Foletta:
No, there has been some significant work done. In fact, UNLV has made some impressive strides in this area over the past several years. Something UNLV had was called the School of Informatics which was identified by the NSA as a Center of Academic Excellence in that area. Informatics is a similar term for cybersecurity. I do think that continuing to expand our efforts in this area is important. No one anywhere is meeting the workforce demand that exists. The bill before you is really just a jumping-off point and offers ways to potentially tie some of this together going forward.

Chairman Elliot Anderson:
I did want to hear this bill just so we could talk about education as an economic development piece. It is important that all of us are thinking that way, not just in higher education but also in K-12. The work we are doing in this Committee is very important so we can diversify our economy and continue the work we

began last session with Assembly Bill No. 449 of the 76th Session. Is there support in Carson City or in Las Vegas?

James R. Elste, representing Nevada Cyber Initiatives:
We are a group of technology professionals, entrepreneurs, and organizations based in Nevada. We are interested in seeing the advancement of the information technology industry and legislative agenda for cyber in Nevada.

I am here to speak in support of A.B. 42 as a subject matter expert in information security or cybersecurity. I am the former Chief Information Security Officer for the State of Nevada, the former director of information security for International Gaming Technology (IGT), and I am also the former director of security strategy for Symantec, the world's largest security company. I have a background in information and cybersecurity that spans over 20 years professionally. My background includes an education and a master's degree from Norwich University, our country's oldest private military academy, in a program that was an NSA Center of Academic Excellence in Information Assurance Education that was specially designed to cover cybersecurity.

There are two considerations I would like to present to the Committee today regarding the establishment of the Cyber Institute. First of all, as previously pointed out, cybersecurity is a complex issue. I can assure you that the threats are evolving very quickly, and there is a need to create effective counter measures because the risks associated with cybersecurity are so enormous. These risks affect our nation, our state, our economy, and our way of life. That is not hyperbole. That is actual fact.

There is a critical need for advanced cybersecurity professionals. For those advanced cybersecurity professionals to share their expertise in education and experience with developing cyber professionals. I use the word "professional" intentionally, because cybersecurity is a profession and one that requires a multidisciplinary approach with a focus on technology to produce experts in this field. I would try to dissuade you from considering the Cyber Institute as a trade school or a purely academic exercise in technology. I view the Cyber Institute as akin to a medical or law school where individuals with interest in those professional fields are afforded the opportunity to develop skills that they can apply practically as professionals once they leave those institutions. The same way a medical professional goes through a premedical education, medical school education, then a three-year residency to develop their skills; we have an opportunity to develop programs that mirror that for cybersecurity professionals. At the end of the day, what it takes to become a cybersecurity professional is a significant intellectual investment in a very specialized field that is highly technical. It involves doing things like threat analysis, creating new and innovative countermeasures, evaluating the risks associated with the use of technology and how to mitigate those risks, and responding to incidents or performing forensics.

Assembly Bill 42 and the Cyber Institute proposed in that bill provide an ideal vehicle for Nevada to develop an effective cybersecurity program that would allow us to develop highly skilled professionals, support the state from an economic development perspective, and support the need across the public and private sector for these types of professionals.

Chairman Elliot Anderson:
Are there any questions?

Assemblywoman Diaz:
With your knowledge in this area, how as a country, nation, or state did we drop the ball in terms of planning ahead to have professionals in this area? Everything has continually gone to electronic databases and means, and we have gotten rid of a lot of paper, so why are we now suddenly seeing that we forgot that aspect? Why are we so behind?

James Elste:
We have fallen behind for a couple of reasons. It is not through an intentional oversight where we simply ignored the security interest of these systems. Technology evolves very quickly, and the adoption of technology in businesses in the public and private sector tends to focus more on the value of that technology without necessarily considering the implications of risk. What we have discovered is that the implementation of the technology has left out considerations for security and put us at risk. I will give you a prime example of that. The Stuxnet malware that was mentioned earlier, was arguably one of the first instances of cyber warfare that includes a piece of malware being written specifically to cause damage in the physical world. It took advantage of vulnerabilities in industrial control systems. Those specific vulnerabilities were, among other things, hard-coded passwords that did not change, which is now considered to be a very bad practice. That was baked into the system when it was implemented and it is very difficult after something has been implemented to go back and retrofit it to improve security.

The other half of the question is how do we get ahead of the curve? The risks are significant. When you look at the type of risks we are exposed to in critical infrastructure, quite frankly, every time the lights turn on, I am very relieved. When the lights do go out, I wonder if they are going to come back on. The system is fragile and is not designed to be resilient or prevent these attacks from causing significant damage. In part, it is in recognition of the risks.

The other part is an investment in addressing these security challenges and trying to resolve some of the vulnerabilities, or produce countermeasures. To do that, and fundamentally to this bill, we need people with expertise in this field that are focused on it professionally.

There are some very interesting educational programs in our university system. There are programs focused on computer science and when you look at those, they include interesting avenues for academic pursuit such as artificial intelligence, gaming theory, or control systems. Things that if you had a choice as a student you might pursue in preference to something like security, which is not necessarily the most glamorous pursuit. We do not currently have in any of our universities a program that is focused specifically on cybersecurity. We have a significant problem, a problem that is part of the speed of evolution of technology and the adoption of that technology, and we have a gap or a vacuum in terms of the professional experts that can address that problem. It is a very critical need.

Assemblyman Stewart:
Are there other states developing these kind of institutes, or are we breaking ground here?

James Elste:
There are a variety of initiatives to develop advanced cybersecurity programs in different states. There are a number of academic programs in universities such as Purdue and Carnegie Mellon that have been recognized as leading in the cybersecurity arena. There are a number of private sector initiatives to develop training programs for cybersecurity professionals. I believe we have a unique opportunity for Nevada to demonstrate leadership in this arena. Where those programs have focused on either strictly academic pursuits or more of a trade school or certification model, what is being proposed in the Cyber Institute is an advanced education program for cybersecurity. While we would not necessarily be the first or only in that pursuit, we would be in the leadership, or the leading echelon of organizations to do that.

Ira Victor, President, InfraGard Sierra Nevada Members Alliance, Las Vegas, Nevada:
InfraGard Sierra Nevada is a program of the Federal Bureau of Investigation (FBI), a private sector program that helps promote protection of critical infrastructure, specifically focused on cyberspace. For the record, I am not an FBI agent, nor are members of our board. However, we do work with the FBI to help protect critical infrastructure.

I want to echo the words of James Elste. We are in support of this legislation. We think the amount of attention that is being paid to this issue is phenomenally important. For a long time, people like me, who have worked in the field and in the trenches every day since the 1990s as information security professionals, have been lone wolves wondering when people were going to take this problem seriously. It is refreshing and exciting to see Nevada taking it seriously both at the state level and in the private sector. We have an opportunity in Nevada to be leaders with the Cyber Institute.

I also want to echo the statements of Dr. Alan Paller regarding the high need for professionals in this field. Dr. Paller recently released an email in a newsletter by the SANS Technology Institute, where he said that professionals in cybersecurity, more specifically, in the field of digital forensics, and in the response to breaches which is the area I specialize in, are now commanding $1,000 an hour for our services. Those jobs are going unfilled. Imagine how great it would be if Nevadans were being trained, and were filling the roles of those high-paid professionals right here. I have seen the testimony and heard the questions from members of the Committee, and I want to assure you as someone who is a professional in the field, the demand is immense. A recent study by the Ponemon Institute, which studies private sector trends, also echoed how severe the shortage is for professionals when there is a cybersecurity breach. The companies that experience cybersecurity breaches are woefully unprepared, and do not have the professionals in place to find out what happened and prevent it from happening again. The demand is authentic, especially in the area of digital forensics and in responding to breaches.

I also wish to echo Mr. Elste's comments regarding the need to have this program oriented toward training professionals very much like we do in the medical community. Some of the best medical care you can receive is at a teaching hospital. A teaching hospital is not literally a place where doctors are taught the academic part of medicine; it is where they get hands-on experience working with the best medical professionals on staff, or more importantly, the best medical professionals who come through the hospital. There could be a specialist in cardiac matters, or a specialist in cataracts. These experts come to these teaching hospitals to treat patients and to teach professionals. This is the type of model that Dr. Alan Paller spoke of, and that I think is so important for us to model in Nevada. That would make us one of the leaders in the United States.

In summary, I want to reiterate that InfraGard Sierra Nevada is in support. We want to be available as experts in the field to help the people who are putting this together.

Assemblyman Aizley:
I am impressed by the notion of a medical or law school-like program, so then we have to ask: How many faculty and departments are you going to have? Are you going to have a paracyber person or systems cyber person? Are you going to give master's degrees? How many courses and how many credits? When the university decided to have the medical school, it was a completely new program brought to the campus. That was not done so much by the faculty, but the faculty would be consulted before it would be done. There is biology that is related to medicine; is computer science related to what you are doing? Or mathematics or physics? You made the need very clear, but the structure of how to get there is not at all clear. Again, I do not like the bill.

Ira Victor:
I am not sure if there is a question there. We are not the author of the exact bill. I would like to address the general concern, if I may. As president of InfraGard Sierra Nevada, we offer our support as subject matter experts to the Committee or those who are involved in the bill, to help shape this in the way that you, sir, on the Education Committee, and others wish to have this program. The goal still remains the same. We are here to help achieve that goal, regardless of how we get there.

Chairman Elliot Anderson:
Seeing no more questions, is there anyone in opposition in Carson City or in Las Vegas? [There was no one.] Is there anyone neutral?

Greg Bortolin, representing Desert Research Institute, Reno, Nevada:
I will keep my comments to how Desert Research Institute (DRI) is applied to this discussion. [Read from Cyber Fact Sheet (Exhibit F).]

Tom Piechota, Vice President for Research and Dean of the Graduate College, University of Nevada, Las Vegas:
I want to thank the Governor's office and the Office of Information Technology for the background information. I am going to take this opportunity to talk to you about the activities at the University of Nevada, Las Vegas related to cybersecurity and, broadly, information technology as it is relevant in this discussion. We take this very seriously in terms of our academic and research mission. [Read from prepared testimony (Exhibit G).]

Joseph Lombardo, Executive Director, National Supercomputing Center for Energy and the Environment, University of Nevada, Las Vegas:
I would like to begin by giving you some background on the National Supercomputing Center. We provide high-performance computing, storage, and networking resources for research and development programs requiring

collaborations at the state, national, and international levels. [Read from prepared testimony (Exhibit H).]

Chairman Elliot Anderson:
Do we have any questions for either of our witnesses? [There were none.] Mr. Foletta, do you have any concluding remarks?

Joseph Lombardo:
No, Mr. Chairman. I thank you and the Committee for the time you have given us this afternoon.

Chairman Elliot Anderson:
Thank you, Mr. Foletta, for your efforts in economic development. It is important for our Committee to have that conversation as we need to know what the end goal is and what we are doing. The end goal really is to grow an economy and make sure people have the tools to participate in the workforce.

I will close the hearing on Assembly Bill 42 and open up for public comment either here in Carson City or in Las Vegas. Seeing none, the meeting is adjourned [at 4:49 p.m.].

RESPECTFULLY SUBMITTED:

____
Sharon McCallen
Committee Secretary

APPROVED BY:

____
Assemblyman Elliot T. Anderson, Chairman

DATE: __________________________

EXHIBITS

Committee Name: Committee on Education

Date: March 11, 2013 **Time of Meeting: 3:23 p.m.**

Bill	Exhibit	Witness / Agency	Description
	A		Agenda
	B		Attendance Roster
A.B. 42	C	Chris Ipsen	PowerPoint
A.B. 42	D	Chris Ipsen	Minutes of the Nevada Technological Crime Advisory Board,
A.B. 42	E	Chris Ipsen	Minutes of the Nevada Technological Crime Advisory Board
A.B. 42	F	Greg Bortolin	Cyber Fact Sheet
A.B. 42	G	Tom Piechota, Vice President for Research at the University of Nevada, Las Vegas	Prepared Testimony
A.B. 42	H	Joseph Lombardo	Prepared Testimony