

Minutes of the Nevada Technological Crime Advisory Board

August 12, 2009

The Technological Crime Advisory Board was called to order at 10:05 AM on Wednesday, August 12, 2009. Attorney General Catherine Cortez Masto, Chair, presided in Room 3138 of the Legislative Building, Carson City, Nevada and via videoconference in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada. The meeting was webcast live.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Nevada State Senator Valerie Wiener (Advisory Board Vice-Chair)
Tray Abney, Reno/Sparks Chamber of Commerce
Gregory Brower, U.S. Attorney, Department of Justice (DOJ)
Donna Crutcher (*Rep. for Dan Stockwell, Director, NV Dept. of Information Technology*)
Sheriff Mike Haley, Washoe County Sheriff's Office (WCSO)
Special Agent in Charge Steve Martinez, Federal Bureau of Investigation (FBI)
Special Agent Melissa McDonald (*Rep for Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE)*)
Assistant Special Agent in Charge Rob Savage (*Rep. for Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)*)
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association

ADVISORY BOARD MEMBERS ABSENT:

Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)
Dale Norton, Nye County School District Assistant Superintendent
Nevada State Assemblywoman Peggy Pierce

TASK FORCE MEMBERS PRESENT:

Sergeant Troy Barrett, Las Vegas Metropolitan Police Department (LVMPD)
Detective Dennis Carry, Washoe County Sheriff's Office (WCSO)
Talova V. Davis, Computer Forensic Examiner, Attorney General's Office (AGO)
Ryan McDonald, Computer Forensic Investigator, Attorney General's Office (AGO)
Gregory Smith, Chief Investigator, Attorney General's Office (AGO)
Supervisory Special Agent Eric Vanderstelt, Federal Bureau of Investigation (FBI)

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director

OTHERS PRESENT:

Edie Cartright
Brett Kandt
Chris Memmott
Sean Neahuson
P.K. O'Neill
Brian O'Callaghan
Kareen Prentice
Lea Tauchen
Greg Whisenant
Bob Young

Agenda Item 1 – Call to Order – Verification of Quorum

AG CORTEZ MASTO:

The meeting is called to order on August 12 at 10:05.

A roll call of the Advisory Board verified the presence of a quorum.

**Agenda Item 2 – Discussion and approval of minutes from October Board Meeting
(Discussion/Action Item)**

AG CORTEZ MASTO:

The next agenda item is the discussion and approval of the minutes of our last meeting. These minutes have been previously distributed. If there are no changes, I will entertain a motion for adoption.

Motion to approve the minutes was made by Mr. Uffelman and seconded by Sheriff Haley.

Motion to approve the minutes was approved unanimously.

**Agenda Item 3 – Annual Election of Chair and Vice Chair (NRS 205A.040)
(Discussion/Action Item)**

AG CORTEZ MASTO:

The Board's governing statute requires annual elections to fill the positions of Chair and Vice Chair. I will now open the floor for nominations for Chair.

Motion to reelect AG Cortez Masto as Chair and Senator Wiener as Vice Chair by acclamation was made by Mr. Uffelman and seconded by Sheriff Haley.

Motion was approved unanimously.

Agenda Item 4 – Report regarding Task Force Activities. (Discussion/Non-Action Item)

AG CORTEZ MASTO:

The next item is reports regarding Task Force activities from concerned agencies including the FBI, Las Vegas Metropolitan Police Department (LVMPD), US Secret Service, Attorney General's Office, Washoe County Sheriff's Office (WCSO), and ICE.

Considerable time has passed since our last meeting. I understand that, since that time, the FBI has undertaken some significant outreach activities and that the Washoe County Sheriff's Office has constructed a new facility it is interested in sharing.

Are there any reports?

SAC MARTINEZ:

Madame Chair, if I may, I would like to introduce Supervisory Special Agent Vanderstelt, the head of the southern task force, to report on its activities.

SSA VANDERSTELT:

Madame Chair, members of the board, good morning and thank you for the opportunity to provide you with an update on our Task Force activities since the last board meeting.

The FBI and Las Vegas Metropolitan Police Department (LVMPD) have been conducting a joint investigation into organized criminal groups involved in the fraudulent sale of vehicles over the Internet. A number of indictments and arrests have been made over the past months. Two of the main conspirators have pleaded guilty and were sentenced to between two and four years federal imprisonment and ordered to pay restitution of over \$500,000.

A man was sentenced to approximately four years for attempting to extort \$250,000 from both Harrah's and MGM. This was investigated as a computer intrusion matter as the subject led the victims to believe he had access to their computer networks and could access trade secrets and personally identifiable information on employees and guests.

Two individuals were indicted in April on charges related to the theft of intellectual property from IGT Corporation. Multiple search warrants were coordinated and executed in a single day spanning several time zones, and one of the subjects was arrested in Latvia. This matter was investigated jointly by the FBI, Customs, and Nevada Gaming Enforcement. The Central Criminal Police Department of the Latvian Ministry of Interior provided significant assistance in the case as did IGT.

Over a dozen individuals have been indicted, arrested, or convicted on federal charges related to child pornography. Especially notable among these cases – an individual was indicted and convicted after he attempted to establish a website depicting child pornography. He awaits sentencing. Two subjects were sentenced in separate cases to approximately ten years on charges of coercion / enticement of a minor. A man was sentenced to more than 24 years behind bars for possession of child pornography and traveling interstate to engage in sex with a 15 year old boy. The man had a prior sex offense conviction. A woman was sentenced to 10 years in prison on a charge of receipt of child pornography.

These are some of the accomplishments I can report that have occurred since our last meeting. As the importance of digital forensics and the scope of work involved in that area is a topic of frequent interest to the board, I'd also like to add that so far this year, our computer forensic examiners have examined over 1,500 items exceeding 25 TB of information. This amount of information is equivalent to about 5.5 trillion pages of text.

In closing, I'd again like to thank the board for extending the opportunity to present this morning. I'm available to answer any questions.

ASAC SAVAGE:

Recently I attended a global conference in Washington. Representatives from all of the 38 Economic Crimes Task Forces, sponsored by the Secret Service were in attendance – some 500 participants in all. A number of important topics were discussed including improvements in the inter-agency coordination that is part and parcel of Economic Crimes Task Forces.

AG CORTEZ MASTO:

I recently read a report about the presentation of Secretary Napolitano. I understand that she stressed the importance of cooperation among state, local, and federal officials. Could you tell us a little more about that? Also, I understand that a cyber czar has been appointed or is about to be appointed. Is that right, Jim?

MR. EARL

Recruitment for that position has been going on for some time. It would report both to General Jones, the National Security Advisor, and to Larry Summers, who heads the President's National Economic Council.

ASAC SAVAGE:

Madam Chair, that is correct. As to your question, one of the main themes of the conference was interagency cooperation at all government levels. As we work on a daily basis and share information and investigations, we have an opportunity to come at the problems we confront from all angles.

AG CORTEZ MASTO:

Thank you for your comments.

SAC MARTINEZ:

Madame Chair, if I might add something. I know the focus of dialog on this issue – trying to place a cyber czar – has been, first and foremost, to concentrate on securing government systems. That would include both federal and state systems, but particularly federal systems. We have had a lot of activity in the form of presumed attacks from external enemies. There will be a big push in that area. This is something that has to be accomplished government wide because everyone is running their own networks. They are working very hard to come up with standards and protocols that everyone can abide by. This likely will have some input on what comes to be seen as best practices for state systems.

As far as promoting task forces, this is really nothing new for us or the Secret Service. We have all been funded to assist as best we can to provide overtime pay, equipment, vehicles and that sort of thing for task force members that come on board to the task forces we sponsor. We will continue to do that. I think we will enjoy adequate funding for these efforts here in Nevada.

AG CORTEZ MASTO:

Great, thank you. Are there any other comments from Board members?

SHERIFF HALEY:

Madame Chair, if we could have a brief update on cyber initiatives in Washoe County from Detective Dennis Carry.

DETECTIVE CARRY:

I am assigned as a detective in the Washoe County Sheriff's Office (WCSO) and I am assigned to the cyber crime unit.

I know you will receive a presentation by Sergeant Troy Barrett of the Las Vegas Metropolitan Police Department (LVMPD). He will discuss Internet Crimes Against Children (ICAC) issues.

We in northern Nevada have been quite busy with ICAC cases and other cyber-related crimes. Although I do not want to speak to specifics regarding numbers, at least one individual who was recently arrested possessed over what we estimate to be over one million images and videos of child pornography. As I was going through the evidence the other day, I realized we will never really know how many images he had. It would take approximately a year to view each image and go through each video. This is a growing problem.

We could probably make a similar arrest every other day if we had the resources and time.

As the government has created the cyber czar position and tries to integrate law enforcement agencies and other government entities into the fight against cyber crime, we recently completed construction at WCSO of the cyber-crime, cyber-attack center. This center will allow regional agencies to integrate into a single location. Computer forensic examiners and cyber crime investigators will focus on attacks and cyber crime related issues.

The benefit of this regional effort – getting all these people into one room – will give us the ability to bounce ideas off one another. Some computer forensic examiners are more trained than others. Some are new. Also, the experience of cyber crime investigators varies with some having different strengths and weaknesses. By putting everyone in the same room, we can build off one another. We can save a lot of time. When a major incident occurs, we will be able to go on the attack right away.

This center, at least initially, will integrate personnel from the Nevada Attorney General's Office, ICE, WCSO, the Washoe County School District Police, and hopefully, the Reno and Sparks Police Departments. Thereafter, we will be open to whomever wants to come on board. We anticipate being able to do a number of good things. Several of the people who will be involved are in Board meeting today. We are just about ready to move in. We are waiting on the resolution of several security issues. We want to make sure everything is secure and safe.

Cyber crime incidents are certainly not slowing down. Sergeant Barrett will talk about the numbers. You will see how the arrests are ongoing. Fraud crimes also continue.

I would encourage members of this Board to talk to other entities and try to get more people involved. The cyber crime center will be able to address issues that are reported to us – either through regular crime reporting or tips we receive from other government entities.

We are going to experience difficulties in working with corporate and business entities. What I mean by that is getting business to disclose to us that they have been attacked, or that they have a hundred thousand customers whose credit card information might have been compromised.

I encourage the Board to address those issues and keep corporate on their toes to report issues to us so that law enforcement can become involved.

AG CORTEZ MASTO:

The opening of the center is certainly good news. Thank you very much, detective.

ASAC SAVAGE:

I just wanted to address the concerns of corporations – to cooperate with law enforcement versus protecting their own internal interests. That was something that came up during the conference last week.

There were members of the private sector that stood up and addressed this issue. While they had previously resisted coming forward, and many times were the subject of extortion from hackers, they had come to realize that by paying extortion and not approaching law enforcement, they only invited additional attacks and more extortion.

There was a move for the private sector to partner with their local task force, the local police, the Secret Service, and FBI. There was realization that the earlier they made contact, the better chance they had to receive support to shore up any vulnerabilities in their infrastructure and to stop making extorted payments.

SHERIFF HALEY:

I have one additional comment. I want to thank SAC Steve Martinez, FBI. He is responsible for sending law enforcement personnel to the National Academy. When I attended courses in 2000, there was a class called "Futuristics". It addressed this particular issue.

Corporations generally train their employees to address narrow issues focused on their companies. Law enforcement trains its personnel to deal with the legal aspects of this problem. We need to bridge those two worlds.

We need to encourage corporations to engage us at a high level while we ensure their organizations are protected and that the information they have is protected.

We are at a crossroads here. We need to engage the public and corporations in a consistent way or our paths will go in different directions.

It is very difficult to train and retain law enforcement officers in the computer forensic investigative field. They are often hired out of law enforcement once they achieve a certain level of training. We have to be able to keep those folks. We have to be able to incentivize them to remain. If we do not, law enforcement at state and local level will no longer be able to investigate these crimes.

AG CORTEZ MASTO:

I appreciate your comments. I am curious whether our corporate Board members have ideas as to how to bridge this education gap – to foster an understanding that law enforcement is out there to support businesses and help them. From your perspective, are there things that you see among your business contacts that bear on this issue?

MR. UFFELMAN:

The financial services industry certainly has engaged with law enforcement at all levels regarding intrusions, data theft, and the like. We have a comfort level with law enforcement. I know there is also sometimes frustration when the dollar loss is so small that we could not get anyone interested.

Often the real question is, "What is the tipping point that will get law enforcement interested?" My CEOs have expressed this concern once and awhile. There was also a comment the other day along the lines of "No matter how hard we work, or what best practices we implement, it always seems the bad guys are a half step ahead of us."

To the extent that there is international cooperation to take major criminals down, that would be good. When we are successful, then that success breeds getting more people involved and more cooperation. It will be more worthwhile to send people to activities to get people cross-trained.

SAC MARTINEZ:

Madame chair, if I might add something. I made reference earlier to an InfraGard meeting last week. We have chapters in both the north and south. The purpose of InfraGard is to bring law enforcement and the private sector together to discuss matters of common interest. We want to provide a comfort level that in the event there is some kind of compromise to a network that there is a means to work investigations discretely. We certainly do not want to put companies at a comparative disadvantage. Much of our work is under the radar screen.

We are not technologically able to do things to investigate without having to shut down corporate networks. We are able to monitor activity and work proactive cases without engaging in a shut-down.

We still need to get the word out. Word of mouth is the best way we have determined. If someone has had a good experience working with law enforcement, then, even if there is a tendency not to

report, word gets around that law enforcement does respond to practical needs. The InfraGard construct is one of the ways we do this.

The northern chapter is very active. I believe there are over 400 members. I am very pleased, and sometimes surprised. I think there are well over 300 members in the south. The program is working well in Nevada. We have had referrals directly out of InfraGard from people, who in the past might not have been nearly as willing to come forward to report a problem. They are now increasingly willing to do so. While we have more work to do, we are bridging that gap.

MR. ABNEY:

It is an education issue. SAC Martinez mentioned InfraGard. The organization I am with, the Reno/Sparks Chamber of Commerce held a joint event with InfraGard at the NV Energy auditorium. This was last year. We had close to 80 attendees. We set this up with Ira Victor. My organization represents companies from the largest employers in the State and Washoe County to the very smallest one-person, home-based businesses. It is a bit difficult to decide who among our membership are more interested than others. However, I think InfraGard is probably the perfect place to do that. You can get everyone in one room. With the number of members in the Chamber, and the number of emails we send out, InfraGard meetings are the perfect way to get the message to the private sector.

AG CORTEZ MASTO:

If there are no other comments, we will move on to agenda item number 5.

Agenda Item 5 – Report on Initiatives in the 2009 Legislative Session (Discussion/Non-Action Item)

AG CORTEZ MASTO:

I believe Mr. Earl and Mr. Kandt are ready to provide information regarding what happened during the session.

I want to give special thanks. I know that during the session, there was a coordinated group effort to support various bills. I want to thank Captain Kuzanek and Detective Carry from the WCSO, LT Sebby, LT Roberts, and Sergeant Barrett from LVMPD, Kristen Erickson from the Washoe County DA's Office, Sam Bateman from the Clark County DA's Office, and, in my office, Keith Munro, Brett Kandt, Edie Cartwright, and Jim Earl.

I know these people worked together constantly in support of the various bills that were important to all of us. I want to thank all of you for your hard work. You are going to hear what they accomplished right now. I think it is pretty tremendous.

MR. EARL:

Members have before them several handouts that relate to agenda item 5. The first is a bill summary. That summary highlights the half dozen or so bills that arose from previous Board meetings. They are arranged pretty much in numerical order. I will speak briefly to most of them, although, I would like to invite Brett Kandt speak to AB 88.

As Brett is coming to the table, let me say that this bill is composed of essentially two parts. The first provides a civil remedy to victims of child pornography. It is based on a Florida statute. I had confirmation earlier this morning that Nevada and Florida are the only two states that have such a civil remedy. That particular portion was not particularly contentious, although considerable legislative attention was directed at it.

The real problem we had related to the second part of the bill. This seemed to me to be a very simple change to the Nevada criminal code. We were attempting to modify the existing

possession of child pornography laws to account for streaming video. That proved to be much more difficult, as Mr. Kandt will get into in just a moment.

This particular issue was identified to the Board by two presentations, including, most recently, the presentation by Detective Carry last October.

MR. KANDT:

Brett Kandt, for the record. I guess I do not really have to say that. The last time I was here in the Legislative Building was during the session. I was before the Judiciary Committee. I am the Executive Director of the Prosecution Advisory Council.

AB 88 was one of the bills in the Attorney General's legislative package. As Mr. Earl mentioned, it had two components. The civil component created a civil cause of action. Victims of child pornography can now seek damages against any producer or consumer of the pornographic material the victim was featured in. The statute presumes a minimum damage of \$150,000. The victim can seek greater damages. I will not spend a lot of time on this. There is a different burden of proof. The victim would have to prove all the elements associated with the cause of action to prevail.

The second component of the bill is the criminal component. It was intended to address what was perceived as gap in current Nevada law regarding consumers of child pornography who access it through the Internet, but do not download a file or take any action that would fall within the scope of the possession statute. Instead they use evolving technology such as streaming video, a webcast, or perhaps some other technology that is not widely used at present.

We wanted to plug that gap. We sought to criminalize that specific conduct. We did have some challenges. One of the reasons is that we did not have the text in the pre-filed bill.

For those of you not familiar with the legislative process, the bills that come from the Attorney General's Office were pre-filed with the Legislature late last year. We did not have the criminal components in the pre-filed version of AB 88. As a result, we had to ask that these be amended into the bill during the hearings. Because we did not have specific language in the pre-filed bill, we invited further discussion and scrutiny.

However, we were successful, not on the Assembly side where the bill originated, but on the Senate side. The Senate included the criminal component into the bill. As part of the legislative process, the bill had to return to the Assembly for concurrence. Through that process, we ended up with the bill in its current form.

Specifically, if you look at section one, this criminalizes the conduct we were concerned with. It specifies that if an individual uses the Internet to control the pornographic material for the purpose of viewing, then a crime has been committed. That term "control" was part of a compromise to get the bill passed.

I had proposed the term "accessed". In fact, when the bill was amended on the senate side, the term "accessing with intent to view" was used. However, as part of the compromise in the conference committee, "access" was determined to be unacceptable, and the term "control" was preferred.

It is obvious that the statute be clear on its face, especially a statute that defines criminal conduct. After doing some research, we had a certain level of comfort that the term "control" would be workable because of the case law from a variety of jurisdictions. That case law generally indicates that "controlling" this material through the Internet encompasses the specific conduct we wanted to criminalize – browsing, entering search terms in a browser, surfing the Internet, viewing pictures and streaming video, and viewing a webcast. I believe you have a copy of my memo.

That was the explanation of the way compromise language was developed. We will have to see how this shakes out in terms of investigations and prosecutions under the new statute.

The statute provides that the first offense is a Category C felony. Any subsequent offense is a Category B felony.

I do want to touch on one additional issue that just came up in the last several weeks. I believe you were provided a copy of an order dismissing a charge of producing child pornography. The case is out of Elko County. The charge was dismissed on the basis that the term "minor" is not defined and is unconstitutionally vague in NRS 200.710.

This raises some concern. Most of the child pornography statutes use the term "minor", but do not define it. The possession statute does not use the term "minor". It deals with "a person under 16 years of age."

The new statute, from AB 88, the "controlling through the Internet" statute, also uses the phrase "person under 16 years of age".

However, this order raises some concerns. It was issued by Judge Puccinelli. He is a good judge. I think he raises legitimate concerns in granting the motion to dismiss. I think it likely that defense attorneys who represent defendants facing the same charges will make the same arguments in other courts. I intend to pursue a possible legislative fix we can consider for the next session. The fix would clarify the term "minor" to clear up any issues in future prosecutions.

AG CORTEZ MASTO:

Are there any questions? Before we move further, I would also like to thank Senator Wiener. She was one of our biggest advocates at the Legislature – not only on these bills you will hear about. She also carried several bills on behalf of the Board and did an incredible job.

MR. EARL:

Moving on to Senate Bill 82, Board members have the legislative summary. You will recall that the subject matter of this bill as passed, criminal use of prepaid cards, came to the Board's attention largely through the efforts and presentation of LT Bob Sebbby of LVMPD and Jack Williams of eCommLink. The bill as unanimously passed out of the Senate committee was in the form the Attorney General's Office had put forward.

Unfortunately, as a result of a series of compromises on the Assembly side, a number of provisions were deleted. The statute as enacted does not contain the step-by-step guidance to law enforcement nor the codified protection of individual rights contained in the original bill. However, it does appear that those gaps can be filled by reference to existing Nevada law dealing with search warrants and the ability of police officers and courts to act in exigent circumstances.

If there are any questions, I would be glad to address them.

Let me turn to Senate Bill 163. This bill was co-sponsored by Senator Wiener and Assemblywoman Parnell. Well over a year ago, Senator Wiener raised the issue of cyber bullying in a Board meeting. SB 163 not only contains specific provisions about cyber bullying, but also an instructional requirement for public schools in Nevada. They need to provide age-appropriate instruction in ethical, safe, and secure use of computers and other electronic devices.

It is interesting that the President's Cyber Space Policy Review contained a recommendation that kindergarten through 12th grade instruction include exactly these same subject areas – cyber ethics, cyber safety, and cyber security. Nevada is clearly ahead of the power curve on this particular concern.

Moving on to Senate Bill 223, this legislation also flowed from concerns expressed by LVMPD regarding provisions relating to credit and debit card offenses. Essentially the bill updates certain existing provisions. As initially considered, it would have had a fiscal note attached. Because of that, certain sentencing provisions were taken out of the bill prior to its initial introduction.

The last bill I want to talk about is Senate Bill 227. This was sponsored by Senator Wiener. In the 2005 Legislative session, a bill was passed requiring businesses in this state to encrypt data containing personally identifying information. That 2005 statute was scheduled to go into effect on October 1, 2008. Prior to that date, the Board heard from Ira Victor and others regarding the difficulties private industry was experienced in attempting to implement the existing statute. As a result, Senator Wiener undertook to introduce legislation that would both fix the anomalies identified and also tighten up the standards, and importantly, apply the requirement to encrypt certain data in transit and certain limited data in storage to government agencies as well.

We spent considerable time on this bill. There was considerable discussion with private sector interests under Senator Wiener's guidance. This began earlier than 6 months before the Legislative session. There were a number of statutory changes that were considered and many that were made before the bill's final passage.

Since then, several things have happened. First, the settlement regarding the TJX data breach has been announced. One of the requirements imposed by that settlement on TJX is to lobby within the PCI community to have the PCI DSS – the data security standard required by contract for retailers who accept payment cards – to include end-to-end encryption.

I have also been requested, and have made several presentations regarding SB 227 – the circumstances surrounding its passage, and what it means for governments and businesses within Nevada. One of those presentations was for continuing legal education credit, and, as a result, I have received inquiries from municipal attorneys throughout the state. Most recently I did a presentation in Las Vegas, where I was invited by CompTIA, one of major IT trade organizations, to brief executives on SB 227. Are there any questions?

MR. ABNEY:

I was into and out of the conversations about this bill during the session. I was sometimes on conference calls with groups out of Washington DC. I was never able to attend the meetings held in Senator Wiener's office. I always had to be somewhere else when these issues came up. Could you just briefly talk about some of the issues that were raised – those that were answered and those that were not? I don't want a long discussion. I know that Mr. Uffelman was involved as well. I would just like to have my understanding filled out a little bit.

MR. EARL:

Probably the most important concern that was raised and addressed came from Nevada Retailer's Association and AMEX. The bill as originally written did not contain any language relating to PCI, the credit card industry and banking security standard. As passed out of the Senate, the bill related to encryption requirements for all data collectors in Nevada. In essence, the Retail Association and AMEX suggested, given many small businesses in Nevada have contact with personally identifiable information primarily through the use of acceptance of credit and debit cards in payment, that the Legislature consider whether compliance with the PCI data security standard would be sufficient to meet the encryption requirement.

After considerable consultation and consideration by me, private sector representatives, and Chris Ipsen, Nevada's Chief Information Security Officer, and after looking at the most recent version of PCI DSS in effect from last October, we concluded that the PCI standard was definitely moving in the right direction. In essence it required a higher standard of care for those transmission paths that were most susceptible to interception of data. In the PCI DSS of today, there is an encryption requirement when credit card data is transferred between point of sale and validator or issuing bank over the Internet. There is no definition of encryption. However, there is

a movement within the PCI community to continually address the issue. The fact that the PCI standard undergoes a series of updates and changes, taking into account the interests of both banks and small retail merchants, was a principle driving factor. Those of us involved in the drafting process, recommended to the Legislature that the PCI standard be included in the final version of SB 227.

Let me mention one other thing. This goes to the helpful roll of InfraGard in its outreach efforts. The northern section's next meeting is on October 15. The president of the northern chapter, Ira Victor, has asked me and others participants involved in SB 227 to present at that meeting. We will be going through an explanation of what problems existed under the old law, what SB 227 was designed to address, how we went about doing so through the legislative process, and the end result of what is an appropriate compliance standard. I would invite you and the Chamber of Commerce, concerned about the impact of SB 227, to attend that InfraGard meeting.

SENATOR WIENER:

There is one additional concern that was raised during the bill's process. Until the final hour, this bill had a veto threat hanging over it. It made it through with the Governor's signature instead thanks to the people that sent support messages to the Governor explaining how it would help people in Nevada. I publicly want to thank the people who were engaged in that process – to explain the bill so the Governor understood that Nevadans would be protected.

One of the other parties involved were telecommunications companies – those companies that transmit the information. We made provisions for them as well. If their only contact with personal information is providing the transmission conduit, that is, they are not collecting the information for their own use, then they are not data collectors under the statute. I explained to them, if you engage with the information, then you become a data collector rather than a transmitter. But, as a data transmitter, I think it is reasonable that they not have the same encryption requirement.

AG CORTEZ MASTO:

If there are no other comments or questions, I have one final one. Jim, to put this in perspective, how many other states have laws similar to SB 227?

MR. EARL:

Presently, there are no other state laws that have similar provisions. Massachusetts does have an encryption requirement, but it is part of a much larger statute that is very regulation heavy. One of the things that distinguishes Nevada's new law from the Massachusetts statute is the safe harbor provision. We expect that the safe harbor provision will incentivize compliance by both government agencies and businesses without the need for either criminal sanctions or a very detailed regulatory environment.

Quite frankly, one of the reasons CompTIA invited me to present on the bill is that it is unique within the United States. I received some very positive feedback. During the presentation, one of the members of the audience, who was much more involved with setting the PCI standards and knows much more about them than I ever could, stood up and gave a heart-felt thank you both to you, Attorney General, and to Senator Wiener. He said the entire PCI community, particularly those related to enforcement should be sending you folks congratulatory letters and bouquets. This is because of the attention the bill focuses on the need for compliance by retailers with the security requirements.

Agenda Item 6 – Presentation by Captain P.K. O'Neill, Division Chief, Records, and Technology Division, Department of Public Safety, on the National Data Exchange (NDEX) Program and Criminal Information Sharing Issues (Discussion/Action Item)

AG CORTEZ MASTO:

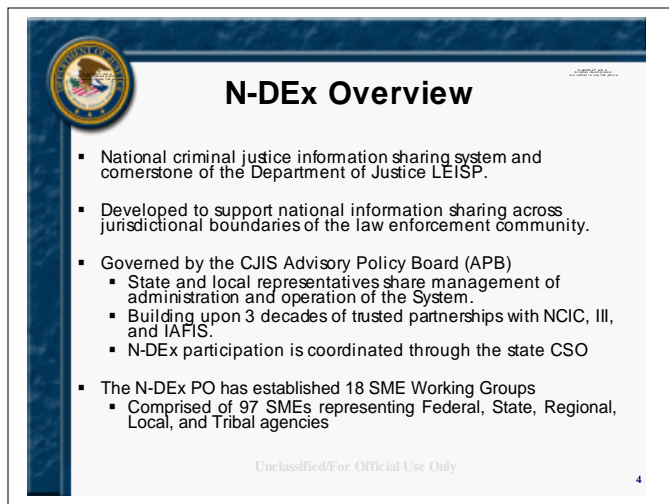
Captain P.K O'Neill will be presenting on the next agenda item.

CAPTAIN P.K O'NEILL:

Thank you, Madam Chair, and thank you to Members of the Board for inviting me here today. I am the Division Chief for the Department of Public Safety Records and Technology Division. I have been requested today to give a short presentation on a national initiative that is being sponsored and developed by the Federal Bureau of Investigation, the National Data Exchange (NDEX).

Normally this part of the presentation is given by a Bureau member. However, that team was just out here two weeks ago. They were unable to make it back from Clarksburg, West Virginia. With their permission from the NDEX unit, they have allowed me to make this abbreviated presentation.

There are some obligatory slides.¹ This is a picture of the criminal justice information services division back in West Virginia. This group is the main driver of the National Data Exchange program. The Law Enforcement National Data Exchange and the One DOJ Systems have a vision. The Bureau has a vision to share complete and accurate, timely, and useful criminal justice information across jurisdictional boundaries; and to provide new investigative tools that enhance the national ability to fight crime and terrorism.

The slide is titled "N-DEx Overview" and features the Department of Justice seal in the top left corner. It contains a bulleted list of key points about the National Data Exchange system. At the bottom, it includes the text "Unclassified/For Official Use Only" and a small number "4" in the bottom right corner.

- National criminal justice information sharing system and cornerstone of the Department of Justice LEISP.
- Developed to support national information sharing across jurisdictional boundaries of the law enforcement community.
- Governed by the CJIS Advisory Policy Board (APB)
 - State and local representatives share management of administration and operation of the System.
 - Building upon 3 decades of trusted partnerships with NCIC, III, and IAFIS.
 - N-DEx participation is coordinated through the state CSO
- The N-DEx PO has established 18 SME Working Groups
 - Comprised of 97 SMEs representing Federal, State, Regional, Local, and Tribal agencies

Unclassified/For Official Use Only

4

NDEX has as its major goal to detect relationships among people, places, things, and crime characteristics. As we all know, starting with the terrorist attack of 9-11, 2001, there were a number of different silo systems. The Bureau realized that in today's world, information sharing is somewhat of a simplistic idea, but has major challenges in implementation. I have to commend the Bureau and its Criminal Justice Information Services (CJIS) Division. They did not look at the problem simply from the Bureau's perspective. They went out to all levels of law enforcement in the criminal justice community, including State representatives, Sheriffs'

representatives, and local municipal police departments. They even presented themselves to the ACLU with a privacy impact statement to look at the issues associated with a nation-wide law enforcement, incident sharing program.

Using those various inputs, they developed, over the last several years, the business design for this national data exchange. In March 2008, they released the first increment of an exchange program. I will show that in just a minute.

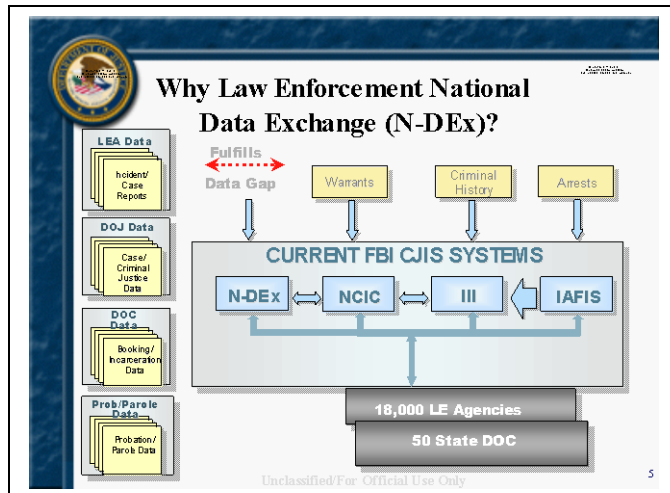
The bottom line is that the program will connect the dots between data that does not seem to be related. It is also available to support multi-jurisdictional task forces on a virtual level. I will show you that you can establish virtual task forces that are not physically formalized.

The overview of the system, as developed by the Department of Justice and its CJIS Division, will support national information sharing across jurisdictional boundaries of the law enforcement community. It is not governed by the Bureau. Rather, it is governed by the CJIS Advisory Policy Board. Every state is a member of that board. Nevada has two representatives. One of my duties

¹ Not all of the slides presented to the Board are incorporated in these minutes.

involves my being the CJUS Officer or CSO. I sit on the board. Next week we will be attending the quarterly meeting of the CJUS working groups and the advisory policy board. The working groups have regional groups. We give our comments to the advisory policy board, which actually controls CJUS. CJUS is currently known mainly as the National Crime Information Center, NCIC, IC3, all that criminal history that involves warrants and other informational work.

NCIC was developed in 1968. NDEX is a further development. As I said, it is governed by the states and by its users.



Currently, NCIC deals with warrants, criminal history and arrest information. These are the informational inputs. If you look at the left of the screen, you will see that there is a variety of information that is missing – law enforcement agencies' data, Department of Justice data, Department of Corrections – the federal corrections system data, and parole and probation data. All of these are missing.

The plan of NDEX is to bridge that gap, and to bring that information into the NCIC system. My prediction, and I have been in law enforcement just

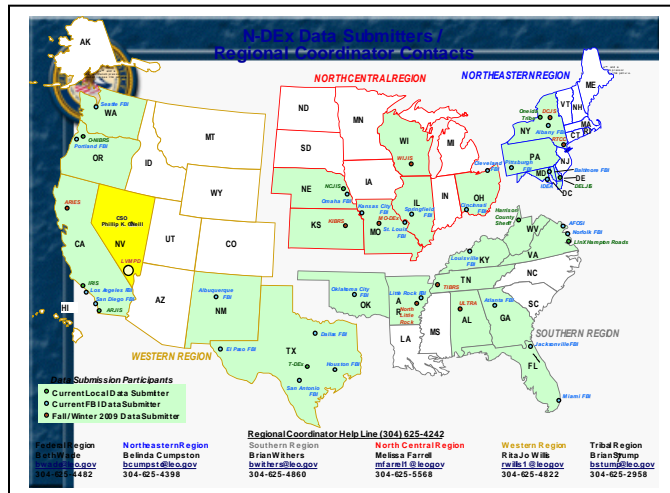
short of 37 years, is that NDEX, 20 years from now, will be virtually indispensable to the officer in the street. That officer routinely asks dispatch to run an NCIC check, or the officer runs it himself. I truly believe that within 10 or 15 years, and definitely within 20 years, the officer will be running NDEX searches to do background work to supplement their investigations. This will be critical in bringing the dots together. That is the goal of the NDEX program – to supply necessary information. When we talk about intelligence-led policing, we truly will have the background information to support our decision making.

The sharing of key data concepts is based on ownership continuing to be owned by the supplier, that is, the agency that submits the information. That agency has the ability to code it as green; this means it is open to anyone running a check. It can be viewed. The agency can put data in as yellow; this indicates that the originating agency wants information back that someone has inquired about the information. Or, the information can be identified as red. This would prevent an inquirer from seeing the information at all. However, the agency that entered the information would be notified that someone made an inquiry that day. There are several reasons for this. If we are working corruption crimes, particularly in political or law enforcement areas, these personnel might have access to run NDEX. We would not want them to see whether others were inquiring about their activities. However, the originating investigator would be given a lead.

Here is a use of the yellow information. In Nevada, we have certain laws that protect juveniles and victims of sexual assault. So, who views the data can be regulate by how the data is entered. This is a key component of the system – particularly in the looking at the privacy impact portion as presented to the ACLU and other contributing organizations. It was important that there be controls like these be in place. To repeat, the data is owned by the agency submitting it. Although it goes to the Bureau and to its servers to be massaged and delivered back, the data is still under the control and ownership of the originating agency. They control how it is entered into the system and how it can be utilized.

One of the other requirements is as follows. If any information is developed in support of either a search warrant or criminal arrest warrant, the inquiring agency or officer must go back to the agency of origin and get its permission to utilize that data in support of any further legal actions.

Turning now to look at the states, the states in green are submitting information to the NDEX program. Nevada is in yellow because we are currently working with LVMPD to map some information within its records management system (RMS) to supply to NDEX. This has not yet been completed.



I would like to draw your attention to Washington and Oregon – where the entire state is supplying information to NDEX. In California, the southern part of California, Los Angeles County, Los Angeles FBI, and the San Diego FBI and San Diego, San Bernardino, Riverside are all supplying information into NDEX. In northern California, an exchange system is being developed from the San Francisco Bay area through Sacramento County.

One of the nice things about the increment, recently released in July 2009, is the ability to share

information among and to set up virtual regional task forces. The officer working cases can create an informal or formal task force, and download various information from searches. NDEX allows searches to be done by names, characters, incidents, vehicles, basically any other parameter. This would include MO's or *modus operandi* of the crime. It can map these and return the information in documents or presentations as desired. This could be geo-mapping or involve the generation of time-lines. It will also do diagramming to illustrate relationships among phone numbers, vehicles, or individuals.

One of the latest releases involves a subscription. An investigator can enter a request into NDEX. While there may be no information currently, the request, in effect, says "Please let me know if this information is received or if something similar is submitted. I would be interested." This allows an investigator to project his interests into the future.

This slide demonstrates that the process is automatic. When the information is entered, it returns to the investigator and the originating agency, either through an email or through a portal.

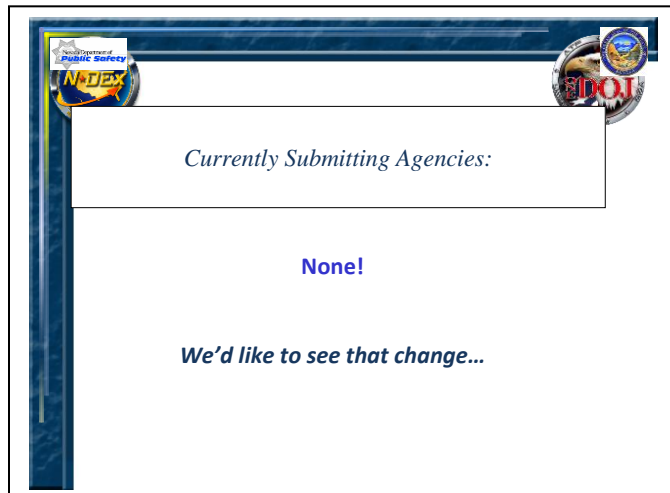
98 Currently Registered Users (Inquiry Only)

Agency	# Users	Agency	# Users
Carson City District Attorney	1	DPS Investigation Div.	3
Carson City Sheriff's Office	1	DPS Parole & Probation Div	1
City of Las Vegas	1	North Las Vegas PD	3
DMV	4	The Attorney General Office	2
DPS	1	Sparks PD	1
Henderson PD	2	Health and Human Services	5
Las Vegas Metro PD	62	West Wendover PD	1
Mesquite PD	9	Yerington PD	1

Now, I would like to move from the national level to what we are doing in Nevada.

In Nevada, the Bureau has allowed unlimited access licenses to any law enforcement or criminal justice agency. Currently, there are 98 Nevada users. They only use the system to submit inquiries. No Nevada agency currently supplies data to NDEX.

Various District Attorneys' Offices and Sheriffs' Offices hold licenses, as does DMV because it has a law enforcement entity. Among the others are Parole and Probation, and North Las Vegas. The Attorney General's Office has two licenses. Even Health and Human Services, in its law enforcement capacity, have the ability to query the NDEX system.

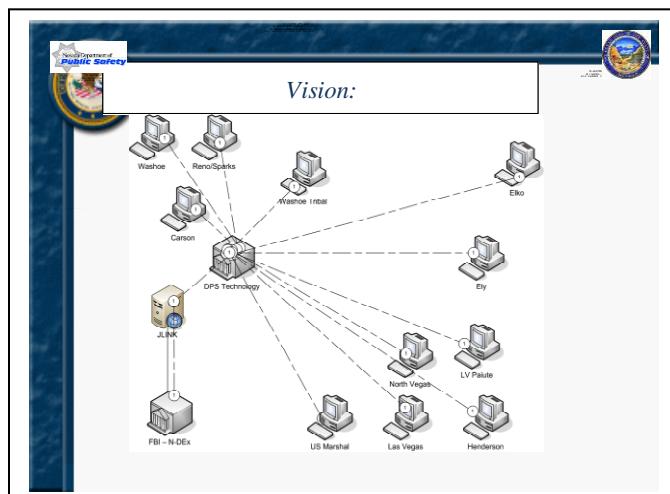


As I said, no one in Nevada currently submits data. We are working at changing that. We have a two-fold plan. I will go into that. DPS is connected to the Bureau through the CJIS division. This is a WAN connection. All agencies are connected to DPS through their various connections that establish the CJIS WAN.

A recently completed 2009 survey showed that there are 58 Nevada agencies that have some form of Record Management System (RMS). Twelve are police departments. Ten are sheriff's offices. Six district

attorney's offices and nine courts. The 21 others are different agencies. Several are within the Department of Public Safety, alternative sentencing, juvenile services, and fire investigators.

These records management systems could be mapped to, and supply data to, the exchange data program.



Our vision is to have all agencies supply their data to the Department of Public Safety, which will then supply it to the CJIS division for inclusion in the NDEX program. We are currently working on a two-pronged attack. We have an immediate plan and a long term solution.

The Department has applied for Rural Stimulus Grant money. We should be notified of any award at the end of this month or in early September. We would identify roughly 11 agencies that currently have RMSs. We will work with those agencies to map their data, upgrade

the network connections to handle the data, and procure any necessary hardware and software to allow us to move data into NDEX.

We understand that if we included agencies in Clark County, Washoe County, Douglas County, Carson City, and then out to Elko County, we would have about 80-85% of the criminal record activity of Nevada. We could accomplish this with the one grant. I would term this a limited success. This is our initial goal.

The future is really our long term solution. Here I would like to commend the collaborative effort between the Nevada Sheriffs and Chiefs Association and its members and our Director, Jerry

Hafen. These groups are taking recent stimulus money that may be flowing through JAG, the justice administration grant, and combining the funds to allow for the purchase and deployment of a state-wide RMS for all agencies that have antiquated systems or have no systems at all.

We would bring the State into the 21st century with this deployment and be able to feed Nevada information into the national system. This would make our information available to us through the NDEX. We would be able to compare our criminal activity to that taking place in California, Oregon, Washington, and to other states.

This will really to support intelligence-led policing – a catchword – but a meaningful one. It will support the Fusion centers so they can see what we are doing in Nevada in comparison to the other states. They can set up regional views of the data that can be expanded or limited as desired. This is the long term objective. This is what we really need in the State.

I would like to bring your attention to something else. I normally open this topic with a joke. Does anyone know where the last stagecoach robbery in the country occurred? Jim, you can't answer this.

It was 1906 in Jawbridge, Nevada. Does anyone know where the first confirmed utilization of NDEX assisted in solving a crime? It was done by North Las Vegas Police Department in October, 2008. I would like to give you a very quick rundown.

North Las Vegas Police Department received information that an individual named "Peanuts" living at a particular address was dealing drugs – including dealing to juveniles. The case was assigned to an analyst to build up additional information because all they had was the name "Peanuts" and the address.

The analyst went to the normal data banks – SCOPE, their CAD system, the RMS, LVMPD's accessible records, and NCIC. He accessed Gang Net – in short, a variety of incident and intelligence data bases. He was trying to identify this person, known only as "Peanuts". He had no results at all.

A subpoena to the power company allowed them to identify who had applied for power. That returned a woman's name and an associate's name. I will use my name for that of the associate, P.K O'Neill. So, the analyst took the name "P.K. O'Neill" and ran it through all the data bases, but he was unable to identify anyone. They did locate a "P.K. O'Neill" in Cal-Gang, the California gang intelligence data base. However, when they pulled up the picture and the physical description, it did not match that of the person that had been seen at the residence.

As a last ditch effort, some would say out of frustration, North Las Vegas had just received a users license for NDEX. He went to the dispatcher and ran an NDEX search on the woman's name. It immediately returned a call for service out of the Los Angeles Sheriff's Department two years prior regarding a domestic incident. The other individual identified was "P.K" with the nickname of "Peanuts".

They were able to pull up that photograph, and I can tell you that it matched the individual living at the residence. It also showed that the individual had a warrant – a felony warrant. The individual had an extensive criminal past including a variety of assaults, sexual assaults on minor children, assaults on police officers, and use of deadly weapons, firearms, during his assaults.

What might have begun as a "knock and talk", where law enforcement just goes up, knocks on the door, and see what occurs, ended up with law enforcement hitting the house with a search warrant in the early morning hours. They recovered several ounces of rock cocaine, limited amounts of marijuana, small amounts of money, numerous firearms and ammunition. This came solely from what had been developed out of NDEX.

I am very proud of this; first, because it occurred in Nevada, and second, because it really illustrates the value of the program. Even the smallest amount of information, here, a call for service that was two year old, became important. I can not say what would have happened on a “knock and talk” at that North Las Vegas address, but I know one thing – something I have seen too often – officers go to a door and do not know what is on the other side – unfortunately the end result is attendance at a funeral within days.

I believe deeply in this program. I complement the way our Sheriffs and Chiefs are currently addressing the issue in unison with the Director of Public Safety.

Lastly, the FBI supplies this at no cost to any law enforcement agency that would like to utilize the program. The Bureau enters its information as does the Bureau of Prisons, ATF, and DEA. NDEX allows us to see their information as well as that of local information. I complement the Bureau not only for developing the program, but also “walking the walk”.

Are there any questions?

AG CORTEZ MASTO:

Thank you, P.K., for that very informative presentation.

Agenda Item 7 – Presentation by Sergeant Troy Barrett, LVMPD, Internet Crimes Against Children, Organization in Nevada and Current Issues (Discussion/Action Item)

AG CORTEZ MASTO:

Agenda item 7 involves a presentation by Sergeant Troy Barrett on Internet Crimes Against Children. Sergeant Barrett is attending from Las Vegas.

SERGEANT BARRETT:

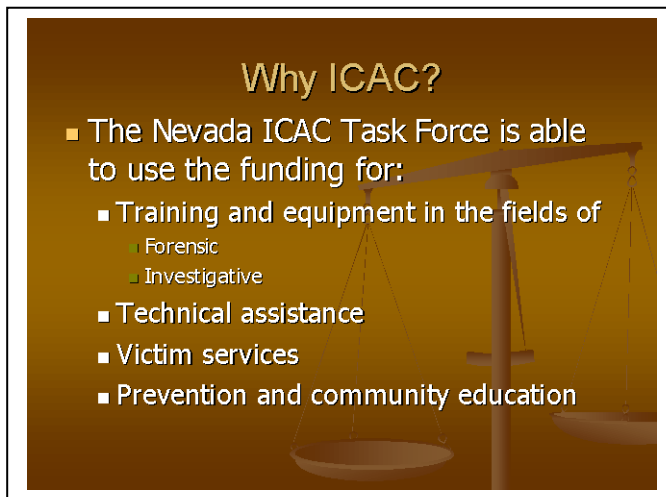
Good morning, Madame Chair, ladies and gentlemen. Thank you very much for your time. I want to provide a bit of background on what ICAC is and what we do. I know many of you are aware of it, but you have also probably seen many PowerPoint presentations in the last year.²

The Internet Crimes Against Children (ICAC) program was created to assist state and local law enforcement agencies in developing an effective response to cyber enticement and child pornography cases. The Las Vegas, Nevada task force is one of 63 in the country. Each of these task forces have meetings quarterly; the commanders talk about relevant events and national issues. The funding comes from the Department of Justice. The national task force also has liaisons with other countries including Australia, Canada, England and Germany.

Who do we work with? First, we work with the AUSA, the United States Attorney's Office, also the FBI, through its Innocent Images Task Force, also ICE, Immigration and Customs Enforcement, the U.S. Postal Inspectors, INTERPOL, the Air Force Office of Special Investigations, especially in southern Nevada considering Nellis Air Force Base, the Nevada Cyber Crimes Task Force, the Clark County District Attorney's Office, the Washoe County District Attorney's Office, and Nevada Parole and Probation.

Who is on the ICAC Task Force? That list includes Las Vegas Metropolitan Police Department, which is charged with being in charge of the task force. We are the administrators of the task force and the grant associated with it. Listed alphabetically, others include Carson City Sheriff's Office, Clark County School District Police Department, Elko County Sheriff's Office, Elko Police Department, Henderson Police Department, Lyon County Sheriff's Office, Mesquite Police Department, Nevada Attorney General, North Las Vegas Police Department, Washoe County School District Police Department, and the Washoe County Sheriff's Office.

² Not all of the slides presented to the Board are incorporated in these minutes.



Why do these organizations join ICAC, and what benefits do they derive? The largest issue is funding. Funding from the Nevada ICAC Task Force is used for training and equipment in the fields of forensics and investigations. The equipment is probably the biggest thing. Many of you will be aware that with computer technology, the speed and memory of computers doubles every 18 months. This means that the bad guys' computer memory and speed doubles every 18 months. The equipment we use to do the forensics and to go on line and look for these guys has to keep up the pace. It is an on-going

battle and a huge expense. The training is never ending also. Just when we get all the training up to speed, after Windows XP comes Vista. Next up is Windows 7. Nor can we forget about Apple or Linux. The training requirement is continuous. These two things mean there is a never ending need for money and supplies.

We also help with technical assistance, victim services, prevention and community education. Technical assistance is provided to everyone in the State of Nevada, whether they are a task force member or not. Dennis Carry helps out a lot in the north. We and the Attorney General's Office in the south provide assistance to those who need assistance with computer forensics. There are many departments that do not have the capability of doing a forensic examination on a computer.

Turning to prevention and education, we have partnered with Nevada Child Seekers. Nevada Child Seekers is able to go out to the schools and give presentations on Internet safety to children. This frees up the time detectives can spend more time getting the bad guys, although we do presentations occasionally.

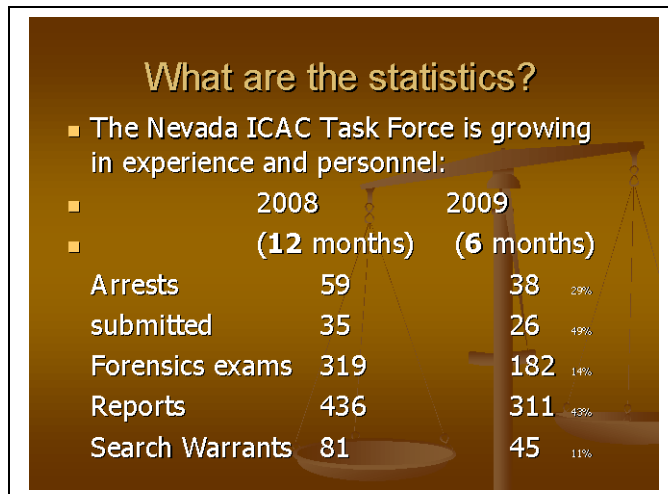
What crimes do we handle? The one you hear most about is child pornography, also enticement and the use of technology to lure a child. This includes something you might have seen on TV several years ago with Dateline, and To Catch a Predator. We also deal with obscenity and lewdness with minors – basically all crimes that have to do with a child, a computer, and are, in some way, sexually related. This is never ending. It is growing all the time. And, as you have heard from testimony up north, it is getting larger and larger.

What else does ICAC do? We conduct proactive and reactive investigations on the Internet. In our proactive mode, we go on line and pose as children. We also go on line to see who is out there and what they are doing. That involves a lot of training and more equipment.

We forensically examine computers. This is the biggest and most essential thing that ICAC does. It takes the most amount of time. Traditionally, we used to say the average size of a computer was 500 GB. We are starting to approach an average size of a terabyte. Now, you can buy a terabyte hard drive for a little over \$100. Unfortunately, we are also starting to find RAIDed systems. Basically, these systems can have three hard drives that act as one. When a system like that is being examined, you need a forensic system that can take in every bit of data in order to do the examination in support of a later criminal prosecution.

We also provide training for professionals. Not only do we provide training for detectives, there is also training available through the national task force for prosecutors and for parole and probation officers. We host our own training here in Nevada and also send personnel off to national conferences. This year, for example, ICAC will be sending 12 to 13 individuals to the Dallas Conference for Crimes Against Children on an all expenses paid basis. This is in addition to the 10 or so people that will be attending courtesy of the FBI. Again, training is continuous.

We host community awareness events in education.

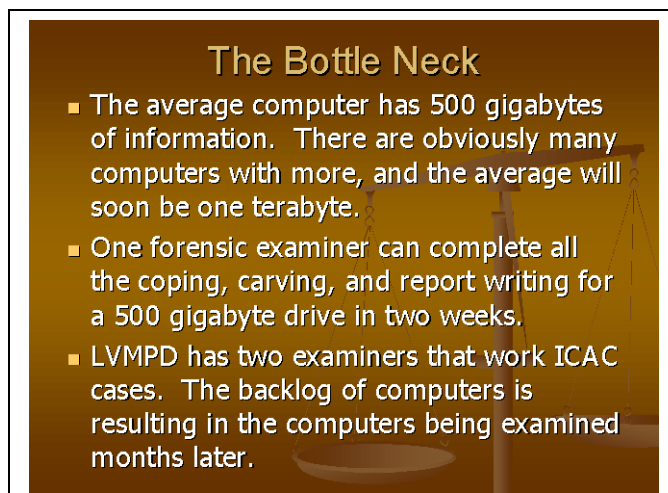


Here are some numbers. These are numbers for just the Nevada Task Force. These are current. We are comparing the entire year of 2008 and the first six months so far of 2009. Last year we had 59 arrests. So far this year, we have arrested 38. We are on a pace to get to 76 arrests by the end of the year – a 29% increase in the State.

Turning to submittal cases, last year we had 35. This year we have had 26, putting us on a pace to get to 52 by the end of the year. That would be a 49% increase.

Turning to forensics exams, last year there were 319. This year, so far, there have been 182. That is only a 14% increase in the number of exams, but that does not account for the increased size of the suspect's computers. Larger hard drives means more time spent by a forensics examiner on any given case. The forensic aspect of these crimes just chews up so much time.

Last year, 436 cases were reported. So far this year, there have been 311. We are on a pace to get up to 622 – a 42% increase.



The final statistic I want to mention is search warrants. Last year in Nevada, we had 81 search warrants. This year to date we have had 45. That represents an 11% increase anticipated for the entire year.

Here is the result of all this. I have had my investigators slow down their proactive activities. This is due to the backlog of computer forensics. Basically, we are creating a bottleneck.

As I have said before, the average computer has about 500 GB of information. There are many that

have more. We have had recent cases with 3 terabytes (3 TB). We had to purchase more equipment just for that case.

On average, a forensic examiner can complete all the copying of the hard drive, all the carving, and reporting of a 500 GB hard drive in 2 weeks. They have to ensure the working copy matches

the suspect drive on a bit-by-bit basis. They have to check every image when possible. Obviously there are some exceptions. In Dennis Carry's case of a million images, well, you just can not check them all. Additionally, an examiner has to describe to the prosecution each image in detail. This just chews up so much time. The backlog is just out of hand.

The Bottle Neck cont.

- It is not difficult for Detectives to locate the suspects for new cases, it is difficult to have the cases ready for prosecution in a timely manner.
- The problem is nationwide within law enforcement. The backlog of forensic work needed is the Achilles heel of ICAC.
- We need more forensic examiners to keep up.

Currently, LVMPD's backlog is multiple months. We are getting close to having a year backlog.

If I got 10 more detectives, they would be busy on the proactive side non-stop. There are enough bad guys out there. But, the forensics of the computers – that is what is really hurting our effort.

This problem is not Nevada specific. It is nationwide. All the ICAC units are discussing it. This is truly the Achilles heel of ICAC – computer forensics. It is what slows us down, and what keeps us from making arrests.

The US Attorney's Office and the Clark County Attorney's Office require a complete computer forensic exam before they will take on a case. So, we have the guy, we do the search warrant, we have the computer, we have a confession, but until the computer forensics are complete, no arrest will be made.

Basically, we need more computer forensic examiners to keep up.

This brings me to the stimulus grant. Recently LVMPD was awarded a stimulus grant that covers a period of 4 years. Obviously, the biggest need is computer forensics. For the first time, we are going to hire a full-time forensic examiner for this 4 year period. The examiner will be assisting all of southern Nevada with forensic needs. This does not mean just LVMPD. It means all of southern Nevada within traveling distance. Obviously, we do not want to ship computers by mail.

Why southern Nevada? First, the average salary to start in the public market is \$90 K per year. We simply did not have enough money to consider hiring multiple forensic examiners. Southern Nevada has the highest population and the largest number of cases.

However, Washoe County is certainly working hard in the north. I have talked to Detective Carry, the annual grant we have received is enabling him to continue getting things done in the north.

We are also working on a Nevada ICAC Task Force logo. The task force, again, is not LVMPD, rather, it is all Nevada. We are partnering with Nevada Child Seekers and the Las Vegas Art Institute. They are assisting with logo production for non-profit organizations. Obviously we are not making any money, so they are helping us. These are the final designs we have. I am partial to the one on the left. We want something that quickly identifies us.

The largest current issue we have is sexting. It is occupying a bunch of investigator's time. This is true not only in Nevada. The concern is nation wide.

In the old days, Johnny and Susie used to go behind the barn. One person would show their parts, and the other would show their parts back. Now, due to technology, Johnny and Susie are no longer behind the barn. They are using a cell phone.

Sexting

- This issue has had the largest impact with ICAC's around the nation.
 - Johnny and Suzy used to go behind the barn
 - Johnny and Suzy now use a camera phone
 - Taking the image is a felony, transmitting the image is a felony, and possession of the image is a felony.
 - By the letter of the law, kids are facing serious charges and sex offender registration requirements for years

Technically, when sexting, Johnny and Susie have committed a whole bunch of felonies. Taking the image is production of child pornography – a felony. Transmitting the images via the cell phone is transmission of child pornography – another felony. Finally, possession of child images is another felony.

So, we have two kids who used to go back behind a barn and this was not considered much. Now, we have three felonies and possible sex offender registration for life charges coming into play.

This does seem a bit much. So, the way we are handling them is this. Children of similar ages who share pictures – essentially the updated behind-the-barn scenario – are handled by us in the exact same way. We contact the parents and ensure they are notified. A parent needs to be notified not only of the act itself but of the dangers associated with it. Once an image goes on the Internet, there is no way for law enforcement to take it back. It is out there – forever. If we could take them back, life would be easier for us. But once it is out there, you can not get it back.

Once we advise parents of the dangers to correct some of the things the kids might be doing, we ensure that the cell phones are destroyed. There are software programs out there that erase data. However, there is always a chance that something might be missed. In no way, shape or form, would we ever want contraband, somehow in our possession, to be released back to the public. So, anytime we get any type of electronic evidence that contains data that is contraband, those items are destroyed at the conclusion of the case.

If we have a case where a child is sharing their sexting photos with an adult, we treat it differently. My apologies, I probably did not do a good job of describing sexting. Normal texting is where written communications are sent back and forth. Sexting is where kids take pictures of their private parts and share those pictures back and forth.

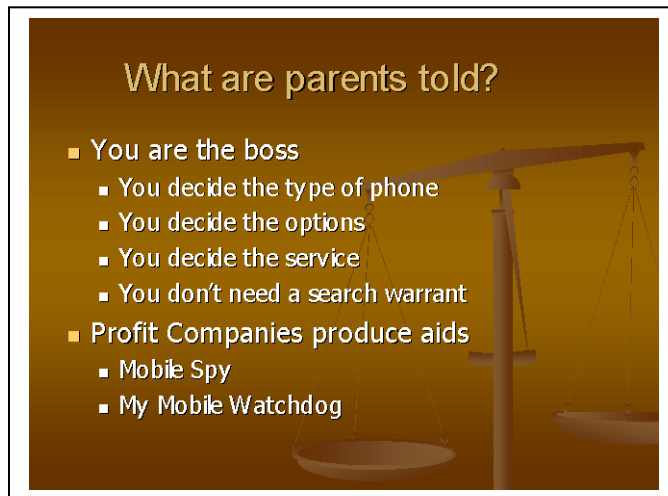
We handle sharing sexting photos with an adult as a criminal case. We now have an adult in the play. So, this is no longer just Johnny and Susie behind the barn.

When kids begin sharing their photos with a larger group of individuals, a school for example, different concerns come into play. This often occurs in the case of a breakup. As many of us will recall, school and high school relationships do not always last a lifetime. Sometimes they last only weeks or months. During the course of a breakup, pictures might get more widely distributed.

In cases like this, we try to identify everyone who has possession of those phones and cameras. Again, we want to get the contraband into our possession.

The case elements will be discussed with the juvenile District Attorney for recommendations. Sometimes we are dealing with bad decisions, sometimes we are dealing with a pattern that qualifies as a criminal act. There are several choices for the juvenile DA. Counseling may be appropriate. Community service, probation, and, if warranted, detention, are alternatives. Finally, all the phones containing contraband would be destroyed to ensure contraband does not go back into the public.

When we contact the parents, what do we tell them to do? Number one is, "You are the boss. You are not your kid's friend. You are in charge. You are responsible for them, and responsible for ensuring they are ready to go out into the public as adults."



Parents get to decide what kind of phone the child has. They get to decide whether it has a camera. They get to take a drill bit to the camera if they so decide. They get to decide the options and the service. Texting is not automatic. It can be withdrawn. It can be reduced or restricted. The phone numbers the phone can dial to can be restricted and from what numbers the phone can receive a call.

Lastly, "As a parent, you do not need a search warrant. You are not a police officer. You have the right to go in and look at your kid's stuff. Find out what they are doing."

There are also some for-profit companies that have tools to help parents monitor their children. Here are two that I have found, Mobile Spy and My Mobile Watchdog. These applications provide the parents with a copy of any text messages their child receives. The same is true of pictures.

In closing, thank you again for your interest and attention. As our society continues to become more comfortable with technology, and as technology becomes more affordable, we must ensure that we renew our capabilities to protect those that can not protect themselves. I would also like to congratulate Detective Carry on his new facility. To the Sheriff, great job for ensuring that did happen. Thank you.

AG CORTEZ MASTO:

Sergeant Barrett, thank you very much for appearing today and presenting to the Board. We appreciate the information you have provided. Are there any questions or comments? Hearing none, thank you again.

Agenda Item 8– Mortgage Fraud Update, Attorney General Catherine Cortez Masto (Discussion/Action Item)

AG CORTEZ MASTO:

Moving on to agenda item 8, which is an update on mortgage fraud from members of the Board. I would to give you a sense of what is happening in my office with respect to mortgage fraud.

As we all know, and as we read in the papers and hear from others, we lead the nation with the number of foreclosures in our State – one of every 14 homes is going into foreclosure. As a result, we are seeing a number of individuals coming into the State to prey on the people going into foreclosure. My office has been very busy investigating and prosecuting individuals who are engaging in foreclosure rescue scams and loan modification scams. We currently have 113 cases to investigate and prosecute. That number is growing, unfortunately for us.

You should be aware that we have the ability to prosecute these individuals thanks to the proactive nature of our Legislature. There are currently 17 different statutes that support criminal prosecution of these individuals. Unfortunately for them, many other states do not have similar

statutes. They have to deal with the issues solely through possible civil remedies. We are fortunate in that sense. We are unfortunate in that we lead the nation in these types of cases. It seems to me that many individuals engaged in criminal conduct come here to prey on unfortunate individuals. We will continue to investigate and prosecute in the State those persons who prey on our citizens.

Having said that, my task force works with local agencies. We work with local law enforcement. We work with federal law enforcement as well. Not only do I have a strike force in my office, there is also a federal strike force engaged in doing the same thing – investigating and prosecuting mortgage fraud issues.

The unfortunate thing for all of us is that there are more than enough cases to go around. My personnel sit on the federal task forces as well to ensure we are not wasting resources by investigating and prosecuting the same type of cases. In actual fact, we are sharing resources. Moreover, we are sharing the types of cases the State will handle versus the types of cases that federal authorities will take.

We have been engaged in this endeavor for a year and a half. We will continue to work in these issues.

I want to thank our federal partners. Without them, we would not be able to get a handle on the number of issues that face us in the State. Two weeks ago, I returned from a meeting in Washington, DC with a handful of other Attorneys General who faced similar problems. We met with individuals from the Department of Justice, Homeland Security, the Treasury Department, the Federal Trade Commission, and the U.S. Attorneys Office. I understand that, after that meeting, federal agencies are trying how they can assist states in addressing mortgage fraud cases. That was the first time my counterparts and I were able to sit down with our federal officials and discuss how to best work collaboratively to address these issues.

I want to continue that dialog as do the other state Attorneys General. We are hearing the same thing from our federal counterparts.

The FBI was represented in these meetings. Mr. Martinez, you and I have not yet had an opportunity to sit down and talk one-on-one. I am hoping that the next time I am in Las Vegas, we will have the opportunity to talk a little bit more about the working relationship we have. I am not sure you are still in Las Vegas, but my intent, on behalf of the State, is to continue to address the mortgage fraud issues. There are several other aspects that I can not go into specifically now, but you will see more involvement from the State level to address these frauds.

Are there any questions or comments with respect to mortgage fraud issues?

SENATOR WIENER:

I think you said there were 113 cases? Do they involve 113 different entities that are preying on our citizens, or do some of those cases involve the same entity?

AG CORTEZ MASTO:

They are different cases unfortunately. The cases are very complex. We may start dealing with a mortgage rescue scam, but will find that the same individuals have created sham companies, which have extended their illegal activities to include, for example, some type of broker fraud or another type of real estate fraud. Since they are complex, it takes considerable time to investigate and move through the process to get to the point of prosecution. Unfortunately, most of the cases we have are different in nature, and deal with either a loan modification scam or some sort of rescue scam.

SAC MARTINEZ:

Madam Chair, if I may. I would like to piggyback on your presentation by giving a quick update on where we are with the mortgage fraud task force we have had in place in southern Nevada since March of 2008.

The FBI has a very rigorous and sophisticated means of doing threat-based resource allocations. I am required to meet with the Director personally over a secure video conference link once a quarter in order to brief him what we are doing and why.

Mortgage fraud did come up on our radar screen, and we have prioritized it over the past year and a half or so as our number one white collar crime threat in Las Vegas. That is part of what prompted us to pull the task force together. Currently, we have the FBI, Postal Inspection Service, IRS, Las Vegas Metropolitan Police Department, the Secret Service, the Nevada Attorney General's Office, HUD's Office of Inspector General, and, of course, the U.S. Attorney's Office, which has been extremely supportive of our efforts in this area.

Part of the effort in kicking off the task force was to set up a hot line. To date, we have had 2,600 calls that have been received and processed. Currently we have approximately 45 subjects already charged by the U.S. Attorney's Office. We are projecting about another 50 within the next 90 days or so.

Asset forfeitures are exceeding \$125 million in this effort. We have over 71 cases currently open. We have targets identified through a very sophisticated process that looks at suspicious financial activity reports using our analytical resources in our field intelligence group. They have identified probably another 300 individual targets that represent frauds in excess of a million dollars. We have a huge amount of work to do. Our headquarters has responded. Our staff has temporarily expanded to include an additional 3 or 4 agents over the next several months. We will have a permanent increase of 7 special agents coming in to work white collar crime, primarily mortgage fraud. We have received an increase of two financial analysts, who will join the one dedicated financial analyst we have now working these issues. We also have a dedicated intelligence analyst that supports the mortgage fraud effort.

So, there is a lot of work that has been done. I think we are having a huge impact, but there is still an awful lot of work yet to do. Our national headquarters has responded. It has identified Las Vegas not only as a lead in the size of the crime problem, but also as a lead in the means taken to address the problem. We have some very innovative ways of going at these cases. We do not want to stretch out the investigations to two or three years. We have been working very effectively with the U.S. Attorney's Office to come up with novel ways to approach these cases. Perhaps "fast track" is not the right term, but we do have the means in place and an investigative strategy that really moves the time line up to get these cases through to prosecution.

There is a lot going on at the national level. The Department of Justice and Congress have been responsive to build up our personnel assets. It is very unusual for an office the size of the FBI office in Las Vegas to get that large an increase in assets to address a particular crime problem. We have been very successful in, first, demonstrating the amount of work that needs to be done here, and, second, the ability to take a very efficient approach to knocking this problem down.

I do encourage you on your next visit to come down so we can talk about what is going on. If you or anyone else has questions or wants information about what is going on in the mortgage fraud task force, I would be happy to entertain them.

AG CORTEZ MASTO:

Thank you. Are there other questions or comments?

SHERIFF HALEY:

Yes. This is Sheriff Haley. To what extent do you perceive that the folks you are dealing with in Las Vegas, the perpetrators of these crimes, once they have picked up the hint that things are about to go sideways, that they then are migrating north? Obviously, I am concerned about that. We do not have anything near the size of the Las Vegas problem in the north, but we do GIS-map [Geographic Information System] all of our foreclosures. We have a significant number per capita. I am concerned about the migration of perpetrators issue.

SAC MARTINEZ:

Mike, my response to that would be that one of the aspects of these crimes is that there is a very good paper trail. So, once we have done the analysis, and that includes a process involving the intelligence analyst and follow-on investigation by an agent, these cases fall fairly neatly into place because of the paper trail that is created in doing the financial transactions. I do not want to oversimplify here. Until we make contact with an individual, they are not necessarily going to have any idea that they are being investigated. Now, the word is probably out that we are working this hard. I suspect that there may be some people who will migrate looking for another place to do their business. I think we have probably seen that in the past.

We probably need to get together to talk about it. If you have someone in your fraud unit who wants to pay us a visit, or get on the phone with Scott Hunter, our supervisor here, we could take a look at who you might suspect in the north. We can work it together from there. I am absolutely open to having that discussion.

SHERIFF HALEY:

I appreciate it very much. Thank you.

Agenda Item 9 – Presentation by Mr. Bob Young, Executive Vice President, Public Engines, Inc, on the proprietary services CrimeReports and CrimeCentral, crime share and analysis web-interfaced software services (Discussion/Action Item)

AG CORTEZ MASTO:

Hearing no other comments, let's move on to agenda item 9. Mr. Young.

MR. YOUNG:

Thank you very much, Attorney General. My name is Bob Young. I am here to talk about CrimeReports.

We are currently the largest crime-mapping and crime-trending company in the United States. My colleague and I met with Attorney General Cortez Masto and the Executive Director, James Earl, to discuss a plan to institute a centralized view of crime data and crime instant data and trending to support better resource allocation and standardized views of crime.

It is a great tool. It allows for the tracking of policy management as regards crimes such as domestic violence and drug trafficking. We have deployed this now in two full states, Utah and Maryland. We are in our second year. It is a fully automated system. It does not require daily resources to run. It updates at least once a day with crime data. It allows for a uniform crime view, and you will see this in our presentation. It is truly made for command and staff level views, and the ability to do crime-trending and crime-management.

Our goal, based on experience, is to get this up and running in Nevada by the end of the year at an extremely low annualized cost.

With that, I would like to hand over to Greg Whisenant. He is the founder and CEO, and is beginning to become a recognized face in the federal, state, and local space, given the success and reach of the company.

MR. WHISENANT:

Thank you, Bob. Good morning, Madam Chair, and members of the committee. Bob gave a great company overview.

I started the company about two years ago. I will get into a little bit of detail in a moment.³ I especially appreciate Senator Wiener still being here, so you can hear a bit of how we approach individual states in that we coordinate directly with legislators.

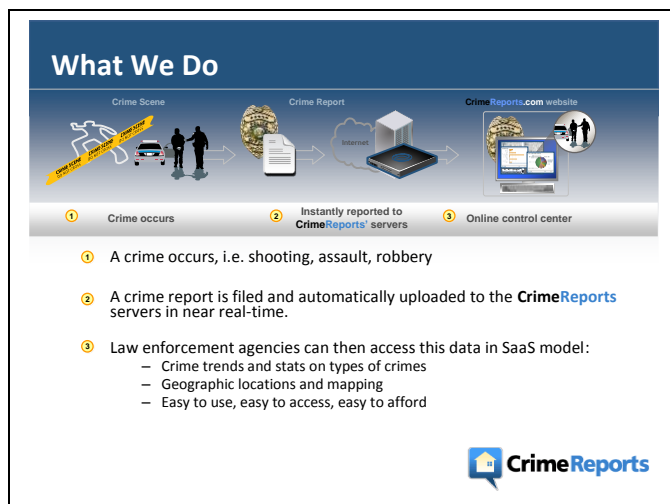
As an overview, I have to say we work for law enforcement. We have a great deal of respect for law enforcement. Our goal is not to function as an open records organization. We are a vendor to law enforcement to help them do their jobs more effectively. We want to lift some of the technological burden that they might otherwise have to do on their own.

Our company helps local law enforcement share and organize crime data in a way that they manage and control. It is easy to install – often the same day. It is low cost, so there is no hardware, software, or maintenance fees. It is near-real-time with no specialized skills required.

As Bob mentioned, we are the largest single-view crime mapping company in the world. We now work with nearly 600 local law enforcement agencies. We have had a 100% successful integration rate with more than 60 CAD and RMS systems nationwide.

Finally, as Bob mentioned, we have statewide deals in Maryland and Utah that were both renewed recently. We have also been featured in national publications. We do not have packets for those members not located in Las Vegas, but we did drop off some brochures and other items including a copy of the Wall Street Journal article that came out. We were on the front page of the Wall Street Journal two months ago. I believe it was June 8. They talked about how neighborhood watch is going online. We have been fortunate to have been able to participate with our law enforcement partners in having positive press.

I was not a party to the original conversation several weeks ago with Attorney General Masto and the rest of the team. As I understand it, the priorities for Nevada law enforcement are a cross-

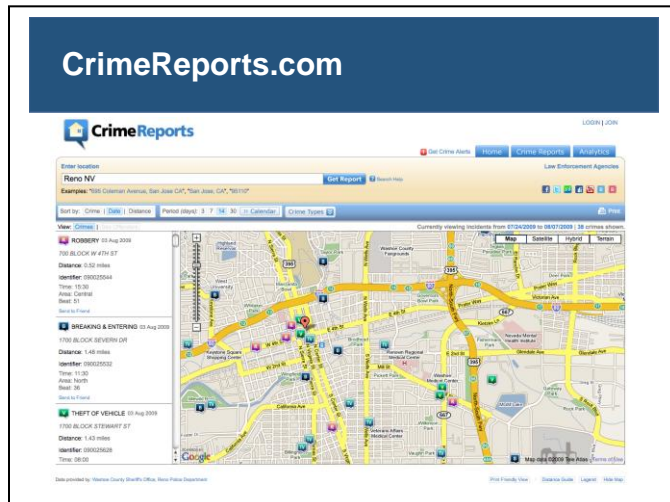


jurisdictional view of crime trends and incident reporting, uniform crime report definitions, a crime repository, and the ability to integrate with various CAD and RMS systems and even spreadsheets for small agencies, and a Nevada-compliant, secure, encryption-based data transfer system. Specifically, for Attorney General Masto, priorities are statewide, near-real-time crime trending interfaces for policy analysis and resource allocation, a consistent, near-real-time analysis and trending of drug incidents (such as meth labs and narcotics trafficking), and, maybe, specific types of incidents within the uniform crime reports definitions that are of special

significance, and state-wide trending of major civil offenses such as insurance fraud, mortgage fraud, and senior fraud, and inclusion of numerous small agencies for a complete view.

³ Not all of the slides presented to the Board are incorporated in these minutes.

Very basically, here is what we do. A crime occurs. Everyone will be familiar with CAD and RMS systems. When I explain this, I usually ask if people have called 911. I have before. It is just like on TV. They ask, "What is your emergency?" Once a police department has verified that a crime has occurred, collects that information in their RMS system. So the record moves from CAD to RMS. It is moved over to CrimeReports in near-real-time. We can have that be as often as within minutes or, minimally, at least once a day. So, next day, the crime data is available.



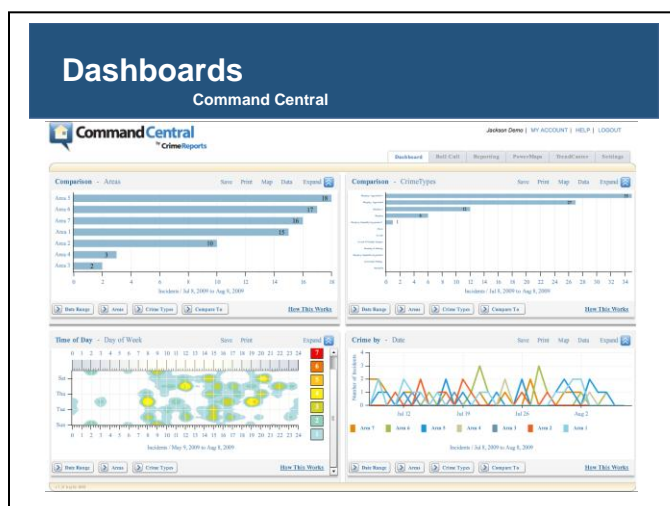
This is a screen shot of the web site I took last week for Reno, one of our participating agencies. This was taken on August 4th. As you can see, there is date from August 3rd on the web site.

We have had a lot of compliments from the general public about how easy it is to access this data, and how all they have to do is pull up the web site, type in their city name, and they are able to access next-day crime data in a visual format. The cost of delivering this service to agencies is, well, put it this way, they spill more in coffee every month than they would spend on our system.

That is really true. We charge either \$100 or \$200 per agency per month as a total fee for the CrimeReports service.

Our second tool is CommandCentral. As we work with law enforcement agencies, we go around and talk directly to them. This was defined as a priority by all of our customers. They have all said that they did not have the ability to see in near-real-time, at a beat level and at a street level, what crimes are occurring and when and where.

CommandCentral is a response to that need. Although this is not an interactive screen shot, if I were on the live web site, you would see that all the elements on this dashboard are clickable. You can interact with them individually.



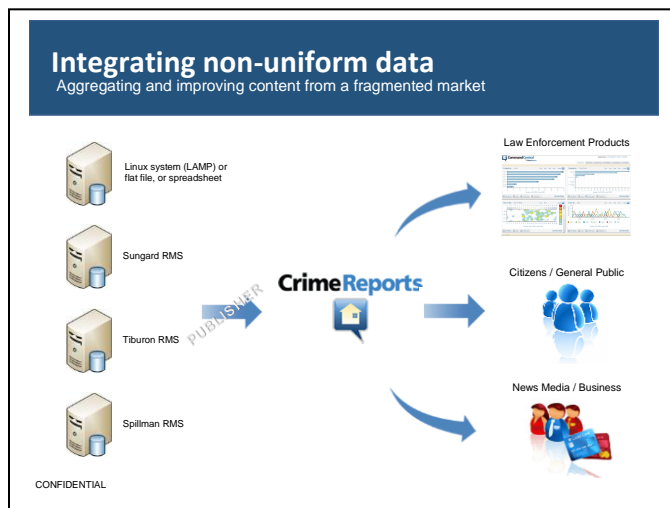
Let me touch on several so you can get a feel for it. In the upper left, you can see several areas that are defined. These are individual beats, defined and shaped by the jurisdiction. They are able to click down and drill down to see what the incidents are and where they occurred.

Below that is a time-of-day, day-of-week analysis, which shows a hot spot on the x-axis (days of the week) and on the y-axis (time of day). You are able to see when there is peak activity for resource allocation. You are able to change patrols and react in near-real-time to emerging threats

instead of waiting and analyzing them at a later date.

This shows crime trends over time. It is a unique part of our product suite. This is a part of CommandCentral as well. Normally, you would see a heat map that would show you where crime has happened. That is ubiquitous. This tool is different. We can now monitor the trend of crime over time. So, you can look at a very specific neighborhood, beat X, and ask whether crime is getting better over the last 90 days or is it getting worse. This tool will tell you that.

One of the key things for us, one of the reasons we have grown so quickly, is that we work with both huge agencies and tiny agencies. I think our largest is LA County Sheriff's Office. We also work with San Jose, San Francisco, Oakland, Portland, Boston PD, Baltimore, Buffalo – cities all across the country. Some of the small ones still have Linux systems or flat file or spreadsheet systems. We have no problem integrating with those. Sometime our integration time will be doubled, from two hours to four hours, but rarely beyond that. Our system is a simple one that will work with any agency.



We basically get a feed of XML data that uses the DOJ standards. This feeds into CrimeReports. The general public is then able to access it. One of the nice things is that there are no connections back into the original data. We do not have the ability to go into crime systems, CAD or RMS systems, at the agency level. It is a one-way push. So, when the public is looking at the data, there is no way to hack into the system and be able to trace back into the law enforcement systems. This is a key point for our agency customers.

I just want to touch on our data center very briefly. We have a secure

data center with networking processes for all customers. Our application is just a publisher that sits inside the network. It can query CAD or RMS. It is encrypted with SSL using a 2048-bit key. As I mentioned, it is a one-way data transfer. We never have access to agency servers for any reason or under any circumstances.

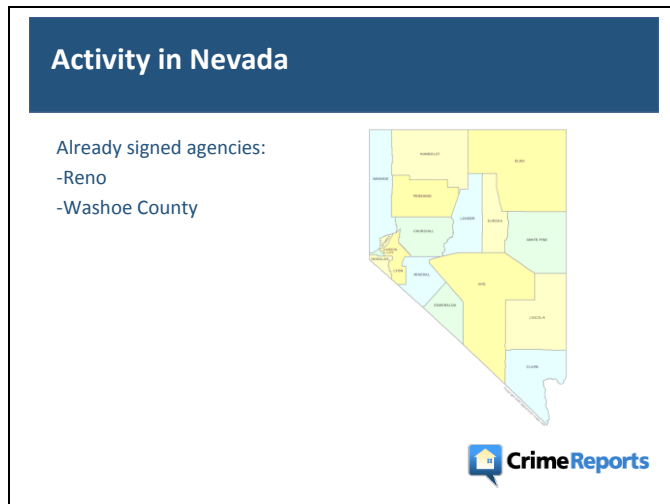
Our data center is SAS 70 certified. I assume that means something to my technological team and to the technology teams in law enforcement. I am not familiar with the intimate details of what that means. These requirements have been laid bare by law enforcement repeatedly, and we have either met, or plan to meet all of those expectations and requirements in short order.

Turning, very briefly, to our statewide projects, in Maryland, we launched with Montgomery County about a year and a half ago. I talked to Christian Mahoney in the Governor's Office on Crime Control and Prevention shortly after that. She said, "You know, the ship has already left port. We are working on our own mapping system statewide." I explained to her what we had. I left the office a little bit dejected, but got a call 5 weeks later. She said that even though they had allocated the resources, we have watched how quickly you have grown and how reliably you have integrated with agencies. We had 45 agencies online within 30 days in the state of Maryland. It is really true that we can do this quickly. They cancelled their RFP and decided to use their money in other ways. I think this is illustrative.

In Utah, we are based in Salt Lake City. We approached the legislature. It made a direct appropriation for a citizen impact board, or something to that effect. It was a transparency web

site for law enforcement. The money was given to the Attorney General's Office. The Attorney General, Mark Shurtleff, awarded that to us. That was renewed last year as well.

To date, we have had 70 agencies in the state join. Both agencies renewed their contracts in 2009.



In Nevada, we have just two agencies, Reno and Washoe County. I do not want to say "just". We are very happy to have them. I worked directly with individuals in Reno, namely, Steve Bigham. I appreciate the Sheriff being here today. Obviously, we would love to be working with the whole state. We think we can get things rolling very quickly by the end of the year.

I will skip over some of these slides. I know we are sensitive on time. Here are several quotes from the Gartner Group we will be able to provide at a later time.

That is all I want to say now. I would like to open it up for questions if any of the Board members have questions, I would like to field them now.

AG CORTEZ MASTO:

Thank you very much. Do we have any questions or comments? Hearing none, let me thank you for your presentation.

Agenda Item 10 – Consideration of Possible Legislative Initiatives

AG CORTEZ MASTO:

Turning to 10a. I want to throw this out as an idea – the possible continuation of the working group we had during the legislative session. Is this something we want to continue in order to work on future legislation that may come before us over the next year and a half to prepare text for the 2011 legislative session. I am curious to see if anyone has any comments.

MR. EARL:

I have done undertaken some background discussion with staff in various agencies. One of the items representatives from LVMPD, WCSO, and the District Attorney's Offices of both Clark and Washoe Counties discussed with Brett Kandt in the lead-up to the last legislative session was sexting and several other ICAC-related issues. Some of those discussions resulted in the legislation Brett Kandt has already discussed. However, there were certain issues, sexting being one, which we simply could not handle within the amount of time we had before the session began.

I also want to note that during the legislative session, Mr. Gammick, the District Attorney for Washoe County, expressed considerable concern about sexting. With that as a backdrop, I talked to Brett Kandt and others. I think I can fairly represent that the group that was formed informally to deal with these issues, as a result of presentations made before the Board a year ago, would be prepared to continue onward. Brett Kandt has volunteered to coordinate that effort. I believe this is a worthy endeavor.

AG CORTEZ MASTO:

I agree. I think this is a good working group. We may want to add a few individuals, for example, from DA's Offices that want to be involved that have not participated in the past.

In addition to sexting, I think Brett just brought up another issue when he talked about the definition of "minor" in our statutes. That is something else we should probably be looking at. I know Senator Wiener, before she left, volunteered to sponsor any legislation we agree on that comes out of this working group. I think it is a good idea to continue the dialog and discussion associated with the working group.

SHERIFF HALEY:

I would like to raise another issue that is a common theme. Earlier, I mentioned that it is very difficult for public safety and district attorney's offices to obtain the appropriate number of FTEs – people to do these jobs. It is also difficult to acquire the necessary skills and maintain the training, and handle the huge load. We need to address those issues and how we are going to keep up with the demand.

Additionally, we need to discuss whether to address these thing at the end-user level is more effective than addressing them at the point of origin, as is done in drug cases.

These two areas are vital for this Board to continue to review.

AG CORTEZ MASTO:

Are there any other comments? Is anyone opposed to continuing this working group? I see none. We will continue and we will go with Mr. Earl's recommendation that Mr. Kandt head the interagency group. The dialog will continue. I would ask, obviously, when you believe it appropriate, you come back before the board and seek our input as well on the various issues.

Moving on to item 10 b, Mr. Earl, are there other issues that need to be discussed?

MR. EARL:

There is nothing I have to suggest at this time. Sheriff Haley has mentioned several things in addition to the ICAC-related working group. If there other issues that Board members would like to identify now, that would be great. As time passes, I am always open and available either to add items to the agenda or to consider how to move forward on a sensitive issue we might not be able to address in a public forum.

AG CORTEZ MASTO:

Thank you. Let's move on to agenda item 11.

Agenda Item 11 – Board Comments (Discussion/Action Item)

AG CORTEZ MASTO:

Are there further comments from members on any matter or issue? Hearing none, let's go to agenda item 12.

Agenda Item 12 – Public Comments (Non-Action Item) :

AG CORTEZ MASTO:

Are there any members of the public in northern Nevada who would like to address the Board? I hear none, are there any members of the public in southern Nevada who would like to address the Board? It does not appear there are any. So, we will move onto agenda item 13.

Agenda Item 13 – Scheduling future meetings (Discussion/Action Item)

MR. EARL

Madam Chair, rather than try to set a particular date, I suggest the Board consider meeting within the first two weeks of November. That would be before the holiday season. I will undertake to poll Board members, particularly those that are hardest to schedule first, in an attempt to set a meeting date within those two weeks if that seems reasonable.

AG CORTEZ MASTO:

Thank you. Hearing no objection, we will move to the next agenda item, adjournment.

Agenda Item 14 – Adjournment (Action Item)

AG CORTEZ MASTO:

Thank you all very much for attending today. We are adjourned [at 12:10 PM].

Respectfully submitted,

James D. Earl

Approved by the Board at its subsequent meeting on December 17, 2009

Minutes of the Nevada Technological Crime Advisory Board

December 17, 2009

The Technological Crime Advisory Board was called to order at 10:00 AM on Thursday, December 17, 2009. Attorney General Catherine Cortez Masto, Chairman, presided in Room 3138 of the Legislative Building, Carson City, Nevada and via videoconference in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Tray Abney, Reno/Sparks Chamber of Commerce
Assistant Special Agent in Charge, Mark Doh (*Rep. for Special Agent in Charge Steve Martinez, Federal Bureau of Investigation (FBI)*)
Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)
Sheriff Mike Haley, Washoe County Sheriff's Office
Chris Ipsen (*Rep. for Dan Stockwell, Director, NV Dept. of Information Technology*)
Nevada State Assemblyman Harry Mortenson
Dale Norton, Nye County School District Assistant Superintendent
Assistant Special Agent Paisley (*Rep. for Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)*)
Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE)

ADVISORY BOARD MEMBERS ABSENT:

Nevada State Senator Valerie Wiener (Advisory Board Vice-Chair)
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association

TASK FORCE MEMBERS PRESENT:

Detective Dennis Carry, Washoe County Sheriff's Office (WCSO)
Jason Darr, Las Vegas Metropolitan Police Department
Robert Duval, Las Vegas Metropolitan Police Department
Talova V. Davis, Computer Forensic Examiner, Attorney General's Office (AGO)
Supervisory Special Agent Eric Vanderstelt, Federal Bureau of Investigation (FBI)

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director

OTHERS PRESENT:

Edie Cartwright, Public Information Officer, Attorney General's Office (AGO)
Ernie Hernandez, Health Division, Department of Health and Human Services
Theresa Presley, Health Division, Department of Health and Human Services
Ira Victor, InfraGard

Agenda Item 1 – Call to Order – Verification of Quorum

AG CORTEZ MASTO:

The meeting is called to order on December 17 at 10:00 AM

A roll call of the Advisory Board verified the presence of a quorum.

AG CORTEZ MASTO:

For the benefit of the Board, we are pleased to have Assemblyman Mortenson join us. He replaces Peggy Pierce. Welcome aboard.

ASSEMBLYMAN MORTENSON:

Thank you.

Agenda Item 2 – Discussion and approval of minutes from October Board Meeting

AG CORTEZ MASTO:

Moving on to Agenda Item 2.

MR. EARL:

I am ready to answer any questions with regard to the minutes. If there are none, I think the Chair would entertain a motion to accept the minutes.

Motion to approve the minutes was made by Sheriff Haley and seconded by Mr. Ipsen.

The motion to approve the minutes was approved unanimously.

Agenda Item 3 – Reports regarding Task Force activities

AG CORTEZ MASTO:

These are reports from agencies that are part of the Board, including the FBI, Las Vegas Metropolitan Police, US Secret Service, my office, Washoe County Sheriff's Office, and ICE. Mr. Earl, do we have anyone interested in providing information that you are aware of?

MR. EARL:

I believe so. The FBI normally leads off. Is there someone in Las Vegas who would like to provide that update?

ASAC DOH:

Madame Chair, I would like to introduce Supervisory Special Agent Eric Vanderstelt to provide an update on the southern Nevada task force.

AG CORTEZ MASTO:

Thank you very much. Mr. Vanderstelt, welcome.

MR. VANDERSTELT:

Thank you Madame Chair. Members of the Board, good morning. Thank you for the opportunity this morning to address you concerning activities of our southern task force since the last time we met.

In October, fifty-three defendants, the largest number ever charged in a cyber crime case were indicted in a multi-national investigation conducted in the United States and Egypt. The investigation uncovered a sophisticated phishing operation that fraudulently collected personal information from thousands of victims that was used to defraud American banks.

Egyptian-based hackers obtained bank account numbers and related personal identification information from bank customers through phishing attacks. Armed with the bank account information, members of the conspiracy hacked into accounts at two banks. Once they accessed the accounts, the individuals operating in Egypt communicated by text messages, telephone calls, and Internet chat groups with co-conspirators in the United States. Through these communications, members of the criminal ring coordinated the illicit on line transfer of funds from compromised accounts to newly created fraudulent accounts.

The United States part of the ring involved runners, who set up bank accounts where the funds stolen from the compromised accounts could be transferred and withdrawn. A portion of the illegally obtained funds were then withdrawn and transferred by wire services to the individuals operating in Egypt, who had originally provided the bank account information obtained by phishing.

In a coordinated take down conducted on October 7, arrests were made in California, Nevada, North Carolina, and in Egypt. Several individuals in Las Vegas were arrested as participants in this scheme.

On November 2, an individual was sentenced to 240 months in federal prison for receipt and attempted production of child pornography.

On November 16, an individual was sentenced to 78 months in federal prison for possession of child pornography after having previously pled guilty. The individual had been employed at the University of Southern Nevada and had used school computers to download images.

In December, a jury returned a guilty verdict against a man who had posted an ad on Craig's List, expressing an interest in meeting a juvenile for sex. An undercover investigator, posing as a 13-year old, responded to the ad. The man asked to meet him at a local area hotel. The man was arrested when he arrived at the hotel to meet with the juvenile. Sentencing in this case is scheduled for March.

These are some examples of activities that were conducted by the southern task force that I am able to share with you this morning.

AG CORTEZ MASTO:

Mr. Vanderstelt, thank you very much. Are there any questions? Hearing none, we appreciate your coming before us this morning. Are there any other comments regarding task force activities?

SHERIFF HALEY:

There is one project that continues to move forward. It originated out of the Sheriffs and Chiefs group and is being managed by Dick Clark from P.O.S.T. That is the RFP on the Records Management CAD System, which would cover both State agencies and law enforcement agencies that do not already have a records management system in the rural areas. I bring this up as a matter of information. The RFP continues to move forward, and we seem to be very close to vendor selection in order to start that project.

AG CORTEZ MASTO:

Thank you very much. Are there any other comments? If not, let's move onto Agenda Item 4, a report from our Executive Director.

Agenda Item 4 – Report by Executive Director

MR. EARL:

Thank you. Let me follow up on something Sheriff Haley just mentioned. Board members will recall that at the last meeting we received a briefing from the Department of Public Safety (DPS) on efforts to move forward with a record management system (RMS) and on the implementation of the federal N-DEx system.

As some of you will be aware, the presenter, Captain P.K. O'Neill, has now retired. As a follow-up, his replacement as Records Bureau Chief, Ms. Julie Butler, has asked that I inform the Board of the following as an update on both the RMS and N-DEx programs. She regrets she is not able to be with us this morning. This is the specific information she provided:

DPS RMS Update

The Department released a Request for Proposals for a Statewide Records Management System through the State Purchasing Division on November 12, 2009. The deadline for responses is January 19, 2010. The scope of work includes a replacement for the Highway Patrol's Computer Aided Dispatch (CAD) system and a Records Management System for the Department that eventually can be expanded to local law enforcement agencies that cannot afford to purchase an RMS on their own. The specifications for the RMS include the ability to submit incidents to the FBI's Law Enforcement National Data Exchange (N-DEx) system. There are other modules to the RMS that would include personnel, equipment, fleet management, and ad hoc reporting capabilities. Our ability to include those modules into the system that is eventually selected will depend on how the bids come in compared with our budget. We anticipate selecting a vendor sometime in March 2010 with a contract start date somewhere in the July-August 2010 timeframe. The delay between the vendor selection and contract start date includes time for contract negotiations and Board of Examiners approval. We are using federal stimulus (ARRA) money for the RMS. To my knowledge, we are not using Homeland Security Grant dollars for this project nor are we contemplating such at this time.

N-DEx Update

The Records & Technology Division received federal stimulus funds for the implementation of N-DEx to 9 local law enforcement agencies that have Records Management Systems of their own: Las Vegas Metropolitan Police Department, North Las Vegas Police Department, Henderson Police Department, Washoe County Sheriff's Office, Sparks Police Department, Carson City Sheriff's Office, Douglas County Sheriff's Office, Washo Tribal Police, and the Las Vegas Paiute Police. The funding is good for two years. Our original plan was that these 9 agencies would connect to N-DEx through our Division's existing connection to the FBI CJIS Division. However, we may have to re-think that due to some capacity issues on our end. We are in the process of setting up a conference call with the N-DEx office to explore alternative connection methods for these 9 agencies. Until we have that call, I really can't give the Board more specifics on how it will work or rolling N-DEx out to other jurisdictions beyond these nine as there are presently a lot of unknowns.

I would like to move on and remind the Board that one of the other issues addressed at the last meeting was the formation of a working group by Mr. Brett Kandt on sexting and Internet Crimes

Against Children (ICAC) issues. Mr. Kandt has asked that I inform the Board that the working group has been established. The group is reviewing documents relating to the sexting laws of all states that have such laws. He pointed out that many do not. This is the first step in their work.

AG CORTEZ MASTO:

Actually, it might be helpful for Board members' information, if we could get a list of the people who are working in that group to all of the Board members.

MR. EARL:

I will be glad to do that for our next meeting. I know a number of different law enforcement agencies are participating, but I do not have the exact information and I will get it.

AG CORTEZ MASTO:

Thank you.

MR. EARL:

The third thing I would like to talk about are contacts I have had with Congressional staffers in Washington DC as a follow-up to a letter written by the Attorney General to Secretary Napolitano.

I expect Mr. Ipsen will talk more about this in a later agenda item, but some of you may be aware that Nevada participates in a group called the Multi-State Information Sharing and Analysis Center (MS-ISAC). That group was established by, and funded by, the Department of Homeland Security.

As Board members will be aware, the Attorney General has written to Secretary Napolitano explaining the legislative success in the last session. She pointed out how those actions place Nevada considerably ahead of the power curve in a number of areas identified as national priorities in the President's Cyber Security Policy Review.

The Multi-State ISAC recently undertook its first information sharing with Congressional staffers. I was asked to participate as a member of a 15-person group to represent state interests to Congressional staffers. Perhaps the most important meeting we had was with the staff director of the Subcommittee on Emerging Threats, Cyber Security, Science and Technology of the House Committee on Homeland Security.

I specifically drew his attention to the points the Attorney General made in her letter to Secretary Napolitano, and reiterated, reasonably forcefully, the suggestion that the Secretary consider moving forward to augment the Homeland Security Grant Program with funds specifically set aside for cyber security projects within the states. I have exchanged several emails with the staff director on that, and can report that he thinks it is a good idea. The real question is whether his members will. He asked that I mention to the Board that the most important input he receives as a staff director comes from Congressional delegates. Given that we are coming up on a Congressional recess, I suggest Board members consider either taking the opportunity if it presents itself, or making the opportunity if it does not naturally occur, to speak with members of the Nevada Congressional Delegation regarding additional grant funds in the Homeland Security Grant Program that go specifically to cyber security issues. I should point out that the Attorney General's letter and my discussions laid emphasis on the fact that any earmarked funds for cyber security issues at the state level should be additional, so that information security officers were not forced to compete with funding for on-going projects that were already part of a long-term grant life cycle.

Moving on to the next item, I would like to draw the Board's attention to the continuing national interest in both the substance and the process associated with the passage of the Nevada encryption law, SB 227.

Since our last meeting, I have made presentations to the Intellectual Property Section of the Nevada Bar Association and have continued conversations with attorneys both in and out of CLE seminars held across the country. Mr. Ipsen presented a briefing on one of his trips to Washington DC to Tech America, the broad-based industry trade group associated with the high tech industry in the United States.

In the future, both Mr. Ipsen and I have been invited to participate on national panels at the RSA Security Conference to be held this spring. In my case, this is solely due to Nevada's consideration and passage of the encryption legislation. Mr. Ipsen has a much broader portfolio than I do.

Despite those successes, there are several bills in Congress that would enact a federal breach law that would specifically pre-empt state laws in the process. Passage of some of these laws might affect the Nevada encryption requirement since there is some indication that the major corporations that opposed the Nevada statute may be more effective in their lobbying efforts in Washington DC.

The next topic I would like to mention briefly are presentations that have been made within the State. During the last month, the Attorney General delivered an address to about 200 State, county, and municipal IT staff during their annual GovTech meeting regarding State legislative initiatives and future concerns. Her presentation served as a jumping off point for a discussion among IT professionals from all over the State. I think Mr. Ipsen will discuss this in greater detail in his presentation under a different agenda item.

Mr. Ipsen and I also briefed the Nevada Homeland Security Commission. My presentation was a shortened version of what I have just said. I think Mr. Ipsen will be giving an updated version later on.

Lastly, as positive fall out from the GovTech meeting, senior management of EMC, a national security company and the parent of RSA, requested information from me on the Tech Crime Advisory Board's organization. They are interested in using our structure as a model they would seek to promulgate through their state contacts throughout the United States. They see us as a desirable model. They have also volunteered to brief the Board on e-discovery issues. That may be scheduled some time this spring.

IBM has also offered briefings on e-discovery and records management system, although those briefings may be more linked to their commercial product offerings.

That concludes the update I wanted to provide.

AG CORTEZ MASTO:

Thank you. Do we have any comments or questions? If not, let's move on to our next agenda item.

Agenda Item 5 – Presentation by Ira Victor, President, Reno Chapter, InfraGard, Hacking the Smart Electrical Grid and Associated Challenges

AG CORTEZ MASTO:

Welcome, Mr. Victor.

MR. VICTOR:

Thank you Madam Chair and members of the Board. I will start my presentation as Chris Ipsen helps me with the technical setup.

Briefly, for those of you who do not know me, I am president of the Sierra Nevada InfraGard Chapter. InfraGard is an FBI program to facilitate cyber security and protect critical infrastructure. It serves as a means to communicate between the public and private sectors regarding these threats. InfraGard is the largest security organization in Nevada, and one of the largest in the country. There are now more InfraGard members in the country than there are staff and agents in the FBI. This was a big milestone that InfraGard passed this last quarter.

I am also co-inventor of a number security technologies related to securing email systems from hackers. I have a lot of experience in my professional life with keeping the bad guys out. Finally, I am co-host of the Data Security Podcast, a net-cast radio program. Some of the materials you will see here today are courtesy of Mr. Tony Flick. I covered Mr. Flick's presentation at the DefCon Hackers Conference in Las Vegas this last summer. He talked about hacking the smart grid. Some of the materials today are from his presentation, used with his permission.

The first several slides are very simple. I am going to talk about what the Smart Grid is, some known security issues, and some recommendations.

What is The Smart Grid?

Three Major Elements

1. Transmission
2. Meters
3. Two-Way Communications/Network

DataClone Labs, Inc.
Ira Victor, CIAC G17799 GCFA GPCI GSEC
DataCloneLabs.com
775-337-8142

There are three major elements to the Smart Grid. It is important to understand them and how they are related. The first is the transmission portion. As electricity is transmitted from its point of generation to points of consumption, the Smart Grid is designed, at least in part, to give up to date information about where that power is and where it is supposed to go. So, the routing of wholesale power is one element of the Smart Grid.

A second element of the Smart Grid are the meters. Businesses and homes have electrical meters. Today these meters simply roll forward to record how much electricity is being consumed. The

concept behind the smart meters that are part of the Smart Grid is that meters will provide a feedback loop. Energy coming in will be recorded as will energy uses inside the business or home – down to specific appliance as the ultimate goal. So, in the morning, when you put your toast in the toaster, there will be a signal that says, two slices of bread are now being toasted. That information would then flow back up through the network, through the grid, to say, in effect, here is how electricity is now being used.

This is really the third element of the Smart Grid, the communication between the two. Now, most of the electrical grid is a one-way information pathway – how much power is being used. The idea is to turn this communication into a two-way communication.

One way to think of this in simple terms is this: Think of it as the Internet versus television. With television, you simply sit down and watch the show. No matter what you are doing, the network has no idea whether you are watching or not, or what you are doing on the other side of the screen. The idea of the Smart Grid is to have two way communication so that the grid knows exactly what you are doing and when you are doing it. It is supposed to facilitate that communication between the use all the way back up the grid.

That is important to keep in mind.


There are two other things to keep in mind about the Smart Grid. One is the security of the data, and trusting the data to be accurate. The next element is the privacy associated with that data.

Now, of course, it is difficult to have privacy without security. A lot of time, you want security with your privacy, so these are very tightly linked together. But, there are issues that relate more to privacy than to security when it comes to understanding the Smart Grid.

NY Times Pull Quotes

Customers in California are in open revolt, and officials in Connecticut and Texas are questioning whether the rush to install meters benefits the public.

NE many find it unfair that they will begin to pay immediately for the new meters through higher rates, when the promised savings could be years away.

 Ira Victor, GIAC G17799 GCFA GPCI GSEC
DataCloneLabs.com
775-337-8142

Understanding these elements is central to understanding some of the public reaction. This is from last week's *New York Times*: "Smart grid electrical utility meters intended to create savings instead prompt revolt." The Smart Grid has been rolled out in various stages across the country – early on in Texas and now in California. A lot of citizens in those states are very unhappy about the results. Here are two important pull quotes from the *New York Times* article. "Customers in California are in open revolt", and "Officials in Connecticut and Texas are questioning whether the rush to install meters benefits the public."

There are privacy concerns – not so much security concerns – in this article. Also there are concerns about cost. In essence, in simple terms, consumers and businesses – the users of electricity – are asked to pay more now in the hopes of paying less later. Some people are concerned about that. They are asking whether there really will be the return.


None of the people concerned about costs are really considering the privacy and security issues. They are looking only at what the bottom line cost is today.

I want to dive more into the privacy and security issues today. That is more of my purview.

Before moving on, we all know public policy is about getting the public move in alignment with the policy direction. It is very concerning that average citizens, who, at least according to the *New*

Issues

- Bi-directional communication attacks, same problems as every other type of network/application
- Web application attacks on data web sites, PLUS electrical info data breaches. Google PowerMeter, Microsoft Hohm. Big does not equal secure.
- Malware and worms on meters, physical attacks
- Attackers profile when people are home
- Fourth Amendment issues still unresolved. What is public? What is private? Opt-in or Opt-out?
- Ratepayers asked to pay more today to save tomorrow

 Ira Victor, GIAC G17799 GCFA GPCI GSEC
DataCloneLabs.com
775-337-8142

York Times, are in open revolt around the Smart Grid. Yet, they are in revolt only about one little slice, which is the cost issue. Most members of the general public are not aware of the security and privacy issues that are coming down the pike. If we add all of these together, it could really make the public policy decision very negative for those in policy positions.

Let's talk about some of these issues, in no particular order. Bi-directional communications – think of networking – presents the same problems in the Smart Grid as it does in every other networking device and system. There is

nothing inherently different about the Smart Grid when compared with what we see today.

Just a few moments ago, the FBI report from Las Vegas discussed banking attacks. That arrest is only the tip of the iceberg regarding what is going on with bank fraud today. According to FBI statistics, this year, we have had over \$100 million in unauthorized banking transactions, perpetrated primarily against U.S. businesses. The bad guys get into the loop, into the system,

and, in the case of the banking attacks as we heard earlier, transfer money from the people that have it to the thieves. This figure deals only with banking.

Any time we have networked systems, we have these issues to deal with. Of course, they are magnified when it comes to electricity.

If a bank you are dealing with makes an unauthorized transaction of \$5,000 from your account, you can say that you will leave the First National Bank of Main Street and go to the Second National Bank of Broad Street. You can take your banking business elsewhere.

You can't do that with electricity, which, by its very nature today, is a utility. There is no competitive pressure that customers can exert on their utility provider if there are security problems with the network. This leaves people very exposed when there are problems. What can you really do once the Smart Grid is rolled out? That is concerning.

Drilling down a little more, let's step away from the meters and the wires. The data about your electrical usage is being highlighted by proponents of the Smart Grid as being able to inform the consumer about when the consumer is using power. So, let's say you are using the toaster to toast only one slice of bread, and that you do that 3 times. Maybe you could use your toaster to toast two slices of bread at the same time, and one slice of bread separately. That would save you one cycle of usage on your toaster. The idea is that information about how you are using the electricity in your home or business is collected and then put on a web site. The web site would then give you tips – like how to make toast more efficiently. I am talking in very simple terms here. It would be more sophisticated for more powerful devices, but that is the concept here.

The information is put on web sites. In other states that have rolled out the Smart Grid, when this information has been posted on web sites, the web sites have not been secured. So, it is very easy for the bad guys to use attacks very similar to what is used on banking web sites to hack into the information that is being collected and stored as part of the Smart Grid web sites. Tony Flick and the researchers he works with found attack holes in the Smart Grid focused web sites that provide information, about your toast for example, that were more than 6 years old. Put another way, the methodology of the attack has been known for 6 years, and this site was put up without the proper security in place. This leaves consumers and businesses vulnerable to that information being exposed.

Think for a moment like a bad guy. You want to find out when someone left their home for the morning. You could say, okay, they make their toast from 7:00 AM to 7:15 AM. They percolate their coffee from 7:00 to 7:20. We see they make a second batch at 7:30. Then, at 8:00, the power usage goes way down. Well, I guess that person leaves for work at 8:00.

Their TV goes on at 5:15 in the evening. Oh, they get home at 5:15. So, I have safely from 8:15 AM to 5:15 PM to get into that person's home and probably be undisturbed the entire day to do whatever I want.

Exposing this information can expose the general public to harm. Of course, the worse thing that can happen in that scenario is that the person decides to go home for lunch that day and runs into a bad guy in the house. Then we could have a situation that would endanger someone physically rather than just a property theft from a house.

Another issue that comes up in dealing with Smart Grid security is the actual security of the meter itself. Tony Flick and his associates worked with scenarios where a meter could be infected by putting an attack on a single meter that would then self-propagate to all other meters in the local area or as wide an area as the attack could go.

One of the principles of information security is that if one has unlimited physical access to a device, then the odds of your cracking into it go up exponentially. The smart meter sitting in a

building or a home poses a situation similar to electronic voting machines. You can buy electronic voting machines on E-bay that are surplus. Bad guys or good guys can buy meters on the secondary market today. This provides unlimited access to the technology. They can get unlimited access to someone's smart meter. They change the code by putting malicious code into the meter, which then propagates automatically. Technically, this is called a worm. By propagating over the network, it gives the bad guys access to disrupt the power system, change what happens with usage. In a worst case scenario, a bad guy could take down parts of the grid through the smart meter by just turning off power.

This brings up a lot of concerns for Nevadans. As a Nevadan, I am aware that two areas of economic importance we have are gaming and mining. Both depend a lot on reliable power. This is perhaps disproportionate compared to other states that might have other industries. If we open our electrical grid to potential bad actors, who can then cause a cascading failure over Nevada, we could disproportionately affect the economics of the State because of the dependency of those two industries on highly reliable power.

These are what I classify as security issues. The next one is more a privacy issue. What is unresolved now from a legal perspective – and, full disclosure, I am not an attorney, and am venturing into an area speaking as a lay person. There are unresolved issues relating to the Fourth Amendment.

As I understand it as a lay person, the courts have made a clear distinction when it comes to privacy. Something that a person does in the general public is considered public, and there is not an expectation of privacy when something is generally viewable. But, what someone does in the sanctity of their home, behind closed doors, is considered legally to be more private. There are many more barriers to exposure of what that person does to law enforcement or to members of the general public.

Sheriff Haley, is there a question?

SHERIFF HALEY:

Are these some of the same issues that are raised with Kindle readers and computer use that is captured by Google and other sites? Or, perhaps, even the alarm systems in our homes that are monitored?

MR. VICTOR:

There are some similar questions. It is interesting that you mention Google. As you will see in one of my slides, Google has a service called "PowerMeter". Microsoft has one called "Hohm", spelled after the electrical term "ohm". There are issues about who owns that data. If you subscribe to the Google Power Meter, does Google own the data? Google would probably say yes. Or, do you own that data because it is about your home? This is unresolved.

There is a law enforcement question here. What access should law enforcement have to this information about how many slices of toast you put in your toaster in the morning, and when you run it? Or, probably more in-depth questions than that. I am using a very simple example as an illustration. Where is the line to be drawn? More importantly, should people in their homes have to opt out of having this information be made more public? That is, should the information be more public by default? Or should people have to opt in to making information more public so that information is kept private by default? That is unresolved. There are many, many legal issues that courts, legislatures, and public utilities commissions have yet to deal with.

Yet, if we go back to the open revolts that have occurred in other states, I think that people, when they become more aware of this, will be very upset to learn their most intimate activities in their homes are now more public than they believe them to be. When I took a shower this morning, I pulled down the window shade. I want to have privacy in things I do in my life. Is the length of my shower something that is the equivalent of me pulling down the window shade? That is an

unanswered legal question at this time. I think it is important for us to answer this before we get too far into the deployment of the Smart Grid. It will be difficult to address these questions effectively after we roll out the Smart Grid. This is key to my concerns and those of many other people when it comes to privacy.

Sheriff Haley, did you have another question?

SHERIFF HALEY:

Before you go on, isn't NV Energy presently pursuing grants that would allow them to roll out a Smart Grid?

MR. VICTOR:

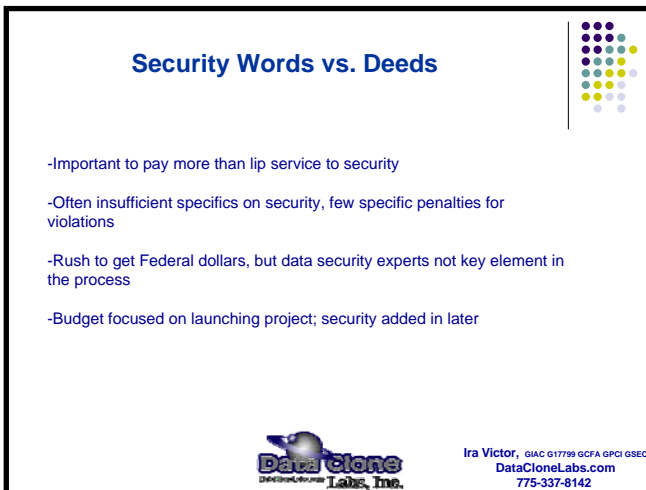
Yes, they are. They applied for a grant back in August. They were awarded grant funds by the federal government. It is a partial grant. Part of the costs will be covered by ARRA funds and part of the funds will come from rate payers to pay for the Smart Grid.

AG CORTEZ MASTO:

Mr. Victor, what is the position of the federal government with respect to the Smart Grid? Is there involvement or oversight?


MR. VICTOR:

There is oversight. But, these issues are not being specifically addressed. This is the nature of my concern. Great question. This actually goes to the next slide.



Security Words vs. Deeds

- Important to pay more than lip service to security
- Often insufficient specifics on security, few specific penalties for violations
- Rush to get Federal dollars, but data security experts not key element in the process
- Budget focused on launching project; security added in later

 **DataClone Labs, Inc.**
Ira Victor, GIAC G17799 GCFA GPCI GSEC
DataCloneLabs.com
775-337-8142

There is a pattern I have observed with a lot of these programs – one that I have even seen at the State level during the last legislative session.

There is an issue brought up about security. Words are put in to the effect, “We will take security very seriously.” But there are no specifics in the commitment. Instead, “The program will take security and privacy into consideration.” Without specifics, words like these end up not meaning very much.

Here is the result. This is from today's *Wall Street Journal* – front page, above the fold, from today's *Wall Street Journal*. I do not want to get into the entire story, but it is directly relevant. The story headline is “Insurgents Hack U.S. Drones.” “Twenty-six dollar software used to breach key weapons in Iraq. Iranian backing suspected.” The drones the U.S. military uses around the world as part of our defense systems uses video. Actually, this is a Nevada story because the drones are controlled out of Nellis Air Force base. The drones use a video link to see where the bad guys are and what is going on in order to launch an attack. Well, as it turns out, the video link is not secure. Our enemies, the enemies of the United States have used \$26 software to intercept our video feeds.

The report asks the question, “Why didn't we encrypt the feed?” The people who worked in this program replied, “We didn't think anyone would notice.”

Then the question is, can't we just fix this by putting in a CD with an encryption instruction? Well, no, we can't do that because the video system is interconnected with all these other systems. So, we have to change all these other systems before we can change that system.

MR. IPSEN:

I just want to pose a rhetorical question. Wouldn't this be in violation of SB 227? (Laughter) They are a data collector, and this is data in transit.

MR. VICTOR:

I guess it would have to read the Social Security Number or the driver's license of the guy in the Al Qaeda truck – to continue your tongue-in-cheek point. They say the satellite imaging is very good, so it might be that good.

But here is the point – very much related to my topic. The drone experience is a result of not putting security, and specific requirements of security planning, at the beginning of a project.

Recommendations

- High Level Security Policy (security term of art) at the start of the process
- Data security experts as important as the Federal dollars
- Standards, controls, encryption. Including network and web application security. Example: Open Smart Grid Group, and the AMI-SEC (Advanced Metering Infrastructure Security) Task Force
- Truly Address Fourth Amendment issues to build public trust

DataClone Labs, Inc.
Ira Victor, QAC 617799 GCPA GPCI GSEC
DataCloneLabs.com
775-337-8142

There is a term of art in security, “high level security policy”. This is a plain language mission statement that spells out what the security goals and mission will be for the project. When you deploy a specific technology, you then write procedures that match and implement the overall goal. But, you do this at the beginning of the process so you do not have to go in and rip out expensive systems to rebuild and re-engineer them, all of which causes delays and more costs.

That is the key thing about today. We are at a critical point with the Smart Grid

in Nevada. We can make a decision to go this way – where we might have to go back, rip things out, and spend more rate payer dollars, or, we can make a decision to include security from the very beginning. We can make security requirements very specific – what we want to achieve specifically.

The good news is that we have high level security policy. That is a standard. We have a group called the Open Smart Grid Group. It has promulgated standards for securing this information. We are on the way with that.

The last thing is harder, but I think needs to be addressed. I am talking about the privacy issues – the Fourth Amendment privacy issues. This needs to be addressed early on. It is a bigger nut to crack. I am aware of that. It is going to affect us anyway. We could be faced with having to undo a lot of systems if the courts make a decision that impact equipment that is already installed and systems that are already in place.

This concludes my presentation today. I am here to answer questions, and am available by email if someone on the Board wants to follow up after today's event.

MR. ABNEY:

Thanks, Ira. What kind of communications have you had with NV Energy about all of this to date?

MR. VICTOR:

I have not reached out directly to NV Energy. I have spoken with Congressman Heller's office because he is on the Ways and Means Committee. They have heard my concerns, but I have not

received a response from them. I have seen NV Energy in the media. There media responses to date have been the standard, "Well, we take security very seriously", but no specifics.

SHERIFF HALEY:

I have a comment. Right now, RTC, NV Energy and DOT are working in concert to build a vast center in the north, following the example in Las Vegas. I sit on a committee that is intertwined with all of this. I find your comments very intriguing. I agree that right now is the time to talk about these issues and incorporate them in our decision making. This is coming. If we wait longer, as you said, we would likely have a lot more costs associated with doing the right thing.

AG CORTEZ MASTO:

Are there any more questions? Yes, Assemblyman Mortenson.

ASSEMBLYMAN MORTENSON:

Thank you. This blows my mind – smart meters. It seems to be the worst idea I have run into in years and years and years.

You are going to raise my electricity rates. We are establishing a can of worms where hackers can shut down power. We are setting up huge, expensive security procedures to try and keep them from doing this. Of course, we know that hackers always manage to get through the security measures.

All this being done in order to tell me that I am toasting two pieces of toast at one time instead of one. I am not going to go to a web site to look at this stuff. I am not going to waste my time learning that I can do two pieces of toast at the same time and will thereby save electricity. Even if I toasted two, I'd turn on the oven to keep one of them warm while I was eating the first one. (Laughter) I would use up more power.

This is just a terrible idea as far as I can see initially.

That's just an opinion.

SHERIFF HALEY:

Madam Chair, I have a follow up comment.

Ira, I think the issue here is how much electricity we have. Where does it need to go at a specific time? And, can you make decisions in your home about using energy at a different time than you would normally use it in order to save money? As a consequence, we would not have to build more transmission lines and more energy producing centers. That is really the focus from a business perspective and the consequences of this.

MR. VICTOR:

That is right. The proponents of the Smart Grid say – and again, I use the toast example to keep it simple – the Grid would monitor when you are using washers, dryers, and hair dryers – appliances that burn up more power than a toaster. Although, actually, a toaster burns up a lot of electricity, you would be surprised.

You would then be able to learn that by shifting your usage – by washing dishes at some time other than between 3 and 5 o'clock, when everyone comes home and turns on their air conditioning in the summer time. That puts a strain on the grid. If you shifted your dish washing time to 8 o'clock, then that would be preferable.

But, this is not that far off from the toaster example. That is the implication.

The ideal, ultimately, is to put financial penalties into place. So, if you run your dishwasher at 4 or 5 o'clock when usage peaks, you get a financial penalty as compared to running it at 8 PM.

MR. IPSEN:

I have a question and a statement also.

I can not quite imagine myself sitting in a Devil's Advocate role against security, but, out of fairness, I want to talk about some of the components of the existing grid versus the Smart Grid. One of the interesting facts about the existing grid is that it is always on.

When we look at networks and routing issues we can see where power is going. But, in order for us to sustain our power now, it always has to be available. When you turn the tap on, it always has to be there. We can not route power. It goes where it needs to go based on the demand at the other end. So, often times, we have to produce power that is greater than the actual consumption. In fact, we have to do this at all times – producing more power than is actually required on the consumption side.

In terms of the benefits of the Smart Grid, I see this as anticipatory capacity. We can begin to manage electricity smartly so that we do not have to produce as much, thereby possibly reducing green house gases and other components. We can use our energy more effectively. I think that is a valid business objective – something we need to have.

But, in terms of the security concerns, I could not have had a better set-up than what Ira has provided to address the importance of planning on the front end. What is it that we can do? What is it that we should do? What is it that we are actually doing with the information that is collected? This is very important. I think business leaders need to hear information on all of these factors so they can make intelligent decisions about how we use a capability going forward. This is kind of an emerging technology.

RAC WHITE:

Ira, I have a couple of questions. Is this an imposed system, or is it a system that is voluntarily accessed? How is that going to work?

MR. VICTOR:

I think you have to ask the decision makers. I can tell you what has been in the press. Most of the discussion has been in terms of voluntary. I gave a public presentation on this topic recently and someone yelled out from the audience: "Oh, voluntary like my water meter!"

Everyone in northern Nevada knows that it is "voluntary" to get a water meter, but the utility has made it quite uncomfortable to stay with the old meter. So, there is a lot of concern among the general public that, in practice if not in law, they will be forced into getting one of these smart meters.

RAC WHITE:

I can see that. The second question I have is this. In evaluating the data, based on what you know about areas where this has been implemented, is that done in an automatic sense, or with the home owners own knowledge or whatever they obtain through their power company to know what they should be looking for when they receive their results. Is there a graph? Do you know in what form the power usage information is provided, or how you can improve usage or cut back? Do you know what form that is provided to the home owner?

MR. VICTOR:

What has been proposed so far, and rolled out on a limited basis, are a lot of analytics. You pull up a web site and it tells you, to use the toaster example, "You are using your toaster to toast three slices of bread three times. Here is how much power you would save if you only used your toaster twice."

There are graphs and charts that show times of usage. The concept is to give you financial incentives to shift your usage and to show how much money it would save were you to shift usage to the recommended ways to consume power.

AG CORTEZ MASTO:

Are there any other questions by Board Members?

SHERIFF GILLESPIE:

Madam Chair, I have a couple of things. Processes in technologies like this are going to continue to surface, because they tend to be more effective and efficient from the business standpoint of their promoters. From a security standpoint, local, State, and federal, we see the consequences of this type of technology only after the fact.

For the purposes of this committee, this is the type of situation where we could use this information to educate, and/or, statutorily require, businesses when they are embarking in rolling out technologies like this to incorporate security aspects. In my opinion, we can not rely on Department of Homeland Security dollars after the fact to come in and fix these cyber-type issues.

Even though Secretary Napolitano has put cyber crime as one of her priorities, if my memory serves me right, the monies coming to us to deal with security issues are not increasing. We in law enforcement have been saying for a while, with regard to cyber issues, that we need to pay attention on the front end. Everyone has heard the phrase "going dark".

Here is part of the problem that continues to confront law enforcement. Part of the reason we are "going dark" from an investigative standpoint is that new technologies are introduced and used by companies without a requirement to provide the same level of access and security that they were before.

When we talk about smart devices and other issues from a committee standpoint, this could be one of the times where we educate the legislature, we educate the Homeland Security Commission, regarding what we see coming. We should do our best to influence them to enact requirements. Why would a business institute the type of security needed if they are not required to. It will cost them more money. It will be an afterthought. Where will the pressure come from for them to implement technology that will combat what we know will happen as a by product of technological change.

We see this in many things we do today. People via the Internet and other networks have access to information that the criminal element uses to its advantage.

An example I would provide is the challenges we are likely to face with the N-DEx process and other exchanges is the security of our law enforcement information when and after it is exchanged. We know it is protected within LVMPD, but when it is released to someone else, we have to ask whether the same level of security is there as it is being transferred. We are responsible for that information.

From our standpoint, we are making sure there are checks and balances if information is to be exchanged before we are willing to give it up. We know we will be held accountable for it.

I don't think that model is there in the business world. I am not saying that to chastise, or give businesses a hard time. I just don't think the requirement is there for them.

From our standpoint, maybe Ira, in conjunction with other folks, would be willing to craft legislation to be brought back to us. They are the technology people. What do we need to do is to place pressure on the technology world to look at issues from a variety of perspectives before things like the Smart Grid are rolled out.

AG CORTEZ MASTO:

Just to follow up on the Sheriff's comments, that was one of my questions, Ira. What is it that we as a Board can do to stay ahead of the curve? Do you have any thoughts on how we can address this issue to, at least, put Nevada in a position where we are looking at the privacy and security things you just talked about – including the integrity of the data and the cost of the data. How do we implement that and get information to the people who need to know?

MR. VICTOR:

That is an excellent question. I think a number of players need to be brought into this. Obviously, there is a major role for the Public Utilities Commission (PUC). PUCs are involved in many states. We have an opportunity here, because of the timing, to get the PUC involved at an early stage.

I think we should involve federal authorities because we are on a multi-state grid. I think there is a role to be played by members of this Board and members of the State legislature because they represent the people and the interests of the people.

I know that is not a specific answer to your question, but it does address the process to move forward.

AG CORTEZ MASTO:

I appreciate that. I do want to put you on the spot a bit because you are obviously the expert here, and I appreciate the topics you bring to our attention with your knowledge and experience.

Would you be willing to sit with me initially to put together a strategic plan on how we address this issue in the State that we would then back to the Board so that the Board is aware of it. I am willing to move forward with the various issues we are talking about. It could run the gamut from education, to reaching out to the necessary regulators, to addressing various security policies. You mentioned earlier that there is an established Smart Grid Group. Is this part of the InfraGard organization or is it a separate group completely?

MR. VICTOR:

Madam Chair, it is a separate organization. It is developing standards for securing this information.

AG CORTEZ MASTO:

Is that just here in Nevada, or is it a national group?

MR. VICTOR:

It is a national organization.

AG CORTEZ MASTO:

Would you recommend that we tap into that group as well?

MR. VICTOR:

Yes, I think it would be a good resource for us to use.

AG CORTEZ MASTO:

OK. So, maybe there is an opportunity for us to brainstorm to come up with a strategic plan that we then come back to the Board itself for members involvement and input as well.

MR. VICTOR:

To come back to your question, I would be honored to work with you on this issue to help Nevada get out in front of these issues.

AG CORTEZ MASTO:

Thank you. Are there any other comments or questions?

MR. ABNEY:

I think we should hear from NV Energy to learn what they have done so far before we get too far down the road of regulations, new laws, and plans. I want to hear from them and what they have done and what they are planning to do. We should make sure they are part of this process. We should work with them as well. That is my only comment. Thank you.

AG CORTEZ MASTO:

Great. I appreciate that. It is a great point. We will include them. Maybe at the next meeting we can have them give a presentation with respect to what they are doing with respect to smart meters.

MR. ABNEY:

Madam Chair, I am willing to reach out to them. Mary Simmons, with NV Energy, is actually the Chair of my board next year. I can reach out and start talking to her about it as well.

AG CORTEZ MASTO:

That's great. Thank you. Are there any other comments? Hearing none, Mr. Victor, thank you very much. It is always very enlightening when you come visit with us.

MR. VICTOR:

Thank you very much, Madam Chair and members of the Board.

Agenda Item 6 – Introduction to Emerging Technologies and Outsourcing Challenges (Safeguarding of Data) and Future Coordination Among State and County/Municipal Information Technology Organizations

AG CORTEZ MASTO:

Moving on to Agenda item number 6, we have a presentation by one of our own Board members, Mr. Chris Ipsen, the State Chief Information Security Officer. He is going to be talking a little bit about emerging technologies and out sourcing challenges and future coordination among State, county and municipal information technology organizations.

MR. IPSEN:

Thank you very much. Let me get into my slides. Now that I have assisted Ira, I want to make sure I can do the same for myself.

I could not have had a better set up. I want to say before I start that Ira and I did not talk before we did our presentations. These were prepared independently. I want to both deal with some of the questions that were asked of Ira and also provide a foundation to make effective decisions about security.

As we move into the world of emerging technologies – and the Smart Grid is an emerging technology – often the technology moves faster than the governance. That is the problem that we are seeing. Our capability exceeds our ability to secure it.

The comments made by Sheriff Gillespie with respect to getting out in front of this are warmly received by me. In terms of the State infrastructure, I have a number of recommendations that, hopefully, the Board can participate with me in propagating throughout the rest of the State so that we effectively secure State information.

One of the key concepts to think about from Ira's presentation is the law of unintended consequences. We have a capability, but what happens with the information once we implement it?

Competing security interests versus business interests – You will see this in one of my first slides. I think this is a fundamental question. I want to set the groundwork to say that I am not in competition with business, but we have to understand our different roles as we embrace business capabilities. We also have to understand what our objectives are.

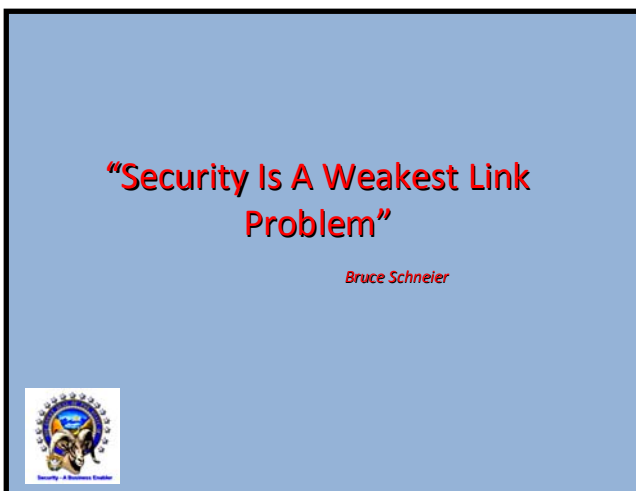
Government has different incentives than the private sector. I think this needs to be captured. I would like to give you an overview of my presentation, giving you a heads up of when to really focus in.

At the beginning, I am not going to talk about the really cool things that Ira got to talk about – all of the threats and the hacks and so forth. Well, I may talk about a few of them.

I want to focus in on how we as leaders make effective decisions. What are the components of the security paradigm that we need to consider? We also need to understand what is the posture of our vulnerabilities. What is it that makes it important we make effective decisions? I want to provide some understanding about emerging technologies. Lastly, I want to provide some recommendations. At the end, I hope we will be able to focus on the recommendations. At the beginning, if you take away nothing else, the first three slides are really helpful in answering the question, "How do we effectively secure the information of the State of Nevada?"

States are the conduit for more sensitive information than any other aspect of society, and that includes the federal government. We provide the conduit from cities and counties. They come through the State, generally going to the federal government. States are the last sovereign stop for that data. What do I mean by that?

The federal government has a purpose for the data as do we. Once we start aggregating the data, we are the last stop for our ability to control outcomes and unintended consequences that Sheriff Gillespie talked about. So, it is appropriate for us to secure data at the state level. That is my presupposition. With that, I would like to review a few fundamentals of information security.



Specifically, this is one of the important things to take away. Security is a "weakest link" problem. You can have all of the security controls in the world in place in your environment. You can be absolutely sure that what you are looking at is secure. But, one configuration change can open you up completely, providing access to all your data without restrictions. If you have one vulnerability that is exploitable, hackers will use that one vulnerability to get to the entire system. If that vulnerability comes from within a user who has privileged access, that vulnerability is expanded logarithmically. For example, if I am an administrator, and you get to my

workstation, then all of my access is transferred to the hacker. One vulnerability on an insider threat, and all bets are off. This is exactly what we see, and, if you are interested, we can demonstrate this for you.

We can show you how a web site browser, through an Internet Explorer vulnerability or a Mozilla vulnerability, while you are on a web site, information can be put on your machine that allows a hacker to access your machine, elevate privileges, and access all information that you have access to. This can be done by exploiting one vulnerability.

The second important point when looking at emerging technologies is to ask, "What are our business requirements?" I know very well, having been in the private sector, and I am not faulting



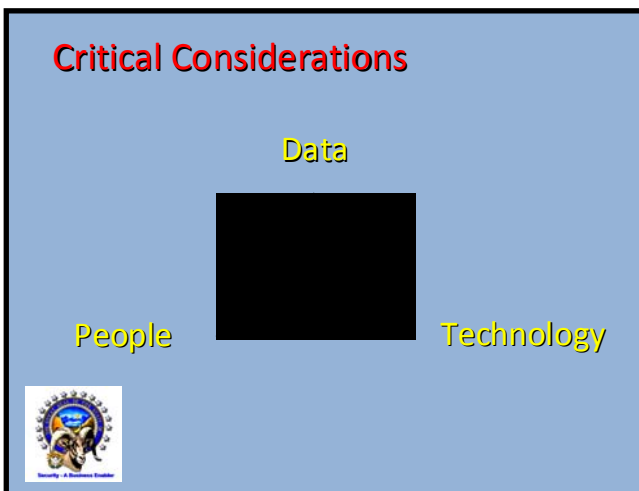
this but rather embrace it, private sector business exists to make a profit. They are going to do what they need to do as efficiently as they possibly can. From a cost perspective, they will do this at the least cost possible.

Government exists to provide a service. That is not to say that businesses do not provide services. But, if you provide a really good service, but are not a profitable company, what will happen? You will go out of business.

If you are a government, and you don't provide service very well, and you focus solely on what the cost ramifications are,

then you falter in that area. What do I mean by this?

We just heard that states require constituents to give us information. Here is an example. My child was born two years ago. Information about my child is required to be collected by the hospital. Hospitals, in turn, have to share that information with the State. This is not an option. This is a requirement.



As a result, our responsibility to protect that data is different from that of a business. If I am a business, I ask, "What is the cost to me to secure this data? More specifically, what is the cost to me from an actuarial standpoint? How much will it cost if my records are compromised? Two hundred dollars?" If I have a hundred records, a compromise would cost \$20,000. "OK, I need to put in controls that equal \$20,000 or less." If I spend \$30,000 to protect that data, then I have made a bad business decision.

Conversely, if I am a government and I collect HIV data (and I notice Ernie Hernandez is here from the Health

Division, hopefully he can back me up on this), what is the cost of compromising that HIV data? Well, the government is not in the business of making money. Rather, we need to look at the long-term consequences to the affected individual. Once it is gone, it is gone. Their ability to get long term insurance, once that information is published on the Internet, will be severely compromised.

We cannot afford to compromise any records relating to health information. We need to consider due diligence not from an actuarial standpoint but from a best practices standpoint – that may

involve a competing business interest from the private sector. How does this relate to us going forward?

We can do some really interesting things with emerging technologies. We can aggregate data and do all of these things that provide transparency. But we have to be mindful of the consequences – especially that law of unintended consequences.

The third thing I want to present – if you remember nothing else – what are the critical considerations that security professionals need to consider when securing the system. What does that mean? We need to talk about people.

If I have privileged administrators – we used the example a year ago – the city of San Francisco's network administrator was able to shut down the entire network because he was the only person who had access to everything. In the Nevada State system, we have checks and balances. We have multiple people performing in different roles. This is called separation of duties.

From an actuarial standpoint, this may not be cost effective. But, from a data security standpoint, it is highly effective and necessary. One of the biggest challenges I have as the State Information Security Officer is balancing those interests – a WAN (wide area network) group will want to do one thing, and the server group will want to do another thing. The question is, "What is the best practice with respect to the data?"

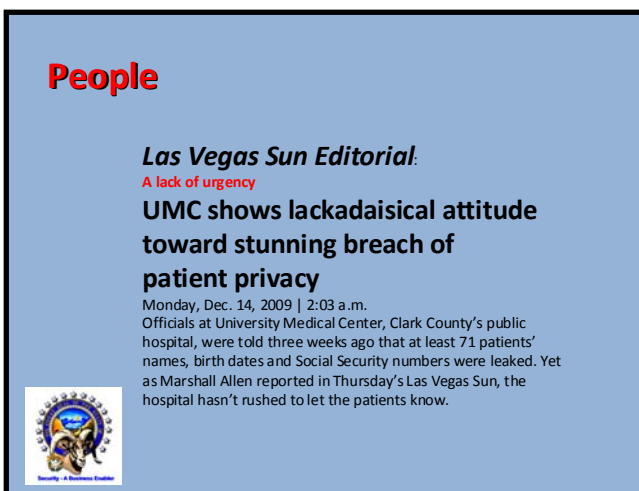
These questions may not be being asked in some of the emerging technologies.

We also need to ask, "How secure is this new technology?" How secure is Facebook as we move forward? Are we even going to think of the security ramifications of Facebook as we move forward, or are we just going to use it?

Sheriff Gillespie had a very poignant point – we need to think about these things before we embrace them going forward.

Lastly, and most importantly, we need to talk about the data. If we do not always think about the data, we have a flawed paradigm. We can talk about the transport, we can talk about the people, we can talk about the technologies, but, if the data gets compromised, we lose. We need a data-centric model. Data loss means we have lost our ability to perform.


The threat. I thought I would use the U.S. drone compromise example this morning, and Ira beat me to it.



People

Las Vegas Sun Editorial:
A lack of urgency
UMC shows lackadaisical attitude toward stunning breach of patient privacy

Monday, Dec. 14, 2009 | 2:03 a.m.
Officials at University Medical Center, Clark County's public hospital, were told three weeks ago that at least 71 patients' names, birth dates and Social Security numbers were leaked. Yet as Marshall Allen reported in Thursday's Las Vegas Sun, the hospital hasn't rushed to let the patients know.



The military drone breach involved twenty-six-dollar-software. That is all it took to compromise those drones. I do not want to belabor the point. We all know there are many threats out there.

The people. This is an editorial from the Las Vegas Sun involving UMC from December 14th. A number of patient records, of people who had been involved in accidents, were sold to attorneys engaged in civil law suits on behalf of accident victims. I don't want to use the term "ambulance chasers", but that is who they were selling the information to. Why did they do that? Well, there is a business incentive. I

know he was in a wreck. Using my contacts, I can get out in front of the rest of the attorneys, and I have a better business model than they do.

People on the inside of UMC are believed to have sold that information for a profit to other individuals. The key is this. Lack of urgency is cited. "UMC shows lackadaisical attitude toward stunning breach of patient privacy."

These are the people who were entrusted with protecting the data. They said, "We're not sure this is really a problem." Maybe there are a few records missing, but we aren't really sure.

It is really easy to bury your head in the sand when dealing with security issues.

When I talk about security, people ask, "How do we know we have a problem? I know my area is secure. I haven't had a breach in 15 years."

I can tell you that, now, in my own office, the Office of Information Security, I can not say that. I would have had to have been monitoring that environment 24x7x365 to validate that some of the more sophisticated threats did not exist in my office.

I would also have to represent that all of the people who worked for me are absolutely trustworthy. I am sorry, I am kind of a distrusting guy. I value the people I have working for me. I think they are great. I think we have the best procedures in the State. I think we have excellent security controls, and people who are dedicated in this area. But, I can not say that we are absolutely secure.



Turning to technology, I want to give really relevant examples if I could. This is not a dig at Microsoft. This says, "The SQL server administrators are not being warned today about an unpatched vulnerability." In effect, Microsoft is saying, "We don't have a patch for this yet." Microsoft developed a product that had weak security controls. The last line of the article is, "Microsoft said it has no plans to release a patch for the vulnerability."

OK, so I own Microsoft SQL server, what do I do now? Here is a respected company in terms of its capabilities and it is not patching a flaw.

What happens when we start to move into the fringe capabilities and we lose control of our ownership of the data? What are they going to do? I can tell you. Recently, and anecdotally, I saw this with Facebook. They did a security upgrade. But, in order to perform the security upgrade, they had to delete all the security settings that you already had on your personal account. I do not have a Facebook account, so I can not say this happened to me. Take this with a grain of salt, but I have heard this from enough people to cause me concern. Facebook exposed everyone's data until they re-enabled those security settings.

Oh, and by the way, one of those settings involves clicking "I do not want you to share my information with data aggregators" – like Google and others. So, if you don't find this box, and check it to say "Don't share my data", then the data gets shared by default. That is how they make money. I understand that. I accept that. But, if we are going to embrace this as a State, given our heightened security concerns, we have to be mindful of what these technologies will do.

Data – Personal Information

NRS 603A.040 "Personal information" defined. "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

1. Social security number.
2. Driver's license number or identification card number.
3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.



Next, let's turn to personal information. I think it is great the State has a data breach notification law. These are the things that are defined as personal information by NRS 603A. These are things that set the trigger for defining a data breach condition. Data has to fall into these categories.

What I am going to say to you is that this is a good start. But with data mash-ups – and we will talk about those in a second – this definition is not enough. We need to look at data in its aggregate form and what the outcomes are. We need to use an outcome based approach to determine whether the data is actually pointing to personal information.

Emerging Technologies

- Virtualization
- Cloud Computing
- Web 2.0
 - Social Networking
 - Data Mashups



What are the emerging technologies? Virtualization is not new. It has been around since the 1970s. Virtualization involves taking many logical servers and placing them on a single physical server. This allows us to do more with less. I can put 15 different servers on a single physical box. This is a great model. I can beef-up two big boxes, and, in real time, I can move servers back and forth so that they are always available to us.

But, when I start to do this, even in my own environment, when I start to bridge security zones, I have to get the wide area networking group to approve it. If the virtualization networking technology

does not do that – if it aggregates all of that authority into one person, and that one person is the server administrator, then, that causes us security problems. I am not saying we should not embrace virtualization. In fact, we should embrace this technology, but we have to embrace it with correct rules.

As a State, we are embracing virtualization. But, it is very difficult. Anyone who comes to me and says, "We have the problem solved, and it is really easy. We can do it for you with no problems." Well, actually have a lot of challenges for them.

The second emerging technology is cloud computing. Essentially this involves a service provider representing that it can provide us with whatever we need. For example, if you need Microsoft Office, we can provide you that service as a web interface. You enter all your data, you store your documents with us, and you do not have to have that technology, that software, on your laptop.

Essentially, the vendor represents that you can capture the economies of scale of everyone using this common technology. We are going to provide it to you, and it is going to be cheaper, faster, and better than you can do for yourself.

The problem is, going back to that model, what about the data? “Well, we have it secured,” is the vendor’s answer. “Don’t worry about it.” What do you mean? “Well, we can take care of that with a service level agreement.” Where does the data reside? “Well, in order for us to maximize our economies of scale, it could be anywhere.” It could be India. It could be China. It could be anywhere. It could be Indonesia, Iran, Iraq, or Mexico – wherever we can find the best deal. Because wherever the Internet exists, we can use local resources and people to provide you a service and to save us (the vendor) money.

But, says the vendor, you can say where you want the data. “OK, I want the data to stay in Nevada.” Sorry, we can’t do it in Nevada. Why would you want it there? Nevada is unstable and has a lot of earthquakes.

Well, we want State data to remain in Nevada because we have sovereign interests in the data. Remember that the State is the aggregator of all information that moves up to federal agencies. Nevada has specific concerns about privacy that might not exist in other states.

Essentially cloud computing is a concept whereby the customer is provided whatever is needed through a thin client, and the customer does not have to provide any infrastructure.

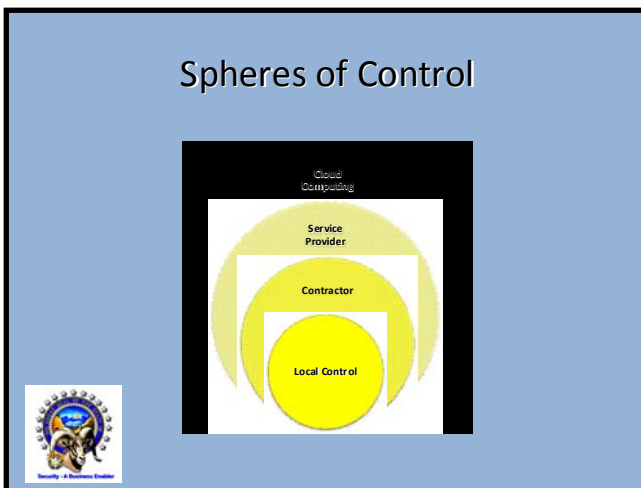
The other part of the new technologies are Web 2.0 or social networking. We know what Facebook is. We have a number of presentations on new web presence. The technology provides ubiquitous access to many people.

The core foundation of many of these sites is that we are not going to have many rules. When we have rules, they restrict your ability to be creative. If we know about this, then, going forward, we can ask security questions to determine whether use of the site makes sense for us.

Data match-ups are an active effort both by social networking sites and the States. The question here is what data do you have that is publicly available on the Internet today. What we are going to do is take that data and combine it with every other agency’s data in your state so that we can aggregate the data to arrive at a common understanding of you as an individual, you as a process, you as a service provider to your citizens. This provides a more transparent view of what the state of Nevada does for its citizens.

There is an active effort called Data.gov. It involves an active effort to encourage data match-ups.

Here is one of the privacy concerns. Let me give you an example. I live in Alaska and I am an Alaska Eskimo Indian and I have HIV. Can you tell who I am from that data? No. But, if I am an Alaska Eskimo Indian and I live in Gabs, Nevada and I have HIV. Can you tell who I am? Probably.



These nuances in working with data present interesting challenges for us moving forward in terms of social networking.

These are the spheres of control. I think this is an important point. Local control is what we have right now. I can touch it, I can feel it, I can own that data. The next level of control is that we can hire contractors to help us do our job better. We do in the State. The third level is that we can have a service provider. Here, you do not hire a contractor, you hire someone who will provide an entire

service to you and manage that service and control how the service is provided based upon your needs. The last level is cloud computing – where everything is provided to you on a “plug and play”, “easy button” solution.

When we look at this hierarchy, there are significant considerations. The first question always should be “Where is the data?” Where does the data reside? Who is accessing that data? What technologies are used?

The entity providing the service will do so with a different solution based on whether it is a business entity or a government entity that has to provide the service.

Can we bridge these gaps? Can we intelligently embrace contractors? Can we intelligently embrace both service providers and cloud computing? I think we can, but we have to ask the right questions.

Key Considerations Going Forward

Data

- Appropriate Data Controls
 - Clear Data Classification Definitions
 - Authority to Require Appropriate Security Controls
 - Where the Data Can Reside
 - Who Can Have Access to Sensitive Data
 - Who Is Responsible
 - Audit Tools
 - Standardized Data Security Contract Language



Key considerations with respect to the data – I think it important if we are going to have effective vendor relationships and effective practices, we need to have appropriate controls around the data. These are the recommendations. We can have clear data classification definitions. We don’t want some one to say, “Well, its kind of sensitive.” Remember the PI definitions. We need to have specific definitions. That’s my responsibility in part, with the State Records Manager. We need to ask what data we are going to classify in order to get it protected. This sounds pretty straightforward, but there are nuances that lead to questions. If a machine is

asked that question, the answer depends on how it was programmed. It can either say “Yes” or “No”. If it says “Yes” and the bin opens, then we have breach.

Additionally, authority to require appropriate security controls is needed. We talked about the consolidated policy, and I am pleased to be able to tell you that the State of Nevada has one of the most robust, early-deployed, statewide information security policies in the United States. It maps to NIST standards and it maps to national applicable ISO standards. These are national standards. We have that.

Here is my problem. Once I tell people that we have a statewide security policy that your agency had input into – all agency ISO’s sat together and hashed it out and agreed – we do not have the authority to require State agencies to conform to the policy. We can say we have a standard, but what enforcement authority do we have?

Do I go to the Governor every single time I have an open wireless access point? The Governor doesn’t want to have to hear about this. Neither do any of the other elected officials. And, I do not want to grab power that should not reside in my office. But, I will tell you that problems exist in State agencies. I know of three of them today. We need to address them, but agencies are telling me that they do not have a problem.

We need authority to require appropriate security controls – where the data resides. If we as a State decide that our data will reside within the State of Nevada, then we need to be able to require that.

If it resides somewhere else, we are giving another authority physical access to our sensitive data. This is a significant problem. If I can't say data is absolutely secure in my environment, given my business mandate, how can I say the State's data is secure somewhere else?

Who can have access to the State's sensitive data? I will tell you right now that every one of your system administrators probably has access to all of your sensitive data – whether you be a police chief or a private. There are generally roles associated with the issue of who can access what data. But, the person who puts the system together defines the controls as they are being deployed. So, every IT system administrator has access to all of the agency's data. This is an important consideration. Should they? And, who is responsible for maintaining that data?

We need to get control of all of this. I have a number of very serious concerns in all of these areas. I am reaching out to the Board to ask for some help. How do we enforce our requirements? We need audit tools. How do we audit to ensure that what is supposed to be done with the data is actually being done? And, this is a big issue, can we come up with standardized data security contract language?

Here is what happens in State contracting. We go out to business entities with a problem to solve. We release an RFP requesting information from vendors. Vendors come back to us and tell us that they can do everything we have requested. We will answer the RFP. We will give you technology that meets your needs.

If we do not include standardized security language in this process, there will be no requirement assumed by the vendor to do what is really necessary.

There is a cost for security on the front side – 6 to 8 to 10 percent on the front side of a project is a typical number for baking security into a solution.

The cost of bolting security on at the end is in excess of 80 to 100 percent of the contract. So, if a project costs you a million dollars to deploy, and you do not put effective, standardized security language in the contract up front, then, after the fact, to make them reconfigure their systems, based on national statistics I have received from the security expert who created SANS, could double the cost of the project. It is very expensive on the back side. On the front side, security is a cost, but nothing like the back side cost. Given the State's business requirements, it is very important to contract for security on the front side.

If we can have standardized security contract language, we can begin to fight this cost battle effectively.

Key Considerations Going Forward

People

Appropriate Validation of Personnel and Behavior

- Background Checks
- Checks and Balances – Separation of Duties
- Change Control Validation
- Clearly Defined Security Protocols



Turning to people, we need to have appropriate validation of personnel and their behavior. We need background checks. I can tell you this right now. Our State security policy requires background checks conducted by the Office of Information Security. Those of you in law enforcement will know that when you do a background check there are nuances to the results. Someone who has a DUI yesterday is different from someone who had a DUI 20 years ago. The same behavior is involved, but the fact that 20 years has transpired can really affect the decision about who you hire to manage your systems.

We have a requirement that we do background checks on people who work on State data. If a State entity contracts with another vendor, and they do not adhere to the State security policy, there may be no language about background checks at all. Some large vendors may say they are not going to subject our employees to background checks – “We vet our employees, and you either take them or you don’t take them.” Well, that’s a problem given the fact that they are going to have privileged access to all of your sensitive information.

Turning to checks and balances, this refers to separation of duties. We need to have that in place and we need to maintain that in place. This is important because we are going through severe budget crises right now. We could ask, “Well, can we do this with fewer people?” Yes, but we have to get rid of those checks and balances because we have no redundancy of people. And, the availability of people goes out the window. We have one line of defense, and if that person gets hit by a bus, forget about data security. Or, if that single person is malicious, then we have the San Francisco incident that we talked about – where one person controls everything and we are submitting our data to the controls exercised by one person. That is a bad security model.

Let’s talk about change control validation. If we want to change something, what happens? Who has the authority? Consider a firewall. Right now, I can change one line of code at the very end and permit any amount of traffic to come through. This is a simple instruction: “Permit IP, Any, Any”. If I put that at the end of a firewall log, all bets are off, because everyone can have access to your data through the firewall. Or, at least, they can access your systems. How do we know that one person did not do that? What if the person made a mistake by typing the wrong entry? People do make mistakes.

So, we need validation. We need change controls to ensure that something like this did not happen before the change is deployed.

We also need clearly defined security protocols – What are you supposed to do, what are you not supposed to do? This goes back to enforceability.

Key Considerations Going Forward

Technology

Appropriate Validation of Technology

- Standardized Contract Language Requiring Adherence to Security Requirements
- Requirements to Remediate Known Vulnerabilities
- Authority to Perform Vulnerability Assessments and Penetration Testing
- Capabilities to Rapidly Address Security Vulnerabilities
 - Tools
 - Flexible Sharing/Funding Approach



Let’s talk about the third area, technology. What do we need to do? Remember the question came up, “How do we get our hands on this? How do we get out in front of these things?” Here are some of the recommendations that I am seeing that we need to have in place to allow us to get out in front of these emerging technologies.

The first is appropriate validation of technology. We need standardized contract language requiring adherence to security requirements. This sounds like the same thing for people, only systems need to take into account their development life cycles. There needs to

be an understanding of the security ramifications of changing a particular line of code. We should be able to test this and verify that it exists. There should be requirements to remediate known vulnerabilities. If we enter into a contract with a vendor, we need to be able to say that the vendor is going to fix it.

And, what happens if a local administrator says, I don’t want to patch my system. I don’t think I have to. LCB auditors come in and say, in all of their audit reports, that you need to stay up to date with your system patching.

If we see it, as the Office of Information Security, we should have the authority to say, "You will fix that, because you are putting the State's data at risk." You as a private business should be able to say that as well.

We need authority to perform vulnerability assessments and penetration testing. If I run a pen (penetration) testing tool on some of our internal State systems, I may be in violation of State law. Yet, if a hacker does the same thing, there are no consequences because we do not know who that hacker is. That is a real problem. Shouldn't we be able to say, "We know of an existing vulnerability, and now I need to determine whether it is a real vulnerability or a pseudo-vulnerability?" We need both the tools – this is a minimal cost – and the authority to look within the State systems for our office to be able to say, "You will not access that data. Although you may exploit a vulnerability, once you get to a certain point, you can not proceed. You must inform the business owner of the vulnerability and then the owner has the responsibility to fix it."

We need capabilities to rapidly address security vulnerabilities. Those of you who work with the State budget process will smile when I say this. If you look at how fast threats are emerging and you look how fast we are able to apply resources to address those threats, well, there is a huge disparity. We need to find a way – maybe it is an enterprise fund – where we can go forward to apply appropriate controls to a vulnerability as soon as it is identified.

We need a legislator to be able to say, "You're right, we don't want that to happen. Here is an emergency fund of money – maybe only \$10,000 – to save \$100 million worth of data." If I don't have that \$10,000, then there is no way for me to get it.

Also, I need a channel, hopefully not in a public meeting – I don't mind talking about it after the fact, but I don't want to give hackers an understanding of what the State's security vulnerabilities are in real time. People ask me what I do, and I respond, generally, that I can't tell you what I do because it is confidential. That is a bad answer. I should be able to tell you about what we have done, and you need to know that we are actively working. I am struggling with this, but I do need a confidential channel to say we need some resources in this area.

And, we need tools and a flexible funding approach. Right now, if you look at the next slide dealing with "key collaborations", there is some good news. Within the State, we have a State IT Security Committee. All of the Information Security Officers from all of the large agencies get together once a month to talk about what our challenges are. But if we all want to contribute to a common solution, we can't do it because of funding rules. So, we need some effective controls.

Key Collaborations

State IT Security Committee
County and City Information Security Officers
FBI InfraGard
DHS Multistate Information Sharing and Analysis Center (MS-ISAC)



County and city Information Security Officers are also joining in on this. At the GovTech Conference that the Attorney General spoke at, we agreed to come together to arrive at some common solutions. Maybe we all need a penetration testing capability. Maybe it needs to reside at the center where it can be expanded out to everyone who wants to participate. Can we find a way to fund this? The cities and counties want to play. And, the State wants to play. We have the opportunity, the question is "How do we make it happen?"

I want to mention the FBI InfraGard program. That is where we get together and share both public and private sector information regarding our challenges and what do we need to do going forward. This is a valuable group.

At the most recent InfraGard meeting in the north, we had over a hundred people in attendance for a security symposium – business people and security specialists. There is a desire to do this.

Finally, the Department of Homeland Security funded Multi-State Information Sharing and Analysis Center is important. Nevada is participating with every other state to share information about what we have and what we can do going forward. The key is, “How do we effectively apply reasonable controls so as to enable business processes?” I am a firm believer that security improves the business environment. It makes it easier for us to move forward. In the absence of security, we have business problems.

We need to come up with ways to intelligently collaborate and work together. We do have challenges. With emerging technologies moving as fast as they are, we need to get ahead with standardized contract language. We need to get ahead of where our data resides. We need to get ahead of issues dealing with what people are accessing our information.

With that, and I know it is a lot of technological information and I apologize, I will wind up. When I get these opportunities, my hope is to give you a foundational understanding of what needs to be addressed and what we can do as a State to more effectively and intelligently embrace emerging technologies. With that, I would like to get any questions or comments that you might have.

SHERIFF HALEY:

I have a comment by way of example. Almost everything you said today, if you watch the continuing controversy involving AT&T and NSA, is being played out in excruciating detail covering almost all the points you made. Regardless of the politics surrounding that issue, if you simply look at the technology dealing with someone being compelled to provide information, or consider this a target rich area for law enforcement, and consider someone saying, “I want to get in there just this one time, or for just this one reason,” then every one of your examples has an overlay in that particular case.

MR. IPSEN:

There are lots of examples. Yours is one. You have highly sensitive information. At the Homeland Security Committee Meeting, that was one of the areas we talked about. Maybe there is some additional discussion that needs to go on about what is happening in Multi-State ISAC and InfraGard.

Here is how I see what is important. If you have sensitive information, which you do, because the Fusion Centers are aggregating sensitive information, then, if that system is insecure in one area that can be exploited, then the entire system is vulnerable. In that case, what we are doing is facilitating access to our sensitive information by aggregating it.

I propose that having an independent resource, like the State Office of Information Security, with penetration testing skills combined with your people and their insight as to where to look to apply security controls, would provide some independent validation that we are doing the right thing.

I don't want to say, “Oh, I've got a great information security policy. Look at this.” If no one follows it, it doesn't do anything. Let's validate it. Let's put a Core Impact-type penetration testing tool on your applications. Let's validate your security controls. Let's look at your separation of duties.

We do this with State agencies. Some of them welcome us in. I love that. They ask us to visit. I now have a 9-month backlog of agencies asking us to come in and do a security assessment.

I have other agencies that say, “I do not want you here. You are not allowed to come in and do this.” I get concerned when State agencies say this. Why do some take the opposite approach – breaking down your doors to get you to come in?

Islands are by their inherent nature insecure. There is a group-think. I am only as good as the people I have in the aggregate of my environment.

If we can define who it is we can trust, and bring them in – not to look at the data – but to look at the controls and ask, “Can you make any recommendations here?” That is a really good thing. People much smarter than I am can come in and say, “Look, have you thought about this? Or, I say this vulnerability, what about this?” Then, through collaboration, we can be more secure.

That is the role model – the last thing I was talking about – we need to facilitate that. We need to apply State resources and have legislation that encourages rather than discourages that behavior.

Right now, I am inhibited from doing what I need to do. That is a real problem. Thank you for that suggestion. It is very valid, and it is valid in all its aspects throughout government and the private sector.

AG CORTEZ MASTO:

Are there any other questions or comments from Board members? Seeing none, Chris, thank you very much for the presentation. It was very informative for us.

Agenda Item 7 – Possible Funding Sources to Support Technological Crime Investigations

AG CORTEZ MASTO:

Mr. Earl, I think this agenda item is in response to our last meeting when Sheriff Haley asked us to review some of the tech crime forfeiture legislation. Is that correct?

MR. EARL:

Yes, it is. Sheriff Haley’s comments were actually a little bit broader than that. We had just finished a discussion about sexting and other Internet Crimes Against Children issues. During that presentation, it became more abundantly clear than it had been before that the efforts to detect and investigate crimes hinged on our ability to attract and provide training for and maintain highly specialized people. These are the people who do computer forensics and do the type of police work that enables them to handle digital evidence.

So, Sheriff Haley, if I could quote you from the last meeting:

I would like to raise another issue that is a common theme. Earlier, I mentioned that it is very difficult for public safety and district attorney’s offices to obtain the appropriate number of FTEs – people to do these jobs. It is also difficult to acquire the necessary skills and maintain the training, and handle the huge load. We need to address those issues and how we are going to keep up with the demand.

Additionally, we need to discuss whether to address these thing at the end-user level is more effective than addressing them at the point of origin, as is done in drug cases.

These two areas are vital for this Board to continue to review.

As a start for that particular review, I have produced a hand out, which is identifiable by the “Agenda Item 7” at the very top.

Board members have turned over almost completely within the last 4 years. But your predecessors, almost exactly 4 years ago, made a decision to hire me. Almost contemporaneously, we decided to move forward with a mission review that commenced in February 2006.

That mission review began with a questionnaire. I will not go through the entire process. But, there were two end items that came out of that. The first was a Board recommendation that additional positions be established in the Office of the Attorney General for computer forensic examiners and associated personnel.

The second, which is what I really want to talk a little bit about, resulted in AB 306 passed in year 2007. It obtained unanimous passage in both houses. What you will see on the right-hand side of the hand out is the Legislative Council's digest describing what that bill entailed. There were some substantive changes to the Board in terms of membership and other things. But the most important item was essentially bringing into the Nevada Revised Statutes legislation that can appropriately be termed the Nevada Technological Crime Forfeiture Legislation.

If I were to explain that to someone who did not want to spend time with the actual wording of the bill, you will see a text box in the left hand side of the first page of the hand out. That is how I would describe the bill to you from my perspective. With the passage of AB 306 in 2007, a reason now exists to charge a crime, which is a tech crime, as a technological crime by adding some additional language to an indictment. It enables the seizure of instrumentalities and fruits of a crime prior to trial. There is an important change in that this particular statute allows forfeitures to be determined at trial by the trier of fact, who has just adjudicated a guilty verdict – unlike the prior situation, where forfeitures had to be adjudicated in an entirely separate civil proceeding. Also, prior to the passage of AB 306 in 2007, law enforcement could keep forfeiture funds only up to about \$100,000 per year. The passage of AB 306 lifted that restriction. It also involves a split of between participating law enforcement agencies and the Tech Crime Advisory Board based on the equitable amount contributions that law enforcement agencies made to the investigation and prosecution.

Essentially this statute came about when a member of the Board, now departed, recognized, as I did, that there was going to be a long-term funding problem for computer forensic examiners and investigators, regardless of whether they were State employees or whether they were hired by district attorney's offices or by law enforcement organizations. These are essentially very expensive people to maintain because the tools they use, the computers and the software, need to be updated on a continual basis. And, their training needs to be updated as well on a continuous basis. This stuff, quite frankly, is not inexpensive.

One of the ways we considered funding was to move as best we could outside of the scope of the State's General Fund and look to potential sources of revenue from the Nevada Technological Crime Forfeiture Law. Based on recommendations from members of federal agencies, I worked with attorneys in the Department of Justice and here in Nevada. The bill, AB 306, is based on federal and Nevada RICO laws, but without some of the more difficult to prove requirements that are contained in RICO statutes.

Given the wide definitional scope of "technological crime" in Nevada, essentially any crime that involves either a network or storage device, directly or indirectly, in the commission of any other crime, we felt that the scope of the forfeiture law would be sufficiently broad to run from Internet offenses involving children, to virtually any type of premeditated fraud. Indeed, almost any type of premeditated crime involves some type of electronics either directly or indirectly. So, potentially, the new Nevada Forfeiture Law had very broad use.

In the last legislative session, based on some recommendations and projections that were identified by the Las Vegas Metropolitan Police fraud unit and economic crimes unit, we put forward, and had passed, a bill that dealt with criminal use of prepaid cards. Now, unfortunately, it was not passed in the form it was initially drafted. As drafted, the bill provided a very careful step-by-step procedure.

The reason that step-by-step procedure was included was that the search and seizure laws in the State, like other states, do not necessarily line up very well with the requirements for electronic

seizure. Many of those procedures were taking out by the second house, the Assembly, during hearings. But that does not mean that we can not move forward with the bill.

So, big picture, the statute that deals with potential freezing and seizure of funds associated with the criminal use of prepaid cards is a specific instance where electronic funds can be made susceptible to the forfeiture statute for technological crimes, passed by the Legislature in its previous session of 2007.

Now, to my knowledge, neither of these particular statutes has been used. I have seen no evidence that any type of forfeiture funds have begun to flow to the Board or have been involved in indictments at whatever level, anywhere in the State.

At the bottom of the page, you will notice that there are possible explanations. I do not know what the explanation is, and, in fact, there may be a series of explanations.

But, quite frankly, I am very close to running out of ideas in terms of targeted legislation using tools that are normally available to prosecutors, prosecuting attorneys, to come up with schemes that would proved for sources of funding outside the State General Fund in support of computer forensic examinations and technological training for law enforcement throughout the State.

With that as background – and let me repeat myself – I am running out of ideas, I turn to the Board for any additional suggestions members have.

AG CORTEZ MASTO:

Thank you, Mr. Earl. Are there any comments or questions from Board members?

SHERIFF HALEY:

I would recommend that your questions be written and submitted to the District Attorneys and their Boards to raise that question. The other thing is that often times, and I have seen this in other types of legislation, often times it is a case of educating everyone in the process. In the case of our own lab, we actually wrote to different sheriffs and chiefs to say we are not collecting fees where fees can be collected. This direct approach has worked for us before. I also suggest that we get folks working on the front line, one of my detectives is here now, talking about why this is not working. That is the point of charge. So, whether or not these things are being considered by the District Attorneys and including these charges in the final case is key.

AG CORTEZ MASTO:

Are there any other comments or questions? Thank you very much, Mr. Earl.

Agenda Item 8 – Board Comments

AG CORTEZ MASTO:

Moving on to Agenda Item 8, are there any comments from the Board?

Agenda Item 9 – title

AG CORTEZ MASTO:

Hearing none, and moving to Agenda Item 9, are there members of the public in northern Nevada who want to address the Board? Seeing none, are there members of the public in the south who would like to address the Board.

SHERIFF GILLESPIE:

I was just going to say, we don't see any.

AG CORTEZ MASTO:

Thank you. Moving on to Agenda Item 10.

Agenda Item 10 – title

AG CORTEZ MASTO:

I suggest we recommend scheduling meetings as we have done in the past with Mr. Earl taking the lead. Is that alright with you, Mr. Earl.

MR. EARL:

That is certainly fine. Subject to any suggestions from the Board, I will undertake either to contact Members directly or through their administrative assistants to target sometime in mid-March for our next meeting.

AG CORTEZ MASTO:

Thank you.

Agenda Item 11 – title

AG CORTEZ MASTO:

Agenda item 11 is adjournment. I declare us adjourned. Thank you everyone for participating today.

Time: 11:58 AM

Respectfully submitted,

James D. Earl

Approved by the Board at its subsequent meeting on March 23, 2010