Minutes of the
Technological Crime Advisory Board

March 12, 2013

The Technological Crime Advisory Board was called to order at 2:02 PM on Tuesday, March 12, 2013. Attorney General Catherine Cortez Masto, Chairman, presided in Room 4401 of the Grant Sawyer Building, Las Vegas, Nevada and via videoconference in the Main Courtroom of the Attorney General's Office, Carson City, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Tray Abney, Reno/Sparks Chamber of Commerce
Professor Hal Berghel, University of Nevada, Las Vegas
Dennis Cobb**,** Co-Director of the UNLV Identity Theft and Financial Fraud Research & Operations Center.
James Owen**,** Deputy Chief, LVMPD, *meeting designee for Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)*
Darin Balaam, Captain, Washoe County Sheriff's Office, *meeting designee for Mike Haley, Washoe County Sheriff's Office*
David Gustafson, State Chief Information Officer, Enterprise IT Services
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association
Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)
Resident Agent in Charge Kyle Burns, Homeland Security Investigations

ADVISORY BOARD MEMBERS ABSENT:

Nevada State Assemblywoman Irene Bustamante Adams
Nevada State Senator Aaron Ford
Daniel Bogden, U.S. Attorney, Department of Justice (DOJ)

TASK FORCE MEMBERS PRESENT:

Dennis Carry, Washoe County Sheriff's Office (WCSO)

STAFF MEMBERS PRESENT:

Belinda A. Suwe, Interim Executive Director

Henna Rasul, Deputy Attorney General

OTHERS PRESENT:

Christopher Ipsen, Enterprise IT Services
James Elste, Nevada Cyber Initiatives
Ira Victor, Infraguard
Edie Cartwright, Nevada AGO

Agenda Item 1 – Call to Order – Verification of Quorum.

AG CORTEZ MASTO:
Good afternoon. We have relocated to my office in the north and the legislators will be unable to join us because the legislature is in session. The first item on the agenda is a call to order and the verification of the quorum.

The Technological Crime Advisory Board was called to order and a roll call of the Advisory Board verified the presence of a quorum.

Agenda Item 2 – Discussion and Approval of Minutes from December 12, 2013.

AG CORTEZ MASTO:
The next item on the agenda is the approval of minutes from the March 12, 2013 meeting. A copy of the minutes was provided ahead of time. Please take a look at the minutes, and I'll open it to any discussion or a motion. Is there a motion to approve the minutes?

Motion to approve the minutes was made by Mr. Uffelman and seconded by Dr. Berghel.

The motion to approve the minutes was approved with nine votes. Mr. Cobb abstained.

Agenda Item 3 – Introduction of New Members.

AG CORTEZ MASTO:
We have a new Senator, Aaron Ford, who unfortunately could not be here because he is currently in session at the legislature.

We also have two other new members who I'd like to introduce you to. The first is Dennis Cobb who I had the opportunity of working with when he was with Las Vegas Metropolitan Police Department. We always talked about inoperability as the issue of the day and believe it or not, it still is. Dennis Cobb is retired from the Las Vegas Metropolitan Police Department as Deputy Chief and now president of DCC Group, Inc. assisting public and private organizations with critical communications technology, processes and capabilities. Dennis is a founding participant in the UNLV/LVMPD Identity Theft and Financial Fraud Research & Operations Center. Dennis, thank you for joining us, we appreciate you being here.

DENNIS COBB:
I'm honored to be here, thank you.

AG CORTEZ MASTO:
Our next new member is Special Agent Burns who currently serves as the Resident Agent in Charge for U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) in Reno, NV with direct oversight of HSI's investigative and enforcement initiatives and operations in both Northern Nevada and Eastern California targeting cross-border criminal organizations that seek to exploit America's legitimate travel, trade, financial and immigration systems. Special Agent Burns is 15 year law enforcement professional. Special Agent, thank you so much for joining us.

SPECIAL AGENT BURNS:
My pleasure, thank you.

Agenda Item 4 – Public Comments.

AG CORTEZ MASTO:
This is the time for public comments. There will be two opportunities for public comment, and this is the first time for the public to address the board. Are there any members of the public here in Southern Nevada who would like to address the board at this time? Seeing and hearing none, is there any member of the public in Carson City who would like to address the board at this time?

DAVID GUSTOFSON:
No, Madam Chair.

AG CORTEZ MASTO:
Seeing and hearing none, we will move on.

Agenda Item 5 – Election of Vice Chair.

AG CORTEZ MASTO:
Traditionally, the vice chair has been one of our legislators. It is my understanding that, although she can't be here, Assemblywoman Bustamante Adams has expressed an interest in being the vice chair. I'm going to open up to discussion for nominations or thoughts about a potential vice chair.

Motion to elect Assemblywoman Bustamante Adams as vice chair was made by Mr. Uffelman and seconded by Mr. Cobb.

The motion to elect Assemblywoman Bustamante Adams as vice chair was approved unanimously.

AG CORTEZ MASTO:
Assemblywoman Bustamate Adams is our new vice chair, then. It is my understanding she will serve one year, is that right Belinda?

MS. SUWE:
Yes, that is correct.

Agenda Item 6 – Discussion and review to confirm selection of Belinda A. Suwe, Interim Executive Director, for Executive Director position.

AG CORTEZ MASTO:
Last meeting, we were able to interview some fantastic candidates; however, we did not have a quorum to actually move forward with the selection process. We decided to appoint Belinda Suwe as the Interim Executive Director and then bring her back to next board meeting that has quorum for the board members to vote to confirm her selection. Henna?

MS. RASUL:
Thank you General Masto, I had an opportunity to speak with Harry Ward, Deputy Attorney General, who attended the last meeting regarding this unique situation. NRS 205A.070 states that the Executive Director can only be elected when there are 2/3 of the board members approving her as appointed to that position. Today, because we have 10 members present for quorum, 2/3 of the members will be 7. So, we will need at

least 7 members to vote in favor of selecting Belinda Suwe as the official Executive Director.

AG CORTEZ MASTO:
Are there any members that believe that they cannot vote on this particular item under the belief that as a representative of a federal agency they cannot vote on administrative matters? Hearing none, Henna, are you comfortable with that?

MS. RASUL:
Great, I'm very comfortable with that. It's just for this limited circumstance I would highly recommend that everyone participate, if they can.

AG CORTEZ MASTO:
Great, thank you. For those members that were not at the last meeting, you have been provided minutes of the last meeting and the resumes of the candidates including Belinda's. I'd like to open it up for discussion or a motion for selecting Belinda as the Executive Director. I will tell you, from my perspective, during the interview, Belinda was the outstanding candidate. I think she will do an incredible job as the Executive Director. Just working with her over the past couple of months, she has done a fantastic job. I will open it up for further discussion or comments. Anyone else?

MR. COBB:
Looking at her resume, Belinda is highly qualified for what I understand this position to be.

AG CORTEZ MASTO:
Thank you, any other members?

DR. BERGHEL:
Since we thoroughly interviewed the candidates last time and we came to a consensus, I will move that we approve Belinda as our new Executive Director.

> *Motion to approve Belinda Suwe as the Executive Director of the board was made by Dr. Berghel and seconded by Deputy Owens.*
>
> *The motion to approve Belinda Suwe as the Executive Director of the board was approved unanimously.*

AG CORTEZ MASTO:

Belinda, welcome aboard, thank you so much.

MS. SUWE:
Thank you very much Madam Chair and board members.

Agenda Item 7 – Reports regarding Task force and Board member agency activities.

AG CORTEZ MASTO:
Are there any agencies that would like to report to the board?

SAC SHIELDS:
I'd like to give an update for fiscal year 2012 for the Electronic Crimes Task Force. It's been a very successful year. To give you an idea of the amount of work we handle, our office of the Electronic Crimes Task Force, when compared to other offices of the secret service as far as the amount of exams processed, is ranked 2 out of 26 with 143 exams. As far as terabytes we ranked 3 out of 26 federal offices with 31.2 terabytes. To give you an idea of how much data that is, the size of the Library of Congress is about 10 terabytes, so it's quite an accomplishment. In addition, with the assistance of our law enforcement partners, which include LVMPD, Henderson Police Department, the Attorney General's Office, DMV in North Las Vegas, Reno Police Department, Sparks Police Department, and Washoe County, we investigated an additional 14.11 terabytes. So, we are doing very well as compared to the rest of the field offices in the Electronic Crimes Task Force.

In addition to that, I participated in the operation black market which is an online investigation involving identity theft and trafficking credit cards. We investigated four people and rounded up 23 domestic and one international offenders. We were able to do 16 seizures over 1 million dollars and in that case alone 8 terabytes of forensic examinations.

So far in 2013, we've had 31 exams of 4.2 terabytes and with our law enforcement partners, they've already contributed 135 exams with 7.69 terabytes.

AG Cortez Masto:
Thank you, based on your experience in the field, are there threats to our cyber security, and are we prepared for it?

SAC Shields:

Yes, we'll be prepared to combat that. With the task force mentality we're able to push capacity with the help of our partners.

AG Cortez Masto:
And how does the sequester impact your agency?

SAC Shields:
We're still taking sequestration day by day with 84 million cut from our budget.

AG Cortez Masto
That's just out of your budget here in Nevada?

SAC Shields:
That's for the U.S. Secret Service.

AG Cortez Masto:
Thank you, any follow up questions or comments? Thank you. Any other task force members?

MR. BALAAM
Our northern Nevada task force with the child pornography and fraud cases has been extremely busy getting both arrest warrants and search warrants. We're seeing numerous cases of child pornography sex offenders reoffending. One of them we recently arrested is charged with sexual assault of 2 people, one being 8 years old. He was a previously convicted sex offender. Two others charged were also previously convicted sex offenders that had new child pornography crimes. And one of the trends we've been seeing is predators are learning how to change their techniques and we're trying to keep up, but it's here to stay and it's growing, and we're trying to keep pace with them.

AG Cortez Masto:
My investigator that works with you on the task force was telling me that the explosion of this means more time spent just on the child pornography issue, which is very scary.

MR. BALAAM
Yes, absolutely.

AG Cortez Masto:

Any questions, thoughts, or comments on this? Thank you. Anyone else from the task force? Thank you.

Agenda Item 8 – Report by Ira Victor, Director, Forensics and Compliance Practice Data Clone Labs, Inc., President, Sierra Nevada InfraGard, A Program of the FBI, Discussion of President Obama's Executive Order on Cyber Security.

AG Cortez Masto:
Ira, welcome to the Technological Crime Advisory Board.

MR. VICTOR:
Thank you, Madam Chair and members of the committee for allowing me the time to talk today about the President's Executive Order on Cyber Security. It is an eight page Executive Order. I'm going to go over some highlights that I think are important for everyone to know and add some of my analysis and how we can benefit here in Nevada from this initiative and the steps that we can take to implement it and build upon it to make Nevada a leader in the area of information security and fighting cybercrime.

Let's start with a couple of items from the Executive Order. The first important item is that the executive order designates cyber security as one of the President's key management priorities and establishes performance metrics around it. As someone who has worked in the field of information security and digital forensics for quite some time, it's interesting how just in the past six months the level of awareness of non-technical people and non-security people has increased in the importance of information security. I think that is reflected in the President's Order and illustrates that this awareness has risen all the way up to the President. People who I never thought would ask about this topic are now asking about it, including those in Nevada. We can take some pride in that and lots of people in this room have been working very hard on cyber security and awareness, and I think we can take advantage of that to make Nevada a leader in the area.

Another area that is important in the President's Order is a framework for intelligence gathering about cyber-attacks and cyber threats on privately owned networks in different sectors and especially talking about critical infrastructure. There's a lot of talk about critical infrastructure in the executive order and that's an area that I'm familiar with because of InfraGard, the program of the FBI that I'm president of here in Northern Nevada, the Sierra Nevada InfraGard. Our mission is to help protect the nation's critical infrastructure. Critical infrastructure is defined in the order as systems, assets, physical or virtual, that are so vital to the U.S. that the incapacity or destruction of these systems

or assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters. These are really the pillars of our economy and nation that the President's Order wants the federal government and private sector to focus on. One element of that is the information sharing between public sector and private sector on threats to those pillars.

Continuing on, it's significant that the President's Order focuses on incident response. That's a concern that security professionals know right away and laypeople or non-technical people may not. To illustrate this concept, we know what first responders are in the physical world, and those are incident response people. And that, specifically, is an area where not just in Nevada, but all over the country, where there are huge gaps in the preparation of organizations. To continue with a slightly different analogy, there was the Hilton fire in Las Vegas. We can't think about putting in the fire sprinklers and emergency exits when you see smoke. That's too late. So incident response is about doing the planning to say we know we're going to have an incident, and what are the plans and preparations both from a technical standpoint and a managerial standpoint, and how are we going to plan for that. That's something I'd like to elaborate on for just a moment. It's not in the Executive Order, but there's another part that talks about game changing technology being encouraged in the Executive Order, so I want to merge those two areas. We think a lot of times about security in terms of firewalls, which is analogized to a castle. You install a moat and a wall and you sit and if the bad guy gets into your castle, you remove him, and then patch up the wall. That whole model needs to be thrown out. The best and the brightest minds in incident response and information security are acknowledging we need to throw out that model. The model instead is we need to recognize that the bad guy is in the castle. That's called the advanced persistent threat. They are always in our castle. So, how are we going to have our incident response people responding when we see that the people are in there, and what do we do to protect our most critical assets inside of our castle? Some of the things we can do, such as in Nevada, are the Data Breach Detection Act which addresses the encryption of vital information. Nevada is a leader in that kind of legislation and it's still brought up at security conferences how innovative Nevada is in this area, and we need to build upon that. Because when you acknowledge that the bad guys are in your castle, now you say where's my family jewels, what am I going to protect? Well, the bad guys are going to get to the family jewels, but if they're encrypted with strong encryption, by definition, they're useless to the bad guys. And that's an example of a different focus.

The fourth item I want to bring up from the Executive Order is the framework for research and development of game changing technologies that have the potential to

enhance the security or liability, resilience and trustworthiness of digital infrastructure. We can do a lot about that here in Nevada. One of the areas that we know is going to experience a lot of growth coming up in the next few years is online gaming. And we can really be leaders here in Nevada by moving towards this new model of the ever present attacker inside our network. We're not going to keep the bad guys out of the online gaming networks. They are going to get in. What we want to do to protect the family jewels inside those networks, that's the mindset we need to have. Also, I want to take a minute in acknowledgement to financial services as well. Financial services are a big part of the economy in Nevada. We need to make sure that people know that when they do business in Nevada and those financial services are done here, that there is good security of that data that moves through our state. That's another important element that is in the critical infrastructure, one of the pillars of critical infrastructure, specifically mentioned our financial systems and a big role of those pillars is here in Nevada.

The next item is something that we're also familiar with here in Nevada. Building a cyber-security based identity management vision and strategy. One of the speakers that is going to follow me, Jim Elste, has been working with INSIT and FIPS on privacy and identity issues. This was great to see inside the President's Order there was a specific mention of privacy and protecting people's privacy. Civil liberty matters are important to people in the general public, and they're important to Nevadans. They're also important to people that are looking to relocate their business or lives to Nevada and for Nevada to grow. Nevada's got a real opportunity again to be a leader in that area with experts like Jim Elste and the work that he's doing. This effort about identity management and strategies is specifically mentioned in the Presidential Order.

Those are the highlights. There are other areas, of course, but I think that those are the ones that I want the members of the board to have a purview and take away. One other takeaway is a fascinating study just released last month by Dr. Larry Ponemon. Dr. Ponemon does research on real world businesses and how they're dealing with security incident response issues. He and his institute, the Ponemon Institute, just released a paper called The Post Breach Boom. This paper can be found at http://www.ponemon.org/blog/the-post-breach-boom. It's really illuminating. How are organizations dealing with the fact that intruders are in our networks and what do they do? Where are they? There are areas in which those organizations are sorely lacking in skilled personnel to deal with these problems. We should look at documents like the Post Breach Boom as part of our roadmap to how we respond here in Nevada to the President's Cyber-Security Executive Order and initiative, since they fit together very

nicely. That concludes my comments for today. I'm here to take questions from the board.

AG Cortez Masto:
Ira, thank you very much. How has the private sector responded to this Executive Order?

MR. VICTOR:
Thank you Madam Chair. I think there's been a general consensus of a happy response that there weren't a lot of mandates. There were concerns that the Executive Order would mandate a certain way to protect information and the Executive Order quite clearly does not say that there should vendor specific solutions or one size fits all. So, that's generally been positive. Also, the industry responded positively about the privacy issues. I think that these privacy issues, including businesses that gather a lot of this private information and want to use it in advertising and other means are starting to recognize that the consumer is concerned about their privacy. And so there's been a generally positive industry reaction to the privacy elements of the Executive Order.

AG Cortez Masto:
Thank you, any other questions?

MR. GUSTAFSON:
Madam Chair, this Executive Order that came out is really great for a lot of those in the private sector, but there's not a whole lot about states in the Executive Order. I haven't had a chance to meet with Homeland Security to figure out what this means to us. What are you hearing and is there anything else that's coming that's more State focused?

MR. VICTOR:
Well, I think that there are hints of it in here if you read between the lines. There's recommendations that all sorts of organizations, whether the public or private sector, look towards standards bodies like FIPS or NIST for guidance. I think we can look to those standards bodies as well as states like Colorado focusing in on critical essential controls that Dr. Alan Paller talked about to this very board and Colorado followed that model. With a six thousand dollar budget, they had a dramatic improvement in information security. That fits into what the themes are of the President's Executive Order. So I think we need to put those pieces together and use our heads to keep it moving in the right direction.

MR. GUSTAFSON:
Thank you. But you don't think there's any specific state government orders that's going to come out?

MR. VICTOR:
No, I don't think there's going to be. I think that this is general guidance to keep us focused on the right goals.

MR. GUSTAFSON:
I think it's great. We've been watching millions of attacks on our local state government every single day, and it's only getting worse. Everybody here says the same thing. It's great that the Executive Order is bringing awareness to this issue and it's a huge win to information security. Thank you for the briefing, I appreciate it. Thank you, Madam Chair.

MR. VICTOR:
You're welcome.

AG CORTEZ MASTO:
Mr. Gustafson, obviously one of our concerns is protecting the state network. What support are states going to get from the Federal Government on any of these issues? Do you have concerns that there isn't collaboration between the federal government and the states to address this issue?

MR. GUSTAFSON:
I think that what we would like from the Federal Government is to issue directives like the Executive Order, but there's only 50 states and there's hundreds of thousands of small businesses that can benefit from an executive order. I think a lot of time they lump states into local government, but we're not really the same animals. So we struggle sometimes with Homeland Security about this as well because there is no federal agency that has a mandate to help states in this way. Homeland Security is largely for non DOD assets, so we states think we're kind of on our own. What we get out of an executive order in this case is more of a private sector fusion, whereas we're not really like them. So, we are challenged sometimes when we work with Homeland Security because they look at us in a different light. And we struggle and we keep working at it.

AG CORTEZ MASTO:
Thank you, it's helpful. Any further questions or comments? Ira anything else?

MR. VICTOR:
No, thank you very much advisory board and member chair for this opportunity to present this to you today.

AG CORTEZ MASTO:
Thank you very much, we appreciate you being here.

Agenda Item 9 – Report by James R. Elste, CISSP, CISM, CGEIT, Chief Cyber Strategist, Nevada Cyber Initiatives, Discussion on cyber bills before the Nevada Legislature (AB 181, AB 42, and BDR 59-808).

Mr. Elste:
Thank you very much Madam Chair. My name is James Elste and the acronyms after my name are internationally recognized certifications on cyber security. I represent the Nevada Cyber Initiative, which is a group of technology professionals, entrepreneurs, and organizations that are based in Nevada that are interested in seeing Nevada advance their agenda and Nevada's agenda in the information services industry. I've been participating in the legislative process this session as a subject matter expert in cyber security, privacy, and identity management. I'm the former Chief Information Security Officer for the State and I was the Director of Information Security for IGT. In 2011 the white house released the National Strategy for Trusted Identities in Cyber Space, the goal of that is to try and address the problem of the lack of trustworthy identities for online transactions. Part of that strategy involves a governance body that would define an identity ecosystems framework and that body is called the Identity Ecosystems Steering Group. I have the pleasure of chairing the Privacy Committee of the Identity Ecosystems Steering Group.

I'd really like to welcome Belinda. I met her at RSA and told her she would have the support of the normal cast of characters, and I'm really glad that she's the new Executive Director of the Technological Crimes Advisory Board, so welcome.

As part of the legislative process, we need to get technologists involved to talk about issues that affect technology and make sure the legislators and the legislative process have the benefit of a technologist's perspective in what is a very complicated process of legislating technology.

Today, I was hoping to cover four bills that are being considered in this legislative session that affect technology or what I like to refer to as cyber bills. I'd like to give a

quick overview of those bills and to answer any questions you have regarding those bills.

AB 181

The first bill is AB 181 http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB181.pdf. This law changes existing statute around unlawful employment practices in chapter 613 of NRS. Effectively, this bill would prohibit an employer from conditioning employment of an employee or a prospective employee based on requiring them to disclose their user name and password to a social media account. For example, it would prevent an employer from asking for the password to your Facebook or twitter accounts as a condition of employment or as a prospective employee. It also prohibits those employers for taking action against an employee for refusing to divulge their user name and password. The other part of this bill is that it doesn't prevent an employee from asking for a username and password on a system that is under the employer's control with the exception of a personal social media account. So, this bill speaks to an issue that is being addressed in 10 other states, which is the terrible employment practice of asking for and inspecting an individual's social media account as part of the employment process. The problem with that is employers are taught not to ask for certain information during the hiring process, such as age, religious affiliation, sexual orientation, and medical conditions, but this information is readily seen by accessing their social media accounts. Additionally, social media credentials are being used as credentials for a number of different transactions. It isn't just a single social media account that employers are gaining access to, but rather if you have someone's Facebook account, you now have digital credentials to a variety of sites. You're exposing that individual's identity to many more problems than simply the benefits that are derived from obtaining that information during the employment process.

The other half of the bill speaks to the use of consumer reports as part of the hiring process. With a number of very specific exceptions, the bill restricts an employer's ability to use a consumer report during the hiring process. Considerations are available for the type of roll the employee might be in. For example, exceptions include if you're handling financial accounts, monitoring transactions, are responsible for access to trade secrets or confidential information, or you're in a management or supervisory role. To add to the concerns of employers using social media, I read an article in BBC of a study with 58,000 volunteers and they have developed an algorithm that allows them to analyze an individual based on their Facebook likes. They were able to predict with 88% accuracy the sexual orientation of males, with 95% accuracy whether the individual was African American or Caucasian, and with 85% accuracy whether someone was republican or democrat, just based on the way they applied likes on Facebook. So,

there are some interesting dimensions of social media that may be fodder for future legislation, but I would suggest that this bill that protects an individual's account and prevents employer's from engaging in a rather dangerous practice is a good piece of legislation.

MR. OWENS:
Are there any businesses that are allowed to do this? Federal? State? Or does this apply to everyone across the board?

MR. ELSTE:
Law enforcement agencies are exempt from the consumer report portion of this. However, the social media part applies to all organizations. In testimony before the Committee on Commerce and Labor both the representative from the Sherriff's and Chief's Association as well as the representative from Washoe County Sheriff's Office testified in support of this bill. From a personal experience, I had a colleague whose professional desire was to be a police officer. As part of the process of being hired, she had to grant them access to her social media account. She was extremely concerned that they might wrongly interpret something they saw on her social media account or otherwise prevent her from becoming a police officer. She is currently serving in one of the law enforcement agencies for our state, so that scenario turned out positively. However, at the comments made at the Committee on Commerce and Labor, although the law enforcement agencies want to perform very rigorous background checks, they really didn't believe that there was a lot of value in having access to an individual's social media account. Rather, they can perform better background checks by looking at what was publicly exposed and using known mechanisms that are available to law enforcement. So, there are no exceptions to the social media account password components of this bill, but the consumer reports does have exceptions that include law enforcement.

MR. GUSTAFSON:
Did you inform the legislature about that article regarding analysis of an individual's Facebook likes?

MR. ELSTE:
The article came out after the testimony before the Committee on Commerce and Labor, so I did not have the opportunity. But, it would be a good idea to include it in the next round of testimony.

<u>BDR 59-808</u>

MR. ELSTE:
The next Bill, BDR 59-808 (AB 385 http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB385.pdf), is a rather unique piece of legislation in that it serves the interest of three very distinct groups: individuals, private industry, and law enforcement. What this bill tries to do is three things. First, it establishes the legislative intent and recognizes that the information services industry is vital to the economy of the state. I think we can all agree that technology is a fundamental driver to the economy and there are advantages to having a strong, healthy, information services industry in the state. Second, it provides protection for a data depositor who is not the subject of a law enforcement investigation or action and ensures that if they are in a contractual relationship with a service provider, that access will be unimpaired. Then the bill goes on to define some terms which don't exist in statute right now like information data and data depositor. The language in section number two talks about unimpaired contractual access for a depositor of services that are located within the state of Nevada. The advantages for law enforcement are fairly clear. If an information services provider is physically located within the State of Nevada, they are in their jurisdiction. And that is a big problem in terms of cyber law enforcement today because countries like Antigua have essentially said they are going to ignore copyrights, allow those that violate copyright laws to have their servers reside there, and they will be safe from law enforcement prosecution. That sort of jurisdiction shopping takes place amongst cyber criminals on a regular basis. They cyber criminals look for a jurisdiction that affords them the best protection from law enforcement. What we're saying in this Bill, is that if you are an information services provider (ISP), and you locate your systems here in Nevada, we will provide you an incentive for that in the form of a protection for those individuals who use your service in a legal manner, in a contractual relationship. This should provide an incentive for businesses to locate here and an incentive for your customers to do business with said business.

The other half of this bill that is a significant benefit to law enforcement is it provides an opportunity to develop a surgical capability to perform investigations on systems that are located in Nevada. So, the bill provides that a relationship can be established between law enforcement and an ISP that is physically located within the state that establishes protocols for performing investigations that are in line with this legislation to protect non-infringing individuals and have those protocols in place in advance of an investigation. That way when an investigation is necessary against an infringing party, you already have an advantage. When we look at the cloud and service providers that have been referred to as cotenant environments, you have multiple people putting information on the same systems: good guys and bad guys. If you go in and simply

shut down the system you may get the bad guy but you may also harm the good guy. The more people and businesses that move their data and services to the cloud, the more important it is to offer them some protection. If I am a doctor and I put my medical records in the cloud, you put me out of business if law enforcement shuts down the server. The language of this bill is stating that we support law enforcement in the development of advanced, more discrete cyber investigations by providing that jurisdiction component for law enforcement. At the same time, we provide incentive for businesses to locate here by protecting their customers' information and provide economic development for the state.

DR. BERGHEL:
We have discussed this before, and I am still just as insufficiently assuaged with this relationship that may or may not exist between law enforcement and the ISP. What reason would I have to believe that there won't be any abuse of privilege?

MR. ELSTE:
I suppose you have to rely on the law enforcement agency to not abuse the privilege. Many organizations have a contractual relationship with their customers and components of that contract that describe their participation in a search warrant or other sort of legal action. So from a contractual perspective if I am an ISP and a law enforcement officer comes to me and says I have a search warrant and I need to find XYZ on your systems, I'm going to comply. I am going to be within the bounds of my contractual relationship with my customers to do so. I don't think there's intent to abuse that privilege from a service provider's perspective. This does not take in to account service providers that are primarily in the business to commit crimes. This assumes that their intent is to perform legal services and engage in business practices that are appropriate. They will be just as happy to have those infringing parties removed from their system and to participate and support law enforcement in removing them from the system. The business will also be happy to have those infringing parties removed if the business is not at risk of losing their legitimate non-infringing customers. I think it really relies on two things, Dr. Berghel. First, it relies on law enforcement recognizing that they have to have a more robust capability for performing cyber investigations and second, to develop protocols and practices with those service providers that are located in the state. By the way, it's not going to be thousands and thousands of companies that you have to worry about. We have Apple, Switch, Microsoft. Those three large companies do business here and have data centers here. They will be examples of the types of companies law enforcement will establish relationships with. So, I think it relies upon the mechanisms of law enforcement as they exist today such as search warrants

and appropriate investigation techniques, and it relies upon the willingness and contractual obligations of that private sector service provider.

DR. BERGHEL:
To follow up on that, one concern that I have is that the terms and conditions of the contract between the ISP and the customer are not publicly available. They're only available to the people that signed the contract. So, one of the things that would make me comfortable with this would be if there was a requirement for public disclosure in general of the kinds of things that can be inspected at that particular ISP via this relationship that they have with law enforcement.

MR. ELSTE:
So you're suggesting that the relationship contract between law enforcement and the ISP not be terms of service for a subscriber to the service? Those are two distinct contracts. I think you might be referring to the one that might be done discreetly between the law enforcement organization and the service provider. Is that correct?

DR. BERGHEL:
You are correct.

DR. BERGHEL:
I would suggest that isn't an unreasonable avenue to address this concern. But I would also argue that those types of agreements between law enforcement and commercial entities are not uncommon. There are several practices that take place that transcend contractual relationships between law enforcement and private sector entities, so I think we'd be well served if we were setting these things up in advance and actually had a contractual relationship. My guess is law enforcement would have limited interest in restraining their abilities to a contract versus a combination of prepositioning things via some memorandum of understanding or other form of agreement and then exercising their correct law enforcement authority under statutes as they exist today. But, it's an interesting problem. We worry about the potential abuse of information by anyone really, not just law enforcement but also intelligence agencies and private sector organizations. It's a fundamental concern about the information people provide and how that information can be abused. However, I think that benefits outweigh the negatives here because if we're protecting law abiding citizens and their access to their information, and we're not impairing law enforcement, but actually reinforcing law enforcement's ability to effectively investigate cyber-crimes, I think that's a benefit for all concerned. And the negatives of concerns of privacy or abuse are off-set by those benefits. One issue I'm surprised that hasn't been raised is the exigent circumstances

component of this where exigent circumstances might be invoked to do something that did impair contractual access. So, I think there's some further discussion to be had on this.

AG CORTEZ MASTO:
I have a particular question regarding section 2B, the bill provides that law enforcement has the ability to access the information if a given crime is occurring under the laws of *this* and they have probable cause. Would it be better to say that this applies to the laws of *a* state instead of the laws of this state? The reason being my biggest concern is that Nevada could become a site for the commission of crimes occurring via the data in other states. Quite often, on the consumer frauds side, we see Nevada, particularly under some of our incorporation laws, makes it easy for fraudulent companies to incorporate and then engage in crime in other states. So, can we address some of the concerns so we do not become the site where this criminal activity takes place? So that other states have a vehicle to address a concern if they see a violation of the laws of their state as well?

MR. ELSTE:
That is a very interesting question for a technologist, Madam General. My perspective as a layman would be certainly there is some mechanism for interstate law enforcement collaboration. So, if I am in California and a crime from California under a California statute is being committed in Nevada, certainly there is some mechanism to collaborate with Nevada to exercise law enforcement action based on the California statute. So, that sort of collaborative principle should be incorporated here, so that what you're describing cannot take place. I think it's a really excellent point because we don't want to become a haven for cyber criminals and if we have the ability to exercise law enforcement investigations and search warrants, etc. in a digital environment, I would think that it would be advantageous to have an avenue for other states to leverage that capability.

AG CORTEZ MASTO:
Exactly, so I think it would be easy to add it just under section B or maybe C. So that it states that they can access such information to further the commission of a crime under the laws of this state or any state.

MR. ELSTE:
With three words you've solved the problem. I think that's an excellent amendment. Because the bill hasn't been published yet, I have no idea what's coming out of LCB

from a publishing perspective, but I will suggest to the sponsoring assemblyman that this is an excellent amendment to this language.

MR. UFFELMAN:
General Masto, should this also be inclusive of federal laws?

AG CORTEZ MASTO:
I would think so. I think we should include all law enforcement agencies both state and federal.

MR. ELSTE:
Thank you, very helpful and constructive.

AB 42

MR. ELSTE:
Next, is Assembly Bill 42 http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB42.pdf. This bill is designed to establish the Nevada Cyber Institute within the Nevada System of Higher Education. The Institute would effectively be a body for the developing and teaching of techniques and practices related to cyber security. Among other things, the bill creates an advisory board who advises the Board of Regents with regards to matters related to the Cyber Institute and it powers the Board of Regents to define an advanced curriculum for cyber security education. Cyber security is an extremely important problem that needs to be addressed. It is a very complex problem and it is one that requires advanced training for professionals in the field of cyber security. I have a masters in information assurance from Norwich University which is our country's oldest private military academy. It was an intensive program that covered cyber security issues, and I think what we're attempting to do with the Cyber Institute is establish what is akin to an advanced program of education the same as lawyers in law school and doctors in med school. A teaching hospital is not a bad analogy because when you look at the medical profession you do premed education, medical school, a residency and now you're ready to perform the act of medicine. Similarly, the goal of the Cyber Institute is to provide the same sort of immersive curriculum and hands on practical application of cyber security techniques to be able to learn how to do threat analysis, develop countermeasures, do risk assessment, etc. The institute would essentially be a teaching hospital with an advanced program for developing cyber practitioners who are about to go into the field and actually perform that work. I think that the concept of the Cyber Institute puts Nevada on the leading edge of the cyber security question from an academic, education, and essentially a workforce

development perspective. The model institute is mapped similar to the Desert Research Institute, where the focus would be entirely cyber security. I think the demand and need for those types of skills is paramount.

DR. BERGHEL:
I think this is a terrific idea and hats off to Lucas and the Governor's Staff for proposing this bill. However, the last page needs to add the College of Southern Nevada in its listing of schools. As far as I know, the only complete forensics lab in the state of Nevada is in the College of Southern Nevada.

MR. ELSTE:
Excellent point. That was language previously in the bill. Chris Ipsen and I will have the College of Southern Nevada added in to correct this oversight. Another aspect of this bill is the resources of the institute will be made available to public and private entities. The notion of a teaching hospital requires you to have patients. In this case, forensic facilities could be leveraged by law enforcement, public sector agencies, and private sector organizations. I think it's an excellent point that we need to identify where those capabilities exist and try to pull those into this institute to create a real center of excellence and capacity for doing these things under a rubric of a teaching hospital.

AG Cortez Masto:
If I'm not mistaken, this bill is the result of a presentation last year of an individual who suggest we create this sort of cyber institute?

MR. ELSTE:
Yes Madam Chair, it was Alan Paller who is the Director of Research for the SANS institute which is one of the largest training entities in cyber security.

AG CORTEZ MASTO:
Yes, he made a compelling argument for this Institute and it's nice to see that it's actually coming to fruition here in the state of Nevada. I applaud you for moving forward with this. That's fantastic.

MR. ELSTE:
Finally, we have SB 25, which is the Attorney General's bill. This bill allows the Attorney General's Office to investigate and prosecute any alleged technological crime. And I believe that is outstanding and I hope it and all four of these bills are passed. These bills advance the cyber agenda in this State. I appreciate the opportunity to speak today.

Agenda Item 10 – Report by Christopher G. Ipsen, CISSP-ISSAP, CISM, Chief Information Security Officer, Dept. of Administration, Enterprise IT Services, Discussion on State IT Security and report on announcements at RSA conference.

MR. IPSEN:
Thank you very much Madam Chair. I hope to highlight a number of the successes of the Technological Crime Advisory Board and explain for the new members, and also give some perspective for the older members, as to why this board is really significant. There have been a number of successes, and from a personal standpoint, and one of the reasons why I'm proud to be a civil servant in this state is we can actually make a difference. First, as already mentioned, Mr. Elste mentioned the teaching hospital approach, which I think was a compelling presentation. AB 42 is a bill that came out of discussions that many of us had on how to advance cyber security education in this state. One of the issues the board could continue to move forward with is that of higher education, as they provide a vehicle for grants and other services in this teaching hospital approach analogy. But as Mr. Elste alluded to, there is a private sector component as well. One of the challenges we're facing is that in higher education, the Board of Regents has constitutional authority. So, as much as we want to suggest methodologies and practices moving forward, the Board of Regents and the university systems have to make those decisions. So, we're at a point where we need to partner effectively with the university system in order to provide a method of teaching that's innovative, forward leaning, and reaches out to the private sector. It also needs to look to instructors who may not be traditional PhDs in the field. I've been working very diligently on this and we're there, and I hope that it comes to fruition effectively. A key take away for the board, is that this idea of a cyber-institute started here at the board. This bill is a direct result of what was presented in front of this board and now we have a significant opportunity to advance this state.

Success story number two is last legislative session we had SB 82. SB 82 requires that all state agencies report all incidents back to the office of information security. Madam Attorney General, you proposed that bill through this board, the legislature approved the legislation unanimously, and the governor signed it. As a result, we now have statistics and are able to measure the number of incidents. The legislation requires that agencies report within 48 hours suspected or known incidents back to Office of Information Security. The reality is due to some of the advanced observational techniques of monitoring services and other types of techniques, the Office of Information Security typically sees the incident first. Then, we report back to the agency, and then we

require the agency to report the incident. In a real world scenario, agencies would be reporting to us and then we would be addressing it. This is likely reflective of what is happening in society as a whole. Of those breaches, typically 95-97% of all breaches are reported by someone outside of the organization that's been breached. So usually it is someone else telling you that you have a breach. So, when we become aware of something, we try to reach out to the state infrastructure and improve our reporting structure. As a matter of principle, the reporting mechanism moving forward is beginning to work and is raising awareness. A year ago at this time the Office of Information Security was receiving about 5 incident reports a month. Each of these incidents takes a minimum of 2-3 hours to resolve. Alarmingly, the number of incident reports is on a logarithmically increasing trajectory. Currently we're on pace to do over 105 incidents this month, which corresponds to at least 1.5 full time employees to resolve and in reality we've got 2 full time employees to address all of the problems associated with security incidents which relates to 33% of my staff working on this one problem alone. The good thing is we wouldn't have these statistics if they weren't required under the statute. However, the down side is in spite of the fact that we're doing better this year than we we were last year by formalizing procedures, increasing communication, we're improving our security, the problem is getting worse. From the RSA Conference, I can assure that what we're seeing is consistent worldwide. The volume and sophistication of threats is increasing. Additionally, we have two firewalls, those facing internet and those facing intranet. The intranets are semi trusted zones, internal partners that we might work with such as Clark County and Reno. The internet is everyone else: China, Pakistan, etc. Our statistics are for the internet facing rejects of connections attempting to come into our network ranges between 300 thousand and one million attempts per hour. Another startling fact is from our intranets, there are 11 million attempts of verified malicious behavior trying to get into our network.

In December 2011, Alan Pallard presented to this board and he implored us to do two things: one was the teaching hospital and the second was the four controls. The four controls include how do we patch our operating system, how do we patch our 3rd party applications, how do we restrict administrative privileges on the work stations and how do we do application white listing. I asked Alan, "How can we get executive sponsorship for a centralized system in a decentralized environment like the state?" Alan responded "Chris, it's not up to them, it's up to you. Leadership doesn't always come from the top down; it comes from having a good idea, pushing it forward, and making it available." With the guidance of the Attorney General and the Governor's directive, we have a solution. We took funds that were earmarked for our email server and we went to Symantec and presented to them the four controls we desired. They delivered with an economical program that includes support controls, standardized

throughout the state, that allows us to push operating system patches, 3rd party patches, allows us and agencies to restrict administrative access on PCs and also allows us to do application white listing, which is very expensive. Additionally, the program includes a web gateway so that we can filter traffic going out to known infected websites and inspect what packages are coming down against known malware. Lastly, and this is really important, one of our concerns is an incident that happens on a Friday after 5 since no one is working. Someone could notify the Office of Information Security, but it may be 2-3 days before anyone is made aware of the problem. This solution allows us to auto quarantine end points. Once you're infected, you're quarantined and off the network and then we can set up a remediation program. The real cost of all this for agencies is approximately $15 per month which is less than antivirus. So, this is a homerun. As a result of this Advisory Board and the presentation of Alan Pallar and years of work, we have a solution. Any questions?

MR. UFFELMAN:
You commented on semi-trusted networks such as Clark County, are you suggesting that their systems have become infected and are then trying to attack your system?

MR. IPSEN:
Absolutely. We're having an active discussion that in order for us to fully trust a partner we have to be able to a) audit their controls and b) verify that the types of controls are consistent with our own policies. So, we set the firewalls and try to use those as control points between these networks. But succinctly, if Clark County gets a virus, the virus tries to go throughout Clark County and anywhere else it can go, and if the virus can go to the state, the virus will go to the state. This is a typical way that a hacker will get into our state network is through a semi trusted zone. And, conversely, our viruses will try and get into their systems as well.

I wanted to also give an update on Mark Weatherford who presented previously before the board. He is tagged as the Deputy Undersecretary for Homeland Security for Cyber Security. He is the highest person in cyber security in Homeland Security. So, a friend of Nevada is in that unique position. He has been very helpful to us and continues to offer to be helpful, particularly with cyber annex for the state and how we address the power grid. So, we have good friends in high places. He was also one of the co-authors of the President's Executive Order on Cyber Security. We also had Jim Richberg, Cyber Lead at the Office of Director of National Intelligence, visit the Board. So, we have many high level friends willing to assist Nevada and this Board.

So, those are some updates for the Board. As we proceed forward, the challenges are daunting or almost impossible. We have to come up with a strategy that on the front end gives us the four controls so we eliminate the possibility of a problem, in the middle we address the advanced persistent threat and on the back end we have a "graceful failure" strategy. Lastly, the Center for Infrastructure Assurance and Security is finishing up a 15 month engagement with the state to bring awareness training to senior leadership within the state. Belinda attended at the last meeting. It included a multi-jurisdictional engagement of north and south, counties and cities, and engaged senior leadership in the importance of cyber security. So to have bills such as AB 42, the President's Executive Order and awareness training, shows that the general public is responding positively to stepping up to the cyber security challenges we are facing. It's been hard work, but I'm very proud and excited of the work we're doing. The work has changed significantly in the last year, and I have to thank this Advisory Board and others to say that the message is being heard and Madam Attorney General, your support has been unquestioned and it gives me reassurance. One great thing about Nevada is our collaborative nature and our ability to get things done.

AG CORTEZ MASTO:
Thank you Chris, and it's clear to me you enjoy your job immensely. Thank you for your comments and all the hard work you've put in to this board not only as a member, but now as someone who continues to support and work with us on behalf of the issues that are so important to this board. So, thank you so much.

MR. IPSEN:
Thank you.

DR. BERGHEL:
I'd like to take this opportunity to mention to the Board that the recent South Carolina Department of Revenue hack that exposed records of every taxpayer in South Carolina indicates just how important your and Dave Gustafson's jobs are. So, thank you for your good work and keep it up.

MR. IPSEN:
Thank you. It's a daunting task. I can't say that a breach will never happen, but we are giving it our best to prevent one. I'd also like to compliment Mr. Gustafson for helping to keep me optimistic.

MR. COBB:

Are you able to tell the breakdown of attacks that are specifically targeting Nevada versus attacks that generally target open holes in infrastructure?

MR. IPSEN:
This is a very high level analysis and I'm not seeing all of the attacks, but rather I'm seeing a very small percentage. What I'm seeing right now is very generic attacks at this point in time. With that said, we are responding to the known attacks now in hopes that we can clean it up using the four controls and increase our reporting capabilities. We just got a homeland security grant for a centralized logging system. In terms of a granular analysis our capabilities are improving every day, but it's tremendously reactive right now.

MR. COBB:
You may be experiencing something similar to what I used to experience working for law enforcement. When people become more comfortable reporting crimes, it looks like there is a big change in the number of crimes occurring, but in fact we just weren't aware of them because they weren't being reported.

MR. IPSEN:
That's a great point. I tried to do an analysis to take away those kinds of new factors and for this data to be an accurate representation of the actual conditions. We're trying to normalize the data to the best of our abilities so that we're comparing apples to apples and oranges to oranges rather than just an increase. Given the fact that we had this reporting capability two years ago, I think this does represent a new upswing in term of the amount of incidents.

AG CORTEZ MASTO:
Thank you.

MR. IPSEN:
Thank you, it was an honor to be here. If I may, I'd like to ask Belinda about her experience at RSA since it was her first time attending.

MS. SUWE:
Thank you, Chris. I enjoyed attending the RSA conference very much. Most of my time there focused on aspects of the human element of cyber security, such as strategies for increasing password security, securing mobile devices, and increasing awareness of phishing and spear phishing. Additionally I focused on topics that included the technological crime cycle and cybercrimes that are not being addressed. Specifically,

one crime discussed is the presence of “ex-girlfriend/ex-boyfriend websites” where compromising photos of an ex are posted. If the ex is not the copyright holder in the photo, they may have an extremely hard time getting the photo removed from the website. Those were just some of my takeaways from RSA. Thank you Madam Chair.

AG CORTEZ MASTO:
Thank you Chris and Belinda.

Agenda Item 11 – Board Member’s Suggestions for a 2013 Goal or Mission.

MR. UFFELMAN:
I’d like to suggest that we keep up to date with the four bills that have been highlighted today, particularly AB 42. I’d like to make sure that someone follows up to let us know how the legislation proceeds and the resulting effects on the economy and the State.

AG CORTEZ MASTO:
Great, additionally, one area I would like to focus on is a topic that was discussed at the conference of Western Attorney Generals, of which I am the chair, and we have a life partnership with Mexico to focus on international crime. International crime may include drug trafficking, weapons trafficking, or money laundering. Recently in Santa Monica, I held a conference on transnational crime to bring together not only our law enforcement on State and federal levels but also our partners in Mexico, as well as private sector partners, service providers, and financial institutions that have a role in transactional crime and how to stop such crimes. One area that I’m interested in is the use of the internet to proliferate crime. For example, using a service agent to proliferate crimes such as selling illegal pharmaceuticals, facilitating sex trafficking, or selling illegal goods. It’s very difficult for us to work with service providers to get these sites pulled down. It’s a challenge for us at the AGs level, and it’s something we want to explore. The internet is an advanced tool to crime and the issue for us is tackling the policing of the internet. Is this something of interest to the Board? As well as keeping a focus on our local infrastructure protection and digital privacy to individuals, consumers, and corporations. Are there any other topics that may be of interest to the Board? As mentioned, we have access to fantastic experts in the field and they can help us in this State to parse through these issues and reach solutions.

MR. BURNS:
Attorney General, on the first topic you mentioned of using the internet for fake pharmaceuticals. Homeland Security is the lead agency of the intellectual property rights center in Crystal City, Virginia and I believe at this point there are 21 other

agencies that we've partnered. I could ask them to come down here and speak to us. They do a fantastic job and it's truly global. They take down fake websites and put our badges up instead and then we monitor how many people click on the websites.

AG CORTEZ MASTO:
That's great, I appreciate that knowledge and we would welcome that participation.

DR. BERGHEL:
Another thought would be investigating to what extent privacy can be protected through statute?

A.G. Cortez Masto:
We've discussed it before, and we can continue with that exploration given our access at this board to law enforcement and corporate partners.

Let's explore these topics further and try and bring people in that can further help research and explore these topics that we've identified. Also, feel free to bring up any other topics of concern at any time. This is not a non-exhaustive list.

Agenda Item 12 – Board Comments.

None

Agenda Item 13 – Public Comments.

None

Agenda Item 14 – Schedule Future Meetings and Agenda Items.

MS. SUWE:
We will try to schedule a meeting for the last week of June. This will allow us to meet before the end of the second quarter, but the legislative session will be over so we will have access to the meeting rooms at the legislature.

Agenda Item 15 – Adjournment

AG Cortez Masto moved for adjournment. The Motion was seconded and carried unanimously. The meeting was adjourned at 3:57 PM.

Respectfully Submitted,

Belinda A. Suwe
Executive Director