

Minutes of the Technological Crime Advisory Board

March 23, 2010

The Technological Crime Advisory Board was called to order at 10:00 AM on Tuesday, March 23, 2010, Attorney General Catherine Cortez Masto, Chairman, presided in Room 4412 of the Grant Sawyer Building, Las Vegas, Nevada and via videoconference in Room 3138 of the Legislative Building, Carson City, Nevada.

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
Assistant Special Agent in Charge, Mark Doh, (*Meeting designee for Special Agent in Charge Kevin Favreau, Federal Bureau of Investigation (FBI)*)
Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)
Sheriff Mike Haley, Washoe County Sheriff's Office
Chris Ipsen (*Permanent Designee for Dan Stockwell, Director, NV Dept. of Information Technology*)
Dale Norton, Nye County School District Assistant Superintendent
Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association

ADVISORY BOARD MEMBERS ABSENT:

Daniel Bogdan, U.S. Attorney, Department of Justice (DOJ)
Nevada State Assemblyman Harry Mortenson
Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE)

TASK FORCE MEMBERS PRESENT:

Detective Dennis Carry, Washoe County Sheriff's Office (WCSO)
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)
Bob Cooper, Bureau of Consumer Protection

Anne-Marie Cuneo, Public Utilities Commission
Jeneane Harter, HiTech Communications
Ernie Hernandez, Health Division, Department of Health and Human Services
Paul Maguire, Public Utilities Commission
Theresa Presley, Health Division, Department of Health and Human Services
Todd Shipley, Vere Software
Mary Siero, Boyd Gaming
Ira Victor, InfraGard
[Others, who did not sign in]

Agenda Item 1 – Call to Order – Verification of Quorum

AG CORTEZ MASTO:

The meeting is called to order on March 23, 2010 at 10:00 AM. The first item on the agenda is the call to order and verification of a quorum. Mr. Earl, please call the roll.

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

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

AG CORTEZ MASTO:

Moving on to Agenda Item 2, the discussion and approval of minutes from the December Board meeting, everyone should have a copy of the minutes. If there are any edits or comments, please make them now. Otherwise, I will entertain a motion.

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

The motion to approve the minutes was approved unanimously.

Agenda Item 3 – Reports regarding Task Force activities

AG CORTEZ MASTO:

Moving on to Agenda Item 3, the reports regarding the task force activities. This is an opportunity for Board Members and concerned agencies to discuss what has been happening within their jurisdictions.

Before we get started, I would like to highlight the recently released report from the Internet Crime Complaint Center (IC3). There is some very interesting information. One area I think is important for all of us to be aware of: in 2009 Internet crime cost users about \$560 million. That was up from \$265 million the year before. This rise reflects a 22% increase in the number of complaints handled by IC3.

What was more startling to me – and I am sure you were all aware of this – Nevada ranked second, behind the District of Columbia, for the highest per capita rate of perpetrators in the United States.

Looking at some of the statistics, it is clear that major areas of complaints are non-delivery of merchandise and repayment, where either a seller did not ship the promised item or the buyer did not pay for an item. These accounted for 11.9% of the complaints.

Advanced fee fraud, a scam where the target is asked to give money up front, often times for a reward that never materializes, accounted for 9.8% of the complaints.

Interestingly enough, the mean dollar loss was \$5,580 and the median dollar loss was \$575, reflecting that a relatively small number of cases involved hundreds of thousands of dollars lost by the complainants. You should have information regarding this.

I would now like to open discussion to member agencies to give us an update as to what is happening in their jurisdictions.

MR. VANDERSTELT:

Good morning, Madam Chair and members of the Board. I am Eric Vanderstelt, Supervisory Special Agent with the FBI. I am pleased to be able to speak to you this morning about some of the activities conducted by our southern task force. You will see we have had a number of convictions of technological crime-related investigations over the last few months since we last met. Some of these convictions relate directly to what you were speaking of, Madam Chair.

In December, a jury returned a guilty verdict against a man charged with coercion and enticement of a minor. In March, he was sentenced to 10 years federal imprisonment.

In December, a man was sentenced to seven years federal imprisonment after having pled guilty to a charge of receipt of child pornography.

Also in December, a man was sentenced to 10 years federal imprisonment after having pled guilty to possession of child pornography.

In January, a woman pled guilty to conspiracy to commit wire fraud and agreed to restitution of approximately \$140,000. Sentencing in that case is scheduled for April.

In January, a man was sentenced to five years in federal prison after a guilty plea to receiving child pornography.

Also in January, a man pled guilty to conspiracy to commit wire fraud and agreed to restitution of approximately \$939,000. Sentencing in that case is scheduled for later this month.

In February, a jury returned a guilty verdict against a man charged with coercion and enticement of a minor. He faces a mandatory minimum sentence of 10 years in prison.

These are some of the examples I can speak of. We have active, on-going investigations that I will be pleased to speak to you more about in later sessions. Again, I would like to thank you for the time this morning to share these results with you.

AG CORTEZ MASTO:

Thank you for joining us this morning. We appreciate the information. Are there other Board members or partner agencies wishing to report at this time?

SHERIFF HALEY:

Yes, Washoe County Sheriff's Office.

DETECTIVE CARRY:

Thank you Attorney General Cortez Masto. I am Dennis Carry, Washoe County Sheriff's Office, Northern Nevada Cyber Center.

The Task Force activities in the north have seen an increase since the last meeting, partially due to the collaboration we have built out of the Northern Nevada Cyber Center, working together, hand in hand. We are able to get through more cases. We have processed and executed over 12

search warrants since the last Board meeting, mainly for child pornography. These have resulted in more than 8 arrests so far. Some of these arrests have involved a subject identified as a nurse at a local hospital in Reno. He had close to a million images and videos of child pornography. He had been doing this all the time. When asked about child pornography and whether he would ever touch a child, this subject responded that he would not want to do that, he doesn't think he would do that, but he really can not predict the future. This really goes to show what type of activities and what type of dangers these people pose.

This subject and two others received life sentences recently, although they may become eligible for parole after 5 to 8 years. They will at least be under life long supervision involving monitoring to see if there are reoccurrences of child pornography crimes.

Another subject is being sentenced tomorrow, who is likely to receive life.

We are busy working intrusion cases as well. We noticed a few computer intrusion cases where password stealers were put on computers. The downloads most likely came from either China or Russia. We are looking at how these occurred in order to address the problem and try to address it in the future.

We are working on several other local cases with the FBI.

Returning to the child pornography cases associated with the eight arrests, we have recovered over 1.5 million images and videos of child pornography since the last Board meeting. So, we have been rather busy. Thank you.

AG CORTEZ MASTO:

Thank you. Are there any comments or questions from Board members? Are there other comments? Mr. Earl, if you would, I think in the last meeting, we had talked about the committee that Brett Kandt was handling regarding sexting and Internet Crimes Against Children (ICAC). There was a question about status and participating agencies. Could you give us an update please?

MR. EARL:

Board members will recall that there were several bills during the last Legislative session sponsored by members. One of the more important dealt with updating Nevada's child pornography laws to deal with streaming video. At that time, there were a number of discussions that involved law enforcement and district attorney's offices. A decision was made not to try and hurry through legislation that dealt with sexting. In the aftermath of the session, Brett Kandt, who chairs the Council for Prosecuting Attorneys, undertook the formation of a working group to look at possible sexting legislation and some additional potential changes to Nevada's child pornography statutes.

This is the question raised at the last Board meeting. He has been working with representative of the Washoe County District Attorney's Office, the Clark County District Attorney's Office, and the Las Vegas Metropolitan Police Department (LVMPD). He is discussing these issues, largely sexting but also ICAC-related legislative changes, with the Sheriffs and Chiefs Association. Brett has told me that he would welcome other participants. Brett is well known throughout the law enforcement community. If other agencies would like to participate in that exercise, they can contact him directly, or contact me, and I will pass contact information on to Brett.

AG CORTEZ MASTO:

Thank you, Mr. Earl. Yes, Senator Wiener.

SENATOR WIENER:

Thank you, madam Chair. Because I dealt with cyber bullying last session, including integrating a definition of "bullying" because we did not have one in statute, either before the end of session, or

very shortly thereafter, I put in a bill draft request (BDR) for sexting. So, I will be happy to work with the working group and with our Board to develop the policy piece. The BDR has been reserved for the sexting subject.

AG CORTEZ MASTO:

Great, thank you. We will let Mr. Kandt know that as well. If there are not other comments, let's move on to agenda item 4.

Agenda Item 4 – Presentation by Matthew Nelson, Senior Legal Consultant, EMC, Meeting the Challenges of Electronic Discovery and E-Compliance in the Public Sector

AG CORTEZ MASTO:

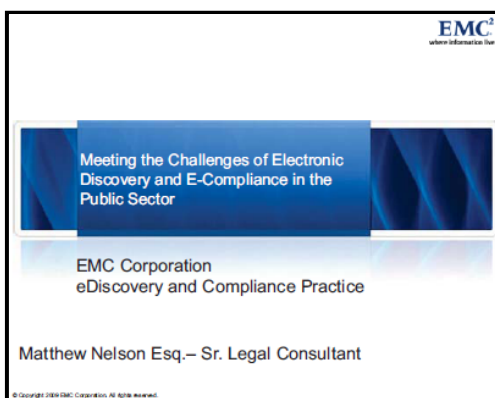
This agenda item involves a presentation by Matthew Nelson.

MR. NELSON:

Good morning, Madam Chair and members of the Board. It is a pleasure to be here today. By way of introduction, I am an attorney and legal consultant in EMC's e-discovery and compliance practice. I need to tell you before I jump into my Power Point presentation that I really appreciate your commitment to spending the next three hours discussing the Federal Rules of Civil Procedure. [Laughter.] Of course, I am kidding.

I am going to take about 30 minutes of your time to talk about this topic – meeting the challenges of electronic discovery and e-compliance in the public sector. I encourage you to ask questions throughout. I want to make sure that I am addressing the objectives you have today in terms of understanding the subject matter better. Please feel free to interrupt me at any time.

By way of background, I believe I was asked to speak today because EMC is known as a company that manages information. We manage information for thousands of customers in the public and private sectors. I specifically work within our global e-discovery and compliance practice as a former litigation attorney to help our customers bridge the gap between the technology department and the legal department. That is a bit oversimplified, but we find that now that we are moving from a paper era to an electronic era, there is a real need to bridge the communications gap that exists. Various departments need to work together to make sure that they meet the legal requirements around electronic discovery.



The discussions points today are listed in this slide. First, what are the differences between the public and the private sectors? Do I need to be as concerned in the public sector as I do in the private sector when it comes to electronic discovery? Second, what are the various approaches to e-discovery that have been evolving over the last 7 to 8 years? Finally, we will wrap up by talking about some of the trends that we have been seeing in the industry from a technology standpoint.

Let me tell you why electronic discovery is important to the public sector. Robert Swofford was a lucky man. He actually won the Florida state lottery a few years ago. Unfortunately, his luck changed. He woke up one night because he heard a disturbance outside. His dog was barking. He woke up, grabbed his firearm, and went outside to investigate.

He saw a couple of people walking around in his yard with flashlights. He encountered these men and was shot seven times. Unfortunately, he was shot by county police officers who had chased a car burglary suspect onto his property.

As you might imagine, an investigation and litigation ensued. The problem is that, as we know, an investigation and litigation triggers a duty to preserve evidence, both on the criminal side and the civil side.

What happened is that Seminole failed miserably in its obligation to preserve information. There was a lot of evidence at issue. The guns that were used in the shooting were recycled. Uniforms were lost. The radio equipment was lost. Also, importantly, there was electronic information that was lost in the form of email messages.

One of the officers involved in the shooting had used his laptop that day, but the laptop was recycled almost a year after the event had taken place. Similarly, there was a request for email and other electronic evidence from other Seminole County employees. That email evidence was lost as well because the county did not have an internal process to preserve the information. Frankly, there was no litigation hold notice provided by Seminole County to its employees.

The in-house counsel for the county received a notice from Swafford's counsel, and he simply forwarded that notice to some key executives within the Seminole County Police Department. They really did nothing after that.

The judge said that this kind of conduct was unacceptable. Judges in this situation, obviously, have a lot of leeway to correct the situation. They often do that by issuing sanctions. That is exactly what happened in this case.

Sanctions: [Swafford v. Eslinger](#) **EMC³**
where information lives

"That we are here on this issue is inexplicable and inexcusable."

- Destroyed ESI and other evidence
- Sanctions
 - Adverse inference
 - No finding about evidence necessary due to bad faith
 - Monetary sanctions of ~ \$300,000
 - Some will be awarded against in-house counsel (later ruling)
- Does this change the playing field?

Swafford v. Eslinger, Case No.: 8:08-cv-00066-04-35DAB, M. Dist. FL (Orlando) 9/28/09

© Copyright 2009 EMC Corporation. All rights reserved.

THE COURT: Well, what was done in response to the letters?
MR. SWAFFORD: Well, we'd have to ask each individual person within each individual -
THE COURT: Well, you've already done that, and what did they tell you?
MR. SWAFFORD: There wasn't anything particular done to segregate evidence.
THE COURT: So, they got the letters, file it, and that was the end of it?
MR. SWAFFORD: Well, yes, Your Honor. Nothing was particularly left back.

Sanctions can come in many different forms. Sometimes there can be a monetary sanction. Sometimes there can be a default judgment where you lose a case without having a chance to try the case on the merits in court. Another sanction we are seeing quite often in these situations is an adverse jury instruction.

The judge in the Swafford case issued both a monetary sanction against the offending parties, and she also entered an adverse jury instruction. To give you a sense of what that adverse jury instruction looks like, it is a very powerful instruction. In civil court, many times there is a

settlement when an opponent knows it is facing an adverse jury instruction. Essentially it allowed Swafford's counsel to walk into the courtroom and, during opening argument say something like this: "Ladies and gentlemen of the jury, there is a lot of information you are going to see and hear over the course of the next couple of days. Unfortunately, there is a lot of electronic evidence you will not be able to see because my opponent here deleted files that he had a legal obligation to preserve."

Now, as you can imagine when a jury hears that kind of opening statement, there is an appearance of impropriety. It does not really matter what the email messages said, or what the content provided. Typically, we find that juries want to deliver a message in that type of situation. So, you will find that the parties settle. This case has not been resolved to my knowledge, but there is that impending adverse jury instruction.

Another important note regarding this case – in-house counsel was held personally responsible for not doing a good job of applying a litigation hold or notifying employees that they had a duty to preserve evidence. He is going to be held jointly and severally liable for the monetary sanction. This is the equivalent to the attorney's fees and costs on the other side that were spent investigating the loss of evidence issue. As you can see, the stakes are very high.

Let me give you another example. Not long ago, the city of Beaverton decided that it wanted to try and annex some unincorporated property that belonged to Nike. The rationale for doing this was rather straight forward. It would increase the tax base by over a million dollars a year, simply by incorporating this unincorporated land.

Folks at Nike got wind of this and requested some public records. Eventually, Nike filed a law suit because it believed the information was not forthcoming. The judge in this case, similarly, was upset at the lack of response by the city of Beaverton. She felt the city was trying to hide

Contempt: City of Beaverton v. Nike EMC²
where information hurt

- In 2004, the Beaverton City Council adopted an aggressive annexation policy that included property owned by Nike
- Nike claimed the City was not forthcoming with public records requests regarding leaders' annexation plans during discovery.
- Judge found the City in contempt of court because leaders hid documents from Nike.
- The City's total cost in the case was at least \$890,000, including the costs of a computer search and the hiring of two private law firms to defend city insurers' actions.
- In the midst of the public records battle, Nike was granted a 35-year exemption from forced annexation into Beaverton by the legislature.

From *The Oregonian* of Thursday, Feb. 22, 2007

© Copyright 2009 EMC Corporation. All rights reserved.

evidence, and that the city was not producing the information that it should have. She too issued sanctions. She also found Nike in contempt of court. I spoke to a group in Portland, Oregon about a year ago. I was told that not only were the taxpayers spending a lot of money on this case, but a number of the public officials were either not re-elected or lost their positions as a result of this incident. As you can imagine, this was very high profile in Oregon.

This provides some flavor for the types of things that can go wrong if you don't handle the electronic discovery issue appropriately. Frankly, in my experience over the past 10 years, I have spent a

lot of time talking to both private and public sector folks. It seems that the public sector has been a little bit slower to recognize some of these obligations. But, I have seen a significant shift in the past two years. There are a lot of agencies looking at how to come up with good internal policies to manage their information more effectively. They are also specifically focused on addressing some of these electronic discovery problems.

Justice Department Requests Millions For eDiscovery EMC²
where information hurt

The Justice Department wants to add dozens of tech-savvy staffers and lawyers to handle the new problems posed by Electronic Discovery

- The Civil Division of the Justice Department
 - 12 new positions
 - \$2 million budget increase
- The Environment and Natural Resources Division
 - 9 new positions
 - \$1 million budget increase
- The Executive Office for U.S. Attorneys
 - 12 new positions for electronic discovery
 - \$2 million

Mainjustice.com, Ryan Reilly, February 17, 2010

© Copyright 2009 EMC Corporation. All rights reserved.

This slide is indicative of that happening at the federal level. You can see that the Justice Department recognizes the need for tech-savvy attorneys and technology that will help it address the problem more effectively than has been done in the past. We are seeing some change.

Let's step back for a second. What is electronic discovery? Technically, it is the exchange of electronic information between parties engaged in litigation. We find that the term is used more broadly. The term is not restricted to litigation. The same obligation to find, preserve, and produce information is really going to occur in other areas as well – internal investigations, regulatory investigations, internal or external audits, and, of course, in the public sector, important to you, under public records acts.

What is eDiscovery? EMC²
where information hurt

Electronic discovery (eDiscovery) is the exchange of information between parties involved in litigation.

Litigation <small>Current and reasonably anticipated state and federal litigation</small>	Investigation <small>State and federal regulators, IRS, OSHA, SEC, NASD, FINRA, NERC, NRC, HIPAA, Data Privacy & Protection</small>	Audit <small>Internal and external audits of the organization's books and records, Defense Contractor Audit, Government Contract Audits</small>	Public Disclosure <small>Federal, State and Local - Freedom of Information Act, Open/Public Records Acts</small>
-----------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------

Another way of looking at this problem is to see e-discovery as just another information management problem. I know that many Board members deal with different types of technical issues and information management issues. I find that e-discovery is a tip of the spear issue. Folks are very focused on it because the risk of non-compliance is extremely high. Also, if good processes and

technologies are not in place, then the cost becomes extremely high as well.

A main driver that many of you are probably aware of is the amendments to the Federal Rules of Civil Procedure in late 2006. The Rules of Civil Procedure are simply the rules that govern the civil litigation process. They have been around since the 1930s. Not until recently have they been changed to deal with the nuances of electronic information. From these rules come some pretty important guidelines.

eDiscovery Trends – 2006 Federal Rules of Civil Procedure (FRCP) Amendments

- Electronically Stored Information (ESI) explicitly included
 - Management **plan** to discovery impacts costs of eDiscovery
- Very early **meet and confer**
- “Preserving” appears in the rules for the first time
- Requirement to understand the **sources** of ESI
- Less obligation to produce “**inaccessible**” content
 - But you still may have to hold it (can be just as burdensome)
- Limited “**safe harbor**” for good faith inadvertent destruction of content
 - Best protection through solid records management program, including litigation hold
- Some protection for **inadvertent waiver** of atty-client privileged materials

Rule 45 – Covers Subpoenas

© Copyright 2006 EMC. Content is All rights reserved.

The rules make it clear that electronically stored information is discoverable if it is relevant and not privileged. They define the term “electronically stored information” very broadly. There was some uncertainty among attorneys as to whether all kinds of electronically stored information must be considered and produced. These rules make it clear that since the term is defined broadly, it doesn’t matter what type of file is being sought or where the information is stored. If it is requested, discoverable (not privileged in some way), then you may have an obligation to produce that information. As you can imagine, organizations that have accumulated data

and have duplicated data for decades face a very big challenge – both in the public and private sectors – to find that information and produce it in compliance with these rules.

What Are The States Doing?

EMC²
where information lives

11 eClerks Electronic Discovery: What Every Attorney Needs to Know 3/19/2010
© Copyright 2006 EMC. Content is All rights reserved.

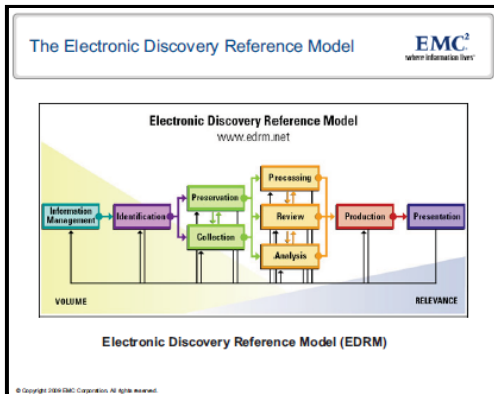
We are seeing states following suit by drafting rules that are similar to the Federal Rules of Civil Procedure that will govern proceedings in their own state jurisdictions. This chart provides an indication of what has been done. For the most part, the state rules pretty closely mimic the Federal Rules of Civil Procedure. There are, however, some variances between states. I will be happy to come back to this group to talk about some of the differences if and when Nevada considers adopting some of its own e-discovery rules.

Next, I would like to discuss three approaches to e-discovery. I want to make clear here that many of you deal with computer forensics, especially on the criminal side. Of course, you are going to yield electronic evidence that is relevant to criminal and civil evidence on the forensic side.

What I am talking about is not recovering deleted files from hard drives, not investigating what web sites a user may have visited, and not tracking IP addresses. I am talking about a similar problem around electronic evidence that is more specifically focused on collecting active files, as opposed to deleted files. The problem there is that there is so much electronic information spread across many different data sources. Active data and deleted data are usually addressed using two different processes.

On the heels of the Federal Rules of Civil Procedure being passed, we saw a group of legal and technology scholars get together to identify the various steps in the electronic discovery process. These are those steps. Information management is something I think of as a long term electronic discovery strategy. Essentially, it is the same thing as an archiving or records retention strategy.

The idea is that you generally want to get rid of any information that you do not have a legal or business reason to keep. Otherwise, you are simply increasing the size of the pool of information that could be subject to the discovery process in the event that there is a law suit down the road.



That is what I think of when I see the first block on this slide "Information Management". The remaining blocks outline the various steps that are taken to respond to litigation, a public records request, or an investigation.

How have organizations addressed these problems? I find that most organizations still are taking the manual approach. What I mean by that is this. As soon as a law suit is filed, and a duty to preserve information is triggered, organizations react in a couple of different ways. They may ask individual employees, who are likely to have information relevant to that case, to identify the files they have

that are relevant. They then will ask those employees to produce those files within the organization.

#1 The Manual Approach

- Data is "collected" by 3rd Party Vendors or Employees
 - Employee self-collection has inherent risks
 - IT or 3rd Party Vendors results in "over" collection
 - Backup tapes are pulled as a final precautionary measure
- Lack of resources & expertise
 - Data may be altered when copied (meta data)
 - IT may be asked to testify as an "expert" witness
 - No chain of custody/audit trail exists or manually created
- eDiscovery expenses
 - No way to cull through data internally so reliant on law firms and vendors
 - Law firm review is not cheap (over \$18k/gigabyte)
- Early case assessment – money spent before value of case evaluated
- Risk of Sanctions - Manual process leads to high risk that data is lost or overlooked

The problem with this approach is that it can be a very risky proposition. Sometimes the people you are asking to produce the information may be involved in the incident and they may not produce the information they should produce. That puts the agency or department at risk. Similarly, their memories may fade over time. Maybe they just forgot about information they possess that is relevant. It may end up not being produced, and that could lead to a sanctions situation. So, that is a risky way to approach the problem.

As a result, we have seen the pendulum swing in the other direction – the over collection of data as opposed to the under collection of data. What I mean by this is to err on the side of safety in order to meet the initial duty to preserve evidence. We see organizations making massive copies of their data. They usually start by pulling their backup tapes and taking them out of their normal recycling schedule. They will also go from employee to employee to make copies of their computer hard drives. They will also start copying data from email servers, from file servers, and from other locations where data might be hiding.

The problem with that approach is that, eventually, someone has to cull through that data, either internally or with the use of third party vendors. Third party vendors charge a lot of money. I used to work for one. We charged thousands of dollars per gigabyte to duplicate files, eliminate file types, run key word searches, all before the attorneys even began reviewing the files. So, there are a lot of challenges with that approach, most of them are expense related.


The problem with the manual approach is that it is risky, because you are manually collecting data and moving it around. This means that metadata could change, for example, changing dates of documents. Judges do not like that either. The costs are extremely high. You are collecting a lot of information, and, eventually, attorneys will be paid to review that information as well to segregate the relevant from the irrelevant files.

We have found that many public sector entities are looking to bring some of the process in house, instead of either relying on a manual approach and/or third party companies to help them cull the data once it has been collected. They have started by focusing on technology that has been in use like email archiving technology or archiving technology. The general idea there is to take the data within a particular department or agency and try to consolidate that data into one central

repository. The idea is that once data resides in a central repository, then we can go to one place to search and find information that is needed for a case.

#2 The Enterprise Approach: Email Archiving **EMC²**
where information lives

- **Pros:**
 - Search Central Repository for eDiscovery
 - Automate Retention Policies for Compliance
 - Reduce Storage Costs
- **Cons:**
 - Archiving is not a complete eDiscovery solution
 - Data must be migrated Before it can be searched
 - Migrating all ESI is unrealistic due to Time & Expense
 - Inability To Define Retention Policies stalls implementation



© Copyright 2009 EMC Corporation. All rights reserved.

Another added value to this archiving technology, and the reason most organizations originally implemented it, is to reduce storage costs. By centralizing information, think of emails for example, and how many duplicative emails an organization might have, those duplicative emails can be eliminated on the back end. This results in a significant reduction in storage costs.

Finally, these same archiving tools can be used to automate an organization's retention policy. So, once an organization has defined its policy, it can use this technology to automatically execute those policies and apply them.


The bad news is that this is not a comprehensive solution for e-discovery. Most organizations have to deal with decades of data, and of electronic information. It simply is not easy, from a technology standpoint, to go out and find all that data and move it into a centralized archive. It is a very time consuming and expensive process whenever you have these investigations and litigations that you need to address.

We also find that organizations have difficulty implementing these archiving solutions because no one can agree on what the retention policy should be. That is always a big challenge, both in the public and the private sector. Many times we see this approach to electronic discovery failing.

3 The New Enterprise Approach: Automated Enterprise eDiscovery **EMC²**
where information lives

Pros:

- Search the enterprise from a single computer
- Attorney Early Case Assessment through instant searching is a reality
- Automate Litigation Hold process
- Legal User Interface to create and manage every new matter
- Reduce processing & outside counsel Costs by up to 50%
- Chain of Custody reports created automatically
- Multiple ROI - Same Solution Can Be Utilized for Data Security, Storage Management, Regulatory Compliance



© Copyright 2009 EMC Corporation. All rights reserved.

What we are seeing evolving is what I call the new enterprise approach to e-discovery. This is a move from the manual approach to an automated way of dealing with electronic discovery. We have the same obligations, but by implementing new technology, that changes the process to a certain extent.

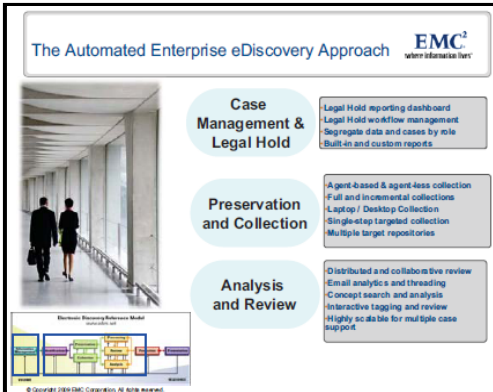
I may get a little more technical here. Forgive me if I become either too technical or too simplistic. I am trying for a middle ground approach. Let me explain how this technology works.

The main idea is that this is an appliance-based technology. All that means is that it is self-contained hardware and software – literally, in a big box. You

take one of these big boxes and you roll it into your department's or agency's data center. Once you have done that, you connect it to your network with the help of the IT staff, and you target the various data sources within your environment that you may want to search for an e-discovery matter or investigation. The various types of data you might consider would include desktops and laptops. As long as a user is connected to the network, you could target those desktops and laptops. File servers and email servers – Exchange, Outlook, Lotus Notes – and different types of archives would be included. Remember, I talked about different types of email archive solutions. Sharepoint is another tool that we are seeing used more and more.

Once you have pointed to these different data sources within your environment, you can then create an index of that data. All that means is that the data now becomes searchable. You do not necessarily have to move that data anyplace, you can search that data within your environment regardless of where it resides. You are searching both the metadata and the text of the

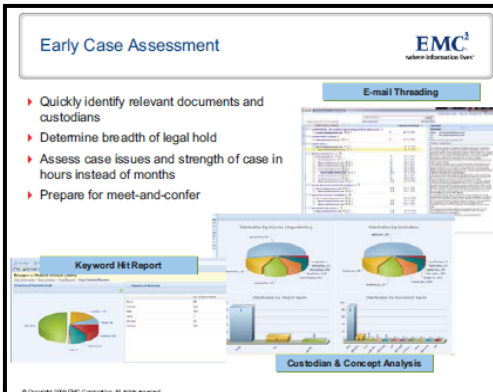
document. You do not need to change or process the data in order to be able to search that information. Think of it as Google searching your own environment.



Once you have indexed the data and made it searchable, the process changes. When I find out about a law suit as an attorney, I know that I have a duty to preserve evidence, but I also want to learn about the case. In the old fashioned way of doing things, I was not really able to understand my case until I have had people collect the data for me and process the data. Only then could I begin reviewing it. But, this technology allows us the ability to do some early case assessment. As an attorney, I might log into the system and run some key word searches of my key employees, who I think are relevant to this particular matter. I can begin to figure out whether I have a good case or a bad case. That early case assessment is extremely

valuable because it gives me knowledge as an attorney. Hopefully, I would be able to resolve the case early before incurring all those downstream expenses and all that downstream time.

Let's assume for a moment that I do not find a smoking gun, and that I am unable to resolve the case quickly. I still need to notify employees that they have a duty to preserve evidence. The same technology will allow you to automate the notification process. I would identify my key employees in a typical situation, and I would send them a notification through this technology, and I would ask them to respond affirmatively that they know they have a duty to preserve evidence and that they are abiding by this duty.



It is one thing to tell employees to preserve information, but it is quite another to actually preserve that information. The next step might be actually collecting the data that might be relevant to this case. At the beginning of the case, I might not know all the details, and I have this broad preservation obligation, so I am going to do a larger "grab" of information, so my collection parameters are going to be pretty broad. Usually, I will focus on key employees and date ranges, and maybe file types. I can use those parameters to construct a search and to find the files that are likely to be relevant to the case. Then, I can take those files and make a copy of them in an automated way, not in a manual way by going from system to system and

computer to computer. In an automated way, I can take the search results and copy them to a secure storage device, so that now, the employee can continue working on his version of the file, but I have met my legal obligation by preserving a copy of the file that can not be altered or deleted. So, I am minimizing the risk to the organization of losing data that I have an obligation to produce.

Stepping back to the legal process, probably the next thing I would do as an attorney is I would have a conference with the opposing counsel. We would probably come to some kind of an agreement with regard to what actually needs to be produced. We would probably narrow the scope of what was originally collected by agreeing on new data ranges. So, for example, maybe my opposition said, "I want all files from 2000 to present." Well, in reality, you probably need only all files from 2005 to present. So we can get rid of those files that aren't relevant. Maybe they

have asked for data from 30 custodians originally, but we have negotiated that perhaps only 10 of those custodians are relevant. So, we can narrow down the parameters that way.

There are certain types of system files that probably are not going to have any data that is relevant to the case. So, there are certain files we might exclude from actual production to the other side. So, through this meet and confer conference between the opposing parties, you will agree to those terms. You will also probably agree to some key words that will be used to then search the data set that has been collected for that case. That data will then be culled down based on those parameters. It will also be de-duplicated.

SHERIFF HALEY:

Sometime during this presentation, would you enlighten us regarding cloud computing and the civil liabilities of the public sector?

MR. NELSON:

Absolutely. What I will do is finish addressing this slide, and then circle back and respond to that question.

Once the parameters have been defined in the meet and confer conference, the specific data set that has been collected can be culled down. Essentially the idea is that the less information that is passed on to third party vendors and opposing counsel and the lawyers that need to review that data, the more money is being saved. This technology is designed to automate that process of culling down the data set, which results in tremendous cost savings.

AG CORTEZ MASTO:

Mr. Nelson, I have a couple questions for you on the process. My office has been dealing with this issue, not only internally, but as the legal counsel for all the State agencies. Clearly, this is a concern for our State clients as well – how we help them to manage that information.

But I want to go back to the first step – which has been our challenge – how we collect that data. Let's just talk about emails and desktops and laptops. There is so much data, just in emails that pass back and forth in my office, let alone across State agencies. The retention policies, and defining those policies, are just gargantuan tasks, and that is our first step. The next step, when we are able to define those policies, is implementation. How do we implement them with the technologies that are available?

Let me give you an example. In my office alone, I get copied on emails, or I am a direct recipient of emails. When do I decide that I have to retain those emails? The ones that I am copied on, or only the ones where I am a direct recipient? If we are retaining all those emails, that is a lot of data. Where do we put that data, and is there technology available to handle all that data, move it, and put it into a format that we can then go back to, cull through, and ultimately decide how to handle it?

To me, that is the hardest part – the retention policies and their definition. And then, once we understand it, making sure our attorneys understand it, make sure our investigators understand it, and ensure we are following it. And, at the same time, also advising our clients.

I know the agencies here will have the same issues, and the attorneys representing them would have the same issues in advising their clients. So, for me, what is important is the retention policy and getting started on that process.

I am curious regarding your knowledge of best practices in this area and your thoughts on addressing just the retention policy and how we would define every single email that comes to us and what needs to be retained and what doesn't.

Clearly, other issues will be involved such as whether or not the communication is privileged. How we define confidentiality? What is available to the public, what is not? I realize that is a whole other issue. However, just defining what emails we keep is really the tough task we have in front of us. For me, that is what we have been working on in my office, and it is indeed gargantuan.

I am curious about your thoughts. In dealing with other agencies, how have they addressed these issues?

MR. NELSON:

I can tell you, Madam Chair, that this is an age-old problem in both the public and private sectors. What we are finding is that organizations are faced with considering several options. Sometimes they take the position that we want to save everything just to ensure that we haven't deleted data that we probably have a legal obligation to preserve. From a retention standpoint, that is problematic because that increases your storage costs. Also, if you are involved in a law suit down the road, that is more information that has to be considered for that lawsuit as well as every subsequent lawsuit. So, you are increasing the pool of information that is discoverable.

The other option is, let's have a very short retention policy. Let's say for email, we want to try and delete everything within two years on a departmental basis. But, your employees, depending on what they do, may need that information for longer than a two-year period in order to do their job effectively.

Also, you may have legal obligations in the public sector to keep information longer than two years. These are kind of the opposite ends of the spectrum. The other thing we see is that organizations try to address the problem by coming up with multiple retention schedules. That forces an employee to choose from 20 or 30 different categories every time they receive an email. They have to place the email into the appropriate bucket, if you will.

Typically, we recommend a smaller bucket approach. You are not asking the employee to become a mini-records manager. Rather, you are automating the process so that the employee has fewer choices to make in terms of into which bucket to place the email. Each of those buckets may have a different retention period.

The general rule of thumb is, "Simpler is better." With the big bucket approach, you may be saving some information longer than you would like, so it is not a perfect system. But, you are also decreasing the burden on the employee to fit the email into the right bucket.

I am not going to solve the policy question in terms of what your policy should be today – that is going to vary from agency to agency. But there are tools to address that. Once the policy has been defined, those archiving tools are useful. There are a number of email archiving technologies on the market. Those technologies are designed to centralize the way email messages are stored.

You can take emails that might be stored on an individual's laptop or desktop – PST files are what they are called – and move them into the central repository. The idea there is that you don't have to look on all the laptops or desktops, you can go to the central depository. That same technology will reduce your storage costs because it can get rid of the duplicative messages on the back end. It is also a central area where you can search to find email messages that might be relevant to a particular matter.

There a lot of different approaches as to how to address the policies. Again, we tend to see the "big buckets" approach as the most successful. Getting buy in from the various stakeholders in the department as well – building consensus – I think is important. Your employees need to know why you are applying these policies. If they feel they are part of the process, they are more likely to follow that policy. But, keep in mind, no policy is ever going to be perfect.

MR. IPSEN:

I would like to follow up with a couple of questions – one of my own, and a follow-up to Sheriff Haley’s. First, do you think it is important to make a distinction between email and other documents that might reside within an enterprise? I know, from a technical standpoint, if you are dealing with all emails, you can search email systems in a pretty straight forward process. But, if you have other documents, is that a consideration? Second, Sheriff Haley posed a very interesting question when he asked about cloud computing with respect to e-discovery. I have concerns about jurisdictional issues, specific to the cloud. If that data resides outside of the jurisdictional capabilities of the state, do you see that as an issue we should be concerned about with respect to retention and legal requirements?

MR. NELSON:

The first question relates to electronic files other than emails. The Federal Rules of Civil Procedure really provide some good guidance in this area. In terms of our obligation to produce information under the Federal Rules of Civil Procedure, those requirements go beyond email. The term “electronically stored information” defines electronic information very broadly. So, you really have to consider any type of information as part of a lawsuit or investigation. That is a big part of the reason why companies and agencies have been looking beyond email archiving solutions. Those solutions only allow email searches. You need to consider all the other content within your organization – whether emails or non-emails – to do a comprehensive search for electronic discovery purposes.

With respect to cloud computing, which seems to be the newest buzz word in technology circles today. The idea is that information is centralized, but you may be centralizing and storing that information off site using a party charged with managing that central repository of information. Centralization, theoretically, seems like a good idea because it provides centralized access to search for information. One of the biggest challenges in that area is around data security. Organizations fear moving significant amounts of data to off site locations. That is a threshold issue that needs to be overcome before a decision is made to move towards cloud computing.

As far as jurisdictional issues go, I don’t really see any unique challenges from a jurisdictional standpoint from these types of cases. That is something I may want to get back to you on, but off the top of my head, I would not anticipate any unique jurisdictional issues for an organization that is taking advantage of cloud computing.

MR. IPSEN:

Specifically, I was concerned about losing data where that data is in another country. If that data is lost, how do you prosecute?

MR. NELSON:

If we are talking about international storage, that is pretty much a unique issue. In the European Union, for example, there are unique data privacy laws. They are different from those we have in the United States. It is very difficult to collect data within the European Union because of the data privacy laws. You have to fall within a specific safe harbor exception to be able to take the data outside the four corners of the corporation.

I am not certain how that applies to the public sector, but I assume the application is similar. Rather than try to guess at a response, I’ll just say that I am not exactly sure how you would approach the situation. I think it would vary depending on the facts of the case. Thank you for the question, and I will try to get back to you with a more detailed response.

Are there other questions from the Board?

I will take this opportunity to wrap up.

From a technology standpoint, we are seeing many companies using point solutions to address the problems I have outlined depicted in this screen. Essentially, most organizations are stuck in the manual approach – approach number one. But, we are seeing a move towards an archiving approach to centralize information and to manage the policies that the organization comes up with. We are seeing that archiving technology being complemented by enterprise e-discovery solutions that allow you to search for data that might reside inside one of the archival systems. But these same systems can reside outside the archival systems as well.

There are many different companies in the marketplace that address specific aspects of this diagram. Some just provide archiving tools; others provide tools that automate the notice process. Still other companies provide tools to collect and search the data. There are other companies that specifically address the processing review and analysis of the data.

What we are seeing as a trend is that the technologies are beginning to merge together. Companies are acquiring other companies and are integrating their technologies together. The idea is to use one solution to comprehensively address this problem.

I will leave you with this in regards to next steps. These are some resources that you can rely on to learn more about this topic. We at EMC publish pretty frequently, and I am happy to direct you to some of the things that I have written and that some of my colleagues have written. There are other resources as well, such as the Sedona Conference and the EDRM Group.

I thank you for your time, and will entertain any other questions.

MR. EARL:

I would like to ask a fairly high level question. As you mentioned, and as the map you displayed shows, Nevada does not have specific e-discovery rules. California recently adopted some within the last year, generally following the pattern laid out by the Federal Rules of Civil Procedure. Could you give us a sense, a feel, for the advantages and disadvantages faced by litigants in a jurisdiction that has a specific e-discovery regime as opposed to a jurisdiction that does not have a specific e-discovery regime?

MR. NELSON:

I think the disadvantage of not having state rules is that, as an attorney, I have less certainty as to what my legal obligations are. Certainty is a big aspect of the law. As a practitioner in the state of Nevada, I would want to know what the rules are. That is going to decrease the burden on the courts, frankly, if the rules are laid out a little bit more clearly than possibly they are now. That is one of the biggest advantages that I see.

The alternative is to look to other jurisdictions for guidance and to look to what they have done and to look to case law in other jurisdictions. That is more of a wide-open process and will probably result in more arguments between parties.

MR. UFFELMAN:

To follow up on Jim's question and your color coded map, what rules does the state of Delaware have? As Nevada attempts to position itself as the Delaware of the west in terms of corporate headquarters and other things – not to say that companies would necessarily consolidate their central systems in Nevada. If we are trying to compete, then we need to compete at all levels, not just what it costs to incorporate or how quickly incorporation can take place.

MR. NELSON:

I am not familiar with the specific provisions in Delaware. I can tell you that most of the jurisdictions that have passed civil procedure rules have rules very similar to the Federal Rules of Civil Procedure. I live in California, and so can give you some examples of the differences between the federal rules and California's rules.

Generally speaking, there are some areas in litigation where certain data types that a party might be requesting are inaccessible because of undue burden or cost. A common culprit is backup tapes. It is very expensive to restore old backup tapes and to try and identify files among millions of files that might be relevant to a particular case. Under the federal rules, a party that claims that it is unduly expensive and burdensome to produce that kind of information must still identify those sources of information for the other party. The other party is then given the opportunity to bring a motion requesting an order that the information be produced even though it may be deemed inaccessible. So, the burden is really on the party that requested the data.

In California, the burden is on the party who receives the request to demonstrate why they should not have to produce the inaccessible data. I know that does not specifically address your question regarding the rules in Delaware, but it is an example of how the rules might differ slightly between jurisdictions

Those are they types of things I think you would want to consider if you indeed are going to go in that direction. A larger issue may be, from a public policy standpoint, who should have the burden of paying for e-discovery costs? The general rule is that the party receiving the discovery request is going to be tasked with bearing the expenses of identifying and producing the data because it owns the data. However, in some jurisdictions, such as California, they have taken a slightly different approach. Often times the requesting party might be responsible for paying the costs of translating some of that requested data into a usable format. So, potentially, that is going to deter litigation. It makes it a little more difficult for a smaller party to request information from a big organization. These are the kinds of policy decisions I think you will be facing as you evaluate the rules.

ATTORNEY GENERAL CORTEZ MASTO:

Mr. Nelson, thank you very much. Thank you for being here and thank you for the presentation.

Agenda Item 5 – Presentation by Gary Smith, Project Director, Robert Stewart, Senior Vice President, Customer Relationship, and Bill Olsen, Director of IT&T Infrastructure, NV Energy, Introduction to the Smart Electric Grid and Information Security Issues

AG CORTEZ MASTO:

Agenda Item 5 is a follow up from our last meeting when we talked about the smart electric grid, its technology, and particularly related information security issues. We reached out to NV Energy. They have graciously come today to give us a presentation on the smart electric grid they are working on. Today we have with us Gary Smith, the project director, Robert Stewart, the senior vice president of customer relationship, and Bill Olsen, who is the Director of IT&T Infrastructure for NV Energy. Gentlemen, thank you for coming this morning. We appreciate you being here.

MR. STEWART:

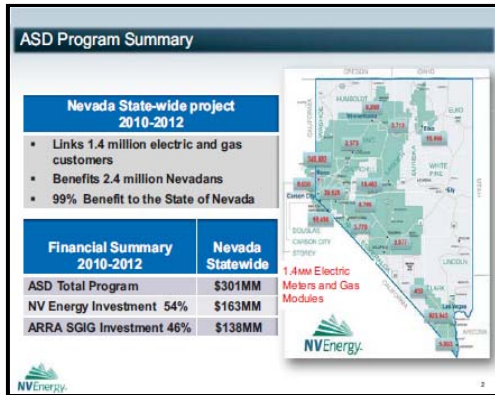
Thank you very much, madam Chair. I am Bob Stewart. I essentially have responsibility for all marketing customer service for our electric and service gas offerings, our energy efficiency programs, our customer renewables, and any other new areas we will be getting into in the future. We are going to have two parts to our presentation today. In the first part, Gary Smith, our director of smart technologies, who is the project director for what we call Advanced Service Delivery, will go through the program. He will talk about the benefits we are working to deliver to Nevada, and he will talk about some of the steps we are taking to avoid some of the missteps that have been going on across the country with respect to implementation of this collection of technologies that make this possible.

Bill Olsen is our director of information technology and telecom infrastructure. He will be talking more specifically about our plan to protect our communications infrastructure that is a part of this project and about protecting customer information. And, by the way, Bill was the leader of our

records retention cross-functional team. He enjoyed the earlier presentation. With that, I will turn it over to Gary.

MR. SMITH:

Madam Chair and Board members, thank you for your time today. I would like to introduce you to Advanced Service Delivery, which is the smart grid project for Nevada.



This is a project that will take place over 2010 through 2012. NV Energy, about a year ago, spent quite a bit of time envisioning what the smart grid ought to look like for Nevada. We are not on the bleeding edge in Nevada. This is something we have been watching the nation as it has unfolded – particularly in California and Texas. They have been rolling out the smart grid for several years. It is right at the heart of full deployment in those states. We have taken our time as a utility company in Nevada before leaping into this initiative.

This is a customer focused initiative. We look at the smart grid from the customer backwards. It does encompass all of Nevada. It is a state wide program. It is 1.4 million electric and gas customers who are covered under the program. It impacts about 2.4 million Nevadans. It is about 99% of the total territory. NV Energy serves 55,000 square miles in Nevada. We are one of the first companies to take on a state wide program, which we are pretty fortunate to be able to do.

The cost of the program, for this foundational infrastructure, is \$300 million. However, we did receive a grant opportunity from the Department of Energy (DOE) under the Smart Grid Investment Grant for \$138 million of the investment.

If you take a look at this grant opportunity, NV Energy went into a competitive environment throughout the nation to compete for this particular grant opportunity. We were awarded in October of this year a grant. This particular grant is about 4 times more award than any other state per customer. We are pretty proud of the competitive nature of receiving this reward for the grant opportunity.



It does not come without hooks. The Department of Energy, in working with them, we went through a very aggressive negotiation process to get the right terms and conditions for this grant opportunity. Then we filed that opportunity with the state's Public Utility Commission (PUC). Back in February, we filed with the PUCN. That will go through hearings, and hopefully, we will have a decision by August of this year.

However, since this is only a three-year opportunity, our window to perform is such that we have started substantial work on the project. We are minimizing our expenses for large procurements, but the planning and integration work has begun.

The Department of Energy required four plans that we had to submit to it. We have submitted three of the four plans per their schedule. The first is the project execution plan. This is normal

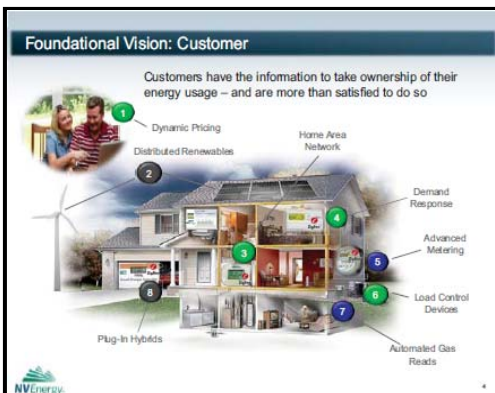
project management activity, cost schedule, both cost and scheduled budgets, that kind of thing. When and what we are going to do on the particular plan. Who does what by when?

The second plan is a cyber security plan. This is what Bill Olsen is here to talk to you about today. It is about how we ensure that what we are building is secure. We have some diagrams to show you how we have learned from other states that have gone before us – how to ensure we have a secure system.

There is a metrics and benefits reporting plan. This deals with how we add value and ensure we are getting the value out of this program as we are installing the basic infrastructure for Nevada.

Then there is a consumer behavior plan. We are kind of unique. Nevada is one of nine utilities throughout the nation that was awarded a portion of their grant to do a consumer behavior study. This is really to test rate options with customers and to see which types of rates the customers really would adopt in a full deployment. So, we have a plan to do a small study around rate options for customers.

We did ultimately sign a definitive agreement. We have signed. We were the first investor-owned utility to sign the formal agreement with DOE. We did that on March 12th of this year.



So, what does this thing look like? We have envisioned the smart grid for Nevada, and we really started with the home or business and worked backwards. Most smart grids start out with the technical aspects of the grid. We started with the customer-facing portion of the project. We envisioned what the future home would look like.

Actually, the home that is up on the board now is becoming reality across the nation, particularly with this stimulus opportunity, there is about 18 million new meters going in during the next 3 years. That is about 30 million meters total. A large portion of the United States is now starting to receive pieces of this technology.

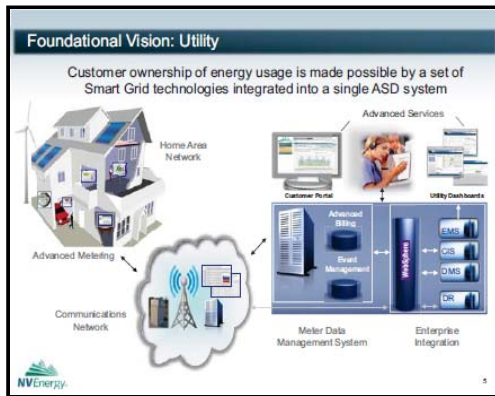
So, what does it do? The smart grid really enables pricing options for customers. I say pricing "options" because not all customers are the same. Not all user habits are the same. So, we have to have options for customers.

It enables distributed renewables. You are starting to see solar panels on homes. You are starting to see some wind generation at the home location. It enables that bidirectional metering, so customers can not only consume generated energy on their own, but they can also sell it back to the grid eventually. This technology starts to allow for that bidirectional metering.

It supplies the home area network. This is an area of the smart grid that is evolving a lot. You are seeing Google and Microsoft and others getting into part of the environment. It is really trying to help customers take ownership of their energy usage. In order to do that, they have to have the information.

The backbone of this particular smart grid allows for 15-minute interval data to be recorded for customers so that they can have the information in front of them to make decisions. I will show you a slide in a minute to show how that will really work. It allows for dynamic pricing programs. We have large peaks during the summer time. Customers have the opportunity to reduce their usage during those times at discounted rates. And, in some cases, get rebates for usage.

Demand response really provides opportunities when we get into peak requirements. It allows us to reduce our generation requirements, purchasing of power plants actually. So, there are opportunities there. Eventually, it gets into the plug-in hybrids. Electrical vehicles are coming. In 2011, you will start to see these come off the manufacturing floors. This infrastructure starts to help customers use their energy during off-peak hours, for example, charging your vehicle at the right time at discounted rates. So, there is a lot of overall opportunity home or business. As you see in this slide, it is starting to become reality throughout the United States.



This is the backbone infrastructure. I call this the cartoon diagram. I have the IT guy next to me, and you could fill the walls with information about how these systems come together in one integrated unit. This is a basic diagram of the foundational infrastructure of the smart grid for Nevada. It does have a lot of back office systems that get revamped or replaced. There is a key system called "meter data management" that is installed. To give you an analogy, we collect about 17 million meter reads a month from our customers today. In the future state of this program, we will be collecting 4.3 billion reads a month on this system. So, we are collecting

a lot more information to help facilitate porting that information back out to customers so they can make better decisions on their energy usage.

The next piece of infrastructure is the communications network. We are kind of unique. There are several types of networks that can be put in to talk to the smart meter. There is a mesh-type network where meters talk to meters that collect and build a network. We looked at this technology and decided not to go there.

What we ended up going with is more of a tower-based technology where we have a higher bandwidth. Why is a higher bandwidth important? We are using the same technology not only to serve customer metering, but we are also using it for distribution automation. We are using it for renewables. We are able to use and double use that network for other applications. This is very, very helpful.

The particular communications we are using is contained within our existing substations, so it is behind closed substation walls. The average height of these towers is about 25 feet, so, it is not intrusive. There are 144 of these towers that are placed throughout the state of Nevada. It is broadband, basically, that allows us to communicate not only to our critical assets but also to each and every home in the state of Nevada.

The metering we are installing is built to NIST (National Institute of Standards and Technology) standards. The metering itself has two communications protocols that can be used – both an IP protocol and a protocol called ZigBee¹, a leading protocol that allows the meter to talk to devices within the home – whether that is an in-home display, thermostat, or, eventually, a washing machine or an electric vehicle. The same types of protocols are becoming standard. We have leveraged to be able to use IP or ZigBee in future applications. So, we have built and designed a system that is upgradeable, scalable, secure, and it is reliable going into the future.

A big part of this is talking about customer benefits. We look at these benefits in three primary categories. There are customer benefits, operational benefits, and then there is demand

¹ ZigBee is a specification for a suite of high level communication protocols using small, low-powered digital radios based on the IEEE 802.15.4-2003 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio. Wikipedia, March 30, 2010.

response – or programs that can generate benefits as well. I am going to talk to you a little bit about customer benefits before we jump into cyber security. I also want to talk about rate options and use of thresholds. I will show you that on the next slide.

Customer and Operational Benefits

- Customer Ownership of their energy use
 - Technology to help customers manage their energy usage
 - Rate options
 - Usage alerts and thresholds
- Operational Benefits lead to future rate reduction
 - Reduction in over 1-million annual truck rolls
 - Reduction in 17-million monthly manual meter reads each year
 - Revenue Protection (energy theft)
- Expanded Demand Response programs avoid future generation investment
 - Secure, reliable, and expandable infrastructure for current and future Demand Response programs
 - Additional 145MW by end of 2012

Jumping to operational benefits, just to put this in perspective, there are about \$35 million in operational benefits by deploying this technology over the next 3 years. That is an annual benefit. It is things like this. We have a million truck rolls that we do a year just to turn customers off and on. These are customer move-in and move-outs; that is a million truck rolls a year. We drive about 2 million miles we drive as a utility. There is a lot of opportunity if you can automate that process. We also go to every single household throughout that map of the state of Nevada. We do that monthly right now. By automating that, there are a lot of operational opportunities.

When we talk about revenue protection or thefts, today we rely on our meter readers to detect whether that meter has been tampered with or not. That is really our only first line of defense around tampering. The new smart meters have automatic tamper detection. We also get to go out and touch every single meter in our service territory to ensure integrity and find these types of tampering. So there are lots of opportunities for savings around future revenue protection.

Ultimately there is demand response – being able to offer programs so that we reduce our peak time – the time we generate the most costs as a generating facility. As we grow that, we can offset purchasing future power plants. So, there is a big opportunity there. What does this do for us? We already have a successful program around demand response, but it is on an old paging technology. This allows us to really bring it behind a secure back end. It makes it reliable and expandable for the future. Through our DOE grant, we will grow demand response by an additional 145 megawatts by 2012.

Customer Benefit

Self Serve

Energy	Self Serve
Bill To Now	\$103
Usage To Now	989kwh
Average Daily Use	\$4.85
Billing Cycle	23Days
Projected Bill	\$110 to \$165

Customer Channels

- WEB
- HAN
- IVR
- Mobile

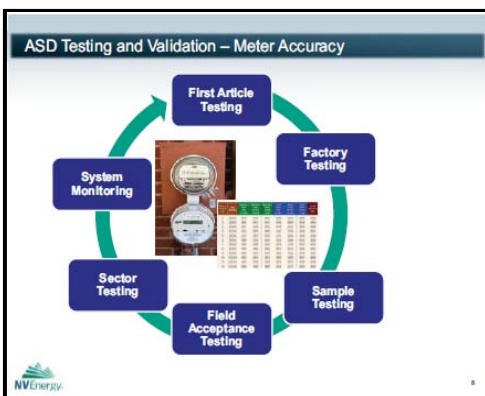
Take a look at this slide. This is really a lot of what the customer can see from the introduction of the smart grid. Again, I introduce this as a foundation. Picture going to the gas station today. There is no sign up indicating the price of gas. You go fill your tank, and there are no gallons tabulated when you fill your tank. You can not understand or see the amount of gas you are putting in your tank. At the end of the day, when you fill up your tank, you don't know how much it has cost or how much it will cost until you get your monthly bill from the gas station. That is how it really is when you look at the utility today. You do not have any insight into what the energy is costing you receive a utility bill, and that is

at the end of the 30-day period. What this technology starts to do, as the foundation of a customer benefit perspective, is that it starts to put up the gas sign. It says, "Here is how much your energy is costing you, whenever you want to see that." Here is the analogy from gallons to kWh [kilowatt hours]. It is really the same analogy. You have a miles per gallon or a kWh to show how much you are using. How much are you using today? What is my average daily use? We really can not tell you today. You see that only at the end of every month. How many days are left until your bill is final? Things like this are things customers are asking for. In the focus groups we have done, the number one thing we want to see is bill to now – what is the energy costing so

that I can budget for it, and so that I can better react to it. What is my projected bill? If I am using at this rate, how much is it going to cost me at the end of the month?

We think that needs to be put on multiple channels. It can not just be on the web site. Not all people have the web. Our studies say that about 67% of the people have web site capabilities. Not all folks are going to have an in-home display. Some folks are going to have a phone, and they can always call in our IVR system and we can port this system to the IVR. But, as technology improves, immediately, we want them to have that capability on the web. We also want them to have capability on the web to find ways to save. That is an important aspect not only of showing the usage, but starting to self-manage energy use. Ultimately, you will be getting information on your smart phone – the phone itself. We can do message alerts: “My bill as of today has reached a threshold of \$100.” Some people would like to know that if we can port this technology to them.

So, there are lots of first-day customer benefits we are able to organize and get out on the front end of this project. I just spent quite a bit of time with San Diego, which is going through a meter deployment now. They have about 600,000 meters in the ground. I asked the project director what was the number 1 thing he would do differently in San Diego if he had it to do all over again. They said they would get this information out – day one – in front of their customers. To date, most of the California utilities do not have this type of information you see on this chart up in front of their customers. They are moving forward on their smart grid initiative, but their customers are still blind around it. That is why you are starting to see a lot of the outcry from California. They just do not see the data.



The last piece I want to share with you is this. You have seen in Texas and in California that there is a lot of outcry around the accuracy of the meters. Meters are pretty darn accurate. They have been made for hundreds of years. We have gone from a mechanical meter to an electronic meter, but we have to make sure, one for one, that these meters are tested and accurate, starting with the factory, starting with the first article testing of how they are configured, ensuring they are configured in the same way as the meter that is on the home today. The first step in this process is to ensure the factory is configuring the meters to our specifications. We are working with the University of Nevada at Reno to actually do some testing of the meters we have

selected. They can go out and look at different vintages of these meters – whether it is a one-year old meter on the home, a fifteen-year old meter, or a thirty-year old meter. We want them to help us as a third party to test. We are going to use their engineering resource to help us test the differences between the old meter and the new meter. That starts with the baseline for us.

Getting back to the factory, we do factory testing. We do our own testing at NV Energy. We then go through a testing process in the field where we put out about 10,000 meters, and we still manually read those meters with our meter readers to ensure we are getting the accuracy so we can build customer trust that the meters are doing what then need to be doing. Then we do it at a larger volume. We do volume testing. Then we do periodic testing to ensure we have meter accuracy.

That is the first step in the smart grid. We believe you have to build customer trust. If we can get the trust in the metering, the rest of the benefits will flow.

In the center of this little diagram is a little picture from Texas. Texas actually had a lot of public outcry about accuracy of meters. Some of the meters that are 30 years old, run a little slower.

They have run down over time. What happens, if you do not know that, you put the new meter on and it is accurate. This does not mean the old meter was bad, it just means that it was tired. They are mechanical, so they do break down.

Texas has done some side-by-side comparisons. They put an old meter on the home and a new meter. They are now measuring the difference between the two. You do this on a kind of random sampling of different meter types. But then, it does bring in good information to be able to help customers understand the differences.

That is a little bit about NV Energy's start of the program. What I would like to do is have Bill Olsen talk to you a little bit about cyber security. That is really what you wanted to hear today.

MR. OLSEN:

When we started talking about this whole project, we understood right up front that security and privacy were major impacts to both the project and to the way we were going to implement our solution. We wanted to make sure we were protecting our customers and that we were protecting the corporation so that we could continue to serve. Security was one of the key design elements as we built out the system – to make sure this was a major design thing right up front.



We put a number of items in place to make sure that we are securing the network that we are building along with this advanced service delivery project.

First of all, the meters we are selecting handle encryption inside the AMI, or the metering network, themselves. We decided that was not adequate in and of itself because it is something we do not have control of. It is provided by the metering vendor. So, on top of that, we are putting in our own encryption technology that sits on top of that. It encrypts the data as it passes through the system. So, we have built-in message encryption to protect the privacy of the customers.

Along with that encryption, we are able to authenticate that the meter is the meter we expect we are talking to and that any signals that the company sends to the meter come from the company and not from a third party. So, we have certificates that handle that authentication on our behalf. We have created virtual private networks (VPNs) to isolate the various components of the network we are building to, again, make sure that in the event there is a compromise of some kind, it is compartmentalized and not spread to the company and not spread across the network itself to other meters. That is the way it is designed.

Gary mentioned that there is a mesh network. That was a possibility. We did not select that, and instead are going for a more traditional star or tower-based network. That does not allow transmission from meter to meter. So, where, in other places, there have been concerns that if you compromise a meter, you can then spread things to other meters. We do not have that as a possibility in our design, right up front, because of the technology we have selected.

We are not just looking at technology, however. We are also looking at some of the processes that are in place. We have put dedicated people on the project right from the start. We have a dedicated security expert from an IT/cyber perspective, who is on the project full time. He is spending all of his time with education, design, and working with the vendors to make sure we are building a secure and safe network to supply this technology.

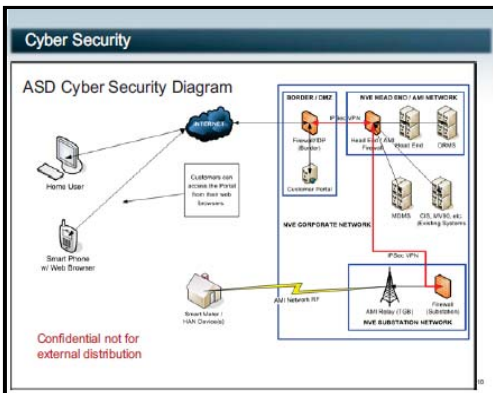
As part of that, we are adding our own firewalls into the network. That allows us to respond separate from what the meters themselves or the network does. There is no such thing as perfect

security. All of you know that based on your professions. The only way we can make it perfectly secure, I guess, is to turn it all off. Of course, that makes it non-functional and is not really the desired goal. Knowing that there is the potential for breach, we are building these firewalls in that allow us to respond independent of the network or the meters themselves.

You have probably heard of zero day attacks. When a zero day attack occurs with a virus or something that infects a desktop, you then have to wait for the anti-virus vendors to catch up. That is day one or day two or later when they catch up to provide protections. The same thing can occur with a meter or other things. If there is an attack that is successful, we now have to wait for the meter vendor to catch up, and we have the 1.4 million meters installed. Instead we have put firewalls in that allow us to isolate and respond to those independent of the metering vendor or others to occur.

We have dedicated security staff inside of IT beyond the ones assigned to the project. We have technologies in place that allow us capture the security logs from all devices across the network, consolidate them so that we can start to see through aggregation when a major event is occurring. We are doing that security event monitoring, and have those technologies in place. We are going to expand those technologies associated with this network. We are installing intrusion detection devices that allow us to identify through both behavior and signature-based tracking when things are not working right within the network.

We are building security incident handling and response processes in place. So that when we have an event occur, we have predefined exactly how we are going to respond to that to make sure that we are not having to go through the process of finding people or identifying who is responsible and how we are going to react.



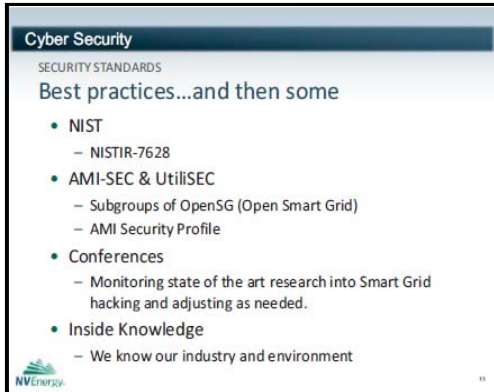
This is a logical diagram of the network we are building. If you look at the blue lines, they identify the individual networks and where they are separated and isolated. You can see the firewalls that separate them from one another. We do isolate any potential problem that might occur.

To follow the network traffic from the smart meter device on the home, we would do the read using the TGB or AMI relay tower. That would then go through a firewall and create an encrypted VPN, which would then talk to the managing component or head end of the AMI network that will be at our corporate offices. That information then passes into our

corporate network, again passing through the firewall, to be stored in the MDMS system that Gary mentioned earlier, where all the meter data – the 4.5 billion reads that occur in a month – is stored. It will then interface, passing through the firewall, into our customer service system or to our major account billing system, which is the CIS, MV90. For our customers to be able to access the data, Gary showed you the display. For customers to be able to access that, they will actually use their own separate connections, so it will not use the corporate AMI network. They will use their own internet, their own phone, their own smart device, however they are accessing it through the internet. They will come through our standard corporate firewalls that are in place today where we offer our customer services today. Similar architecture will remain in place in order for them to get to that customer portal to see their data.

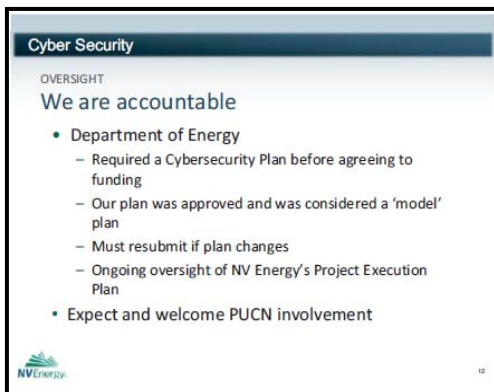
We are implementing best practices in security standards across the board. The NISTIR 7628, which is the national standards that are being developed by NIST. I believe NERC [North American Electrical Reliability Corporation] and FERC [Federal Energy Regulatory Commission] are giving input into those. I believe at the last meeting there was some discussion about the Open Smart Grid. Open Smart Grid is kind of an over-arching body that is defining APIs or

Application Program Interfaces. There are two subgroups that are part of that, the AMI Sec and the UTIL Sec, that are actually working on the security components associated with that. The vendors we have selected participate in those groups, and we are looking at all of the standards they are producing to make sure we are in compliance in implementing the technologies they are identifying as important as part of that.



We regularly attend conferences and other industry educational outlets for us to make sure we are keeping up with the technology as it is developing. I believe at the last meeting there was a presentation where there was discussion from a presentation given at Black Hat in 2009. We had people in the audience at that session. So, some of our security people were there. They were aware of the information, and have done additional research since then to identify whether it applies to us or not and what kind of measures we need to take. We are making sure we are covering all of those kinds of events and are operating inside the industry where not everything is shared with the public. We are

getting that inside information that not everybody is able to obtain to make sure we are ahead of the game and that security is definitely a driving force for us.



Finally, we are not doing this in a vacuum. Gary mentioned that the DOE required us to submit a cyber security plan as part of our application. We submitted that. In fact, the DOE security experts who looked at it identified our plan as the best they had seen. They considered it a model plan that they are expecting other utilities and other people who are applying for the grant to follow. Obviously, they have to customize it for their own individual environment, but our plan was identified and it identified security right up front as built in and not as an after thought.

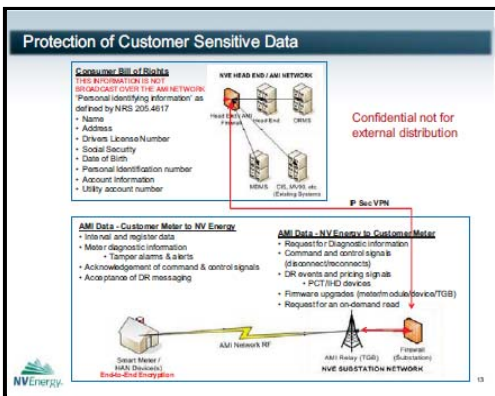
If we change the way we implement it, we are required by DOE to resubmit the plan and to notify them of changes. As part of the ARRA grant we are receiving, we have regular oversight from the DOE to make sure we are complying with those requirements.

Finally, as Gary mentioned, we have submitted to the PUCN as part of our integrated resource plan the ASD project. We both expect and welcome their involvement when it comes to security and requirements around maintaining privacy and protecting both the consumer and the corporation.

MR. SMITH:

We have one more diagram here for you and it has to do with customer sensitive data. There is a lot of talk in industry, "Will the utility be able to monitor my toaster?" – things of that sort. That is just not true.

There are requirements for customer sensitive data. We operate under this NRS 205 or 617 around customer sensitive data where we have to protect our customers' data. There are protocols when that is breached. But there is a list here of types of data that is sensitive, that the company determines is sensitive. As Bill talked about, that is behind the firewall. That is something that is fully protected.



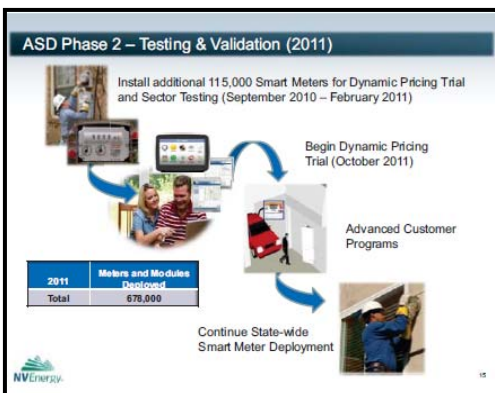
What we are actually doing on this network though is transferring usage in aggregate. We do not know what really happens within the home. What we are interested in is what the 15-minute aggregate piece of that load and porting that back so that we can provide that back to the customer in an environment that they will understand. There are also some protocols, some messaging, that we do to ensure, for example, that if there is an outage on the home, you are no longer going to have to call us and say, "NV Energy, my power is out." We are going to have detection that says, "Hey, we just got a last gasp from that meter, and it died. What happened?" So, we will have automatic notification. There is

messaging coming to and from the home. As well as we can move customers in and out of homes through a disconnect switch, that, then, is protected as well.

What we have here is a diagram that says here is the type of information that is flowing on the AMI network. Here is the type of information that does not transfer on the network itself.



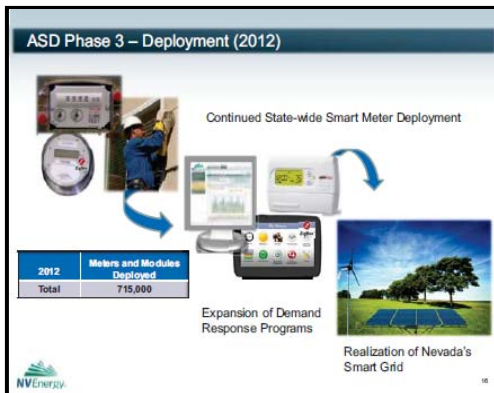
I would like to follow up with three quick slides. I know we are running out of time here. In your packets is a very high level implementation plan for the project. Again, we filed this program overall, both north and south, with the Public Utilities Commission. In February, we filed in the south. Just this last week, we filed the amendments for the IRP in the north. We did reach agreement with the DOE just a couple of weeks ago, the final agreement. So, those are now submitted to the Public Utilities Commissions. We are in final contract negotiations with our vendors. We did not want to enter into those contracts until we had a final agreement and understood the rules with the Department of Energy. We are entering into these agreements now. However, all of those agreements have "out" clauses if we do not get PUC approval.



We started back in October with our vendors designing this program, back in October of 2009. We are coming out of the planning phase of the project now. We are starting to go into the design and build portion of the project, which really encompasses the back office systems development work that will take place. However, by August of this year, we will be able to put out the first 10,000 meters. Those meters, the first 10,000, will be for field acceptance testing. We are already doing first article testing back in the plants. We are doing testing on our own. We are having UNR help us with some testing. We will put about 10,000 into the field and start to test the communications network.

We will not turn on the billing portion of that network until we are comfortable that we have accuracy, total accuracy, of these meters. We will have 10,000 meters out in the first part of August. We will continue to deploy, but we will not exceed 50,000 meters in the field until field acceptance testing has passed.

Once that takes place, we are to the end of 2010. As we start 2011, we are going to put out about another 125,000 meters in southern Nevada. This is the pilot area that we will do our consumer behavior plan with these customers. There are about 125,000 customers that are in a pilot area, and about six to eight thousand of those customers will ultimately opt in to a dynamic pricing trial. We will allow them to select from a couple of different types of advanced rates – critical peak pricing and an enhanced TOU rate. That is no longer mandatory. Originally, DOE was trying to get customers to mandatorily go onto, or participate, in these programs. They backed off of that. We think that is a good idea. We want customers to have choice on these options. We will be able to monitor these customers over a two-year period – those that are on these new types of rates. That information will help us into the future to recommend rate programs for our customers. Again, that pilot program will start in October of 2011.



The first meters that will hit the north, the northern part of our service territory, will be in April and May of 2011. We will finish deployment of all meters by the end of December 2012.

Once these meters are out, we can then expand into other types of programs for our customers. These include more enhanced demand response types of programs. We can expand to programs on distribution automation, where we can get more benefits from understanding how our network is working in real time. Right now, we receive an outage and we are rolling trucks. We could put in sensors to be able to say, this substation is having a problem, let's go take a look and see what is going

on. We could make adjustments from the back office on that electrical equipment, which is back to the operational savings.

That concludes our presentation. We will take questions. Thank you.

SENATOR WIENER:

Mine will not be a technical question. You mentioned several times the next steps with the Public Utilities Commission regarding your roll out. Let us say that they do not buy into your plan. You mentioned early on that there is a three-year window on the funding. So, if the PUC does not buy into what you are presenting in April, or it buys in differently, what then happens?

MR. SMITH:

The first step in that is the contract we have negotiated with the Department of Energy. It has clauses regarding what would happen if the utilities commission does not give approval. Basically, it is a back-out provision. The \$138 million is then handed back to the Department of Energy. We are able to walk away from that contract. The dollars, however, that we spend between now and that time period do not have to be paid back to the DOE. So, we can basically part ways. DOE would then take that \$138 million and offer it up to another state.

MR. IPSEN:

I have a couple of questions, actually. First of all, I want to applaud your stated commitment to security and its practices. I do have a couple of questions. With proper controls, can we get a copy of the cyber security plan that you have registered with the Department of Energy?

MR. SMITH:

Yes, we can.

MR. IPSEN:

Great. Also, with respect to the smart grid, can you speak to how the smart grid interfaces with the not-so-smart grid? I know there are different security controls associated with each of those.

MR. OLSEN:

I am not so sure what you mean by "not-so-smart grid". I assume you are talking about the current distribution system.

MR. IPSEN:

That is correct.

MR. OLSEN:

Our advanced service delivery project is not currently including the distribution network. The distribution currently runs through an EMS [Energy Management System] system using SCADA [Supervisory Control and Data Acquisition]. That will continue at the current time. We are building in the network to be able to do that in the future, but that is not a part of this three-year plan.

MR. IPSEN:

I just have one other quick question. You mentioned controls and a security plan, how about validation of those controls? I would assume you are doing something to validate that those controls are having the intended effect you are proposing that they have. Can you speak to that?

MR. OLSEN:

We do. The DOE is acting as some oversight for that. The way we are architected within the IT department is that my group handles the infrastructure and the deployment. The security group handles the policy and the oversight of my group to make sure we are following those. So, with the security group, we have created separation of duties. They are not the ones doing the implementation. They provide the oversight, structure, and the policy. We implement. They watch over our shoulders to make sure we are following their rules.

MR. SMITH:

I have another comment to that. When you get on the technology side, we talked a lot about accuracy of the metering itself. There are similar plans when you get into the back office with the systems, the systems testing and ensuring appropriate controls. Again, you are going in and doing a little bit of surgery on our billing system. Any time we touch our billing system, we are pretty sensitive to that. Customers are sensitive to that. So, we are ensuring that is thoroughly tested to the point where we have kind of carved the communications and the metering as a stand alone infrastructure. What will happen, once we are comfortable in the testing, we can turn on the billing component of it. So, we can go out and test communications, go through field acceptance testing; we can test the metering, but we do not have to turn on the billing component – the interval reads that we get. We are still manually reading those meters until we ensure that the controls are in place to turn it on.

Again, these are lessons learned from California and Texas, where it is real sexy to go throw meters out in the field. Everybody feels good, but you have to have these back office systems ready to accept them.

MR. OLSEN:

We have a very robust ITIL-based [Information Technology Infrastructure Library] change management system in place. It manages all of our application changes across the board. We are not in any way weakening those. In fact, we are strengthening those specific to this project along with the comprehensive STLC [System Testing Life Cycle] that surrounds the IT systems associated with that.

MR. IPSEN:

Great. Actually, I have one follow up question, if I might. I noticed on your slide you mentioned that PII is not broadcast over the network. Is it unicast, or uni-directionally sent across the network?

MR. OLSEN:

No, it is not. The information we are receiving would be command and control. It would be sent out from the utility. We are receiving back usage data from the meter. So, we are not transmitting name, address, driver's license, or anything like that across that network.

SENATOR WIENER:

Again, not very technical, and Jim can follow up. We have done co-presentations before. We have one of the country's toughest encryption standards in statute. It took a lot of work to get that through. Do we have an assurance – and I heard "encryption" a lot in your presentation – that we meet or surpass these standards? We went to great lengths to establish this in statute, and we had a lot of people challenging us along the way, very large organizations who did not agree with us. Do we have assurances that we meet or surpass the Nevada standard for encryption?

MR. OLSEN:

Yes, we are actually doing double encryption on these. The meter itself encrypts, and then our VPN [Virtual Private Network] encrypts over the top of that. So, yes.

SENATOR WIENER:

And that is the vendor encryption you mentioned earlier?

MR. OLSEN:

The vendor encryption is at the meter. The firewalls are handling the VPN encryption. We control that independently with our own certificates that we are using today to meet the Nevada standard.

SENATOR WIENER:

At what point, if there is a breach, would you know?

MR. OLSEN:

It is hard to predict the future, so I could not tell you. But we do have active logs. We are capturing logs from all of our security devices. We have active monitoring of all of that. So, we should know very early with that kind of an occurrence. Until you describe exactly what kind of an attack, I really could not ...

SENATOR WIENER:

But, given no specifics, you would determine what kind of an attack should one happen and how to address it and get it under control?

MR. OLSEN:

Yes. The logs should definitely show that kind of information. The active monitoring should capture that very early. Again, we are using intrusion detection that is both signature based and behavior based. So, when you see the behavior changing, even before signatures are developed, we are able to capture that information.

SENATOR WIENER:

And you would know the scope of the breach – the extent and the details of the breach?

MR. OLSEN:

That would take some work. Again, it depends on the type of event. But we should be able to develop that kind of information, obviously doing the necessary research from a cyber perspective.

SENATOR WIENER:

I am sure Mr. Ipsen would like to see that as well.

MR. SMITH:

I have a follow on to that. The way this network is built out, at each substation location – there are 144 of these sites – and each one of these is firewalled as well. Each site only handles about 10,000 customers. Again, we are isolating. If we had to go shut things down on an intrusion, you could isolate down to either the meter level or to the substation level.

MR. OLSEN:

To each individual tower.

MR. EARL:

First, let me congratulate NV Energy on submitting a cyber security plan that was so well received by the Department of Energy as part of the grant process. You both mentioned, and I noticed that one of your slides includes a reference to the NIST Interagency Report 7628. Board members have extracts from that particular document. That forms the basis of my question.

The NIST document points out that the envisioned smart grid “will be a ripe target for malicious, well motivated, and well funded adversaries.” It also points out that the electric smart grid must be build future proof. “It needs to be able to adapt to changing needs in terms of scale and functionality, and at the same time, needs to be built to tolerate and survive malicious attacks of the future, which we can not even think of at this time.”

Now, recognizing that the NIST recommendations and standards will change over time, and recognizing that you are now at the stage where you are in the final process of contracting with vendors, could you give us an idea of what NV Energy’s strategic plan is with regards to distributing the retrofit security costs between ratepayers and the suppliers and vendors you are now negotiating with?

MR. SMITH:

Real quick on that. The communications network, as well as the metering vendor – The first part of this selection process was partnering with vendors that are the leaders in the market. We wanted to pick folks that are going to be there a while. That was the first thing.

The second thing is we did pick standards that are on the front end and are now being adopted by NIST. We have people that are very involved on the NIST front. They are seeing where that puck is going. So, these standards that are being formulated – we are on the forefront of that. To the point that the metering we are installing allows for firmware upgrades. This means we can send in upgrades to the meter as technology and standards change. So, you have a gut of a meter there, and we can actually communicate different protocols, as standards do change, to that particular meter.

I think Bill can talk about the back office piece of this as well.

MR. OLSEN:

Right. We have built the network to allow for firmware upgrades so we can change the security profile of the network itself. We are also adding in the firewalls to allow us to independently change the security profile both on the front end and on the back end. As to the strategy for distributing the cost, I assume it would work the same way that we do currently – whether it be an operational expense or a capital expense. We would follow our normal practice.

AG CORTEZ MASTO:

Are there any additional questions? Alright, thank you very much, gentlemen. It was an informative presentation. We appreciate you taking the time to be here.

MR. OLSEN:

Just a quick aside, I worked on the e-discovery for our company for a year. I would be happy to share our guidelines with you, along with training videos we did for the company, if you are interested in that.

AG CORTEZ MASTO:

We are very interested. We appreciate the offer. Thank you.

My intention is to get everybody out of here by noon. We have five minutes left by my clock. What I want to do is this. Anne-Marie Cuneo is the Director of Regulatory Operations for the PUC. My understanding is that she is in Carson City. There she is. She has graciously come to listen as well as to answer any questions we might have regarding the PUC's regulatory oversight of this issue. Anne-Marie, thank you very much for being here.

Agenda Item 6 – Questions and Answer Opportunity with Anne-Marie Cuneo, Director of Regulatory Operations, Public Utilities Commission (PUC) of Nevada, regarding the role and decision schedule of the PUC in Smart Electric Grid Implementation

MS. CUNEO:

Thank you very much. My name is Anne-Marie Cuneo. I have with me Paul McGuire. He is the manager of our Engineering Division. Let me give you a quick bit of background on the Public Utility Commission's role in this process.

The Public Utility Commission acts as a quasi-judicial agency in this regard. The three commissioners, since this case is in front of them right now, are not allowed to comment on the subject. However, I am the Director of Regulatory Operations staff. This staff is a separate, independent entity, which happens to be charged with the same goal as the commission, which is to balance the interests of the rate payers and the shareholders. In furtherance of that goal, the Regulatory Operations staff is made up of divisions of economists, accountants, and engineers. We have our own staff counsel as well. We look through all the filings that are made to the Commission and provide our recommendations to the Commission as the State's expert witnesses.

The integrated resource plan was filed by the Nevada power company in early February. It included a component you are familiar with as the smart grid or AMR. Testimony from staff and other interveners, such as Bureau of Consumer Protection and any other interested party, will be due the last week of April.

The Commission will be having a hearing on this matter at the end of May. We are under some very tight statutory deadlines and we will have a decision in this matter by August 3rd. We have 180 days to process the case.

The analysis that the staff will present and the Commission will view – we look at everything. We look at the relative cost/benefits of the project. We look at the future savings that utilities estimate to make sure the costs and benefits are not only reasonable and accurate, but are in the best long-term interests of the public.

I will cut this short to make sure we do not go over time. We are available for any questions you may have.

AG CORTEZ MASTO:

Are there any questions? Hearing none, thank you again for being here. We appreciate it.

Agenda Item 7 – Board Comments

AG CORTEZ MASTO:

Moving onto agenda item 7, are there any comments from the Board? Alright.

Agenda Item 8 – title

AG CORTEZ MASTO:

Are there any public comments? Are there any comments from members of the public here in Las Vegas who would like to address the Board? Seeing none, are there any members of the public in northern Nevada who would like to address the Board.

MR. EARL:

There are a number of members of the public here, but none of them are stepping up.

Agenda Item 9 – title

AG CORTEZ MASTO:

Alright. Agenda item 9 is scheduling the future meetings. I suggest we continue to schedule our meetings in the same manner we have in the past with the help of Mr. Earl.

Agenda Item 10 – Adjournment

AG CORTEZ MASTO:

Moving onto agenda item 10, our adjournment, we are adjourned. Thank you very much.

Time: 11:59 AM

Respectfully submitted,

James D. Earl

Approved by the Board at its subsequent meeting on July 22, 2010.

Minutes of the Technological Crime Advisory Board

July 22, 2010

The Technological Crime Advisory Board was called to order at 10:00 AM on Thursday, July 22, 2010. Attorney General Catherine Cortez Masto, Chair, presided in Room 4401 of the Grant Sawyer Building, Las Vegas, Nevada and via videoconference in Room 3137 of the Legislative Building, Carson City, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Nevada Attorney General Catherine Cortez Masto (Advisory Board Chair)
Nevada State Senator Valerie Wiener (Advisory Board Vice-Chair)
Daniel Bogdan, U.S. Attorney, Department of Justice (DOJ)
Captain Tom Hawkins, Las Vegas Metropolitan Police Department (LVMPD), *meeting designee for Sheriff Doug Gillespie, LVMPD*
Lieutenant Jerry Baldrige, Washoe County Sheriff's Office (WCSO), *meeting designee for Sheriff Mike Haley, WCSO*
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 in Charge Rob Savage, U.S. Secret Service (USSS), *meeting designee for Special Agent in Charge Richard Shields, USSS*

ADVISORY BOARD MEMBERS ABSENT:

Tray Abney, Reno/Sparks Chamber of Commerce
Special Agent in Charge Kevin Favreau, Federal Bureau of Investigation (FBI)
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association
Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE)

TASK FORCE MEMBERS PRESENT:

None

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director

OTHERS PRESENT:

James R. Elste, Symantec
Bob Cooper, Bureau of Consumer Protection
Dan Jacobsen, Bureau of Consumer Protection
Dennis Carry, WCSO
Suzie Block, Attorney General's Office

Kristen Hansen, Attorney General's Office
Lydia Sittman, Attorney General's Office
Ira Victor, InfraGard
Kristin Erickson, Nevada District Attorney's Association
Teri Mark, Nevada State Library and Archives

Agenda Item 1 – Call to Order – Verification of Quorum

AG CORTEZ MASTO:

The meeting is called to order on July 22, 2010 at 10:00 AM. The first item on the agenda is the call to order and verification of a quorum. Mr. Earl, please call the roll.

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

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

AG CORTEZ MASTO:

Before moving to the next item of business, first let me say that we are joined by U.S. Attorney Dan Bogden. Welcome back, Dan. It is great to have you. Thank you very much for joining us today.

Item 2 is the discussion and approval of minutes from the March Board meeting. If there are any edits or comments, please make them now. Otherwise, I will entertain a motion.

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

The motion to approve the minutes was approved unanimously.

Agenda Item 3 – Reports regarding Task Force and Board member agency activities

AG CORTEZ MASTO:

Agenda item 3 is our report regarding task force activities. At this point, we usually hear from various entities interested in giving us an update. Obviously, the FBI is not here. Would any other Board member like to give us an update on the activities of their office?

LIEUTENANT BALDRIDGE:

Madam Chair, from the Washoe County Sheriff's Office, we have Detective Carry with us to provide an update from the task force.

DETECTIVE CARRY:

Thank you Attorney General. The task force in the north has been very busy since the last meeting. We have served approximately 10 to 12 federal and state search warrants relating to child pornography in addition to various fraud-related search warrants. Just the other day, we had a sentencing in federal court. The subject was involved in possession of child pornography. He received 60 months. We have had several other people who have pled out during the interim since the last meeting but have not been sentenced yet.

We have had approximately 5 indictments and have recovered probably over 100,000 videos and images of child pornography and other related child exploitation crimes.

AG CORTEZ MASTO:

Thank you very much, Detective Carry. I also understand that Mr. Ipsen has some information regarding participation in cyber competition sponsored by the Department of Homeland Security.

MR. IPSEN:

Absolutely. Thank you very much for the opportunity.

I want to take a second to complement the Nevada contingent to the annual Department of Homeland Security cyber security challenge. It was held in Washington DC last month. This is a competition where each state sends a representative group of cyber security professionals. They challenge each other. The first day is a day of training. The second day is a day of competition. Each group works against every other group in the competition. They have 10 minutes to secure their machines and then two hours to defend them against other groups. After that, they reverse rolls.

In this year's competition, a multijurisdictional group of individuals from Nevada won the competition.

Last year the competition was won by a multi-state group. This year Nevada's group of John Lusak, from the Office Information Security, Anthony Workman, from the Department of Public Safety, and Eric Hohman from Washoe County, competed and won the competition. Not only did they defeat everyone in the competition this year, but last year's champions as well. This was really a feather in Nevada's hat.

On a personal level, I want to say it was really nice to be in a position where Nevada finished number one, rather than the number 50 we so often hear about. We really have some great assets in Nevada. I think that was born out this competition. We will have an opportunity next year to defend our title. We will also have the opportunity to extend these capabilities nationally by working with other people. This is a really important area. It is where the rubber meets the road. You can talk about people being in cyber security, but until you subject yourselves to competition with other highly capable professionals, only then do you really know what you are capable of doing. I really commend them in their efforts.

We also had an opportunity to talk about some of the challenges that face the state with officials from the Departments of Homeland Security and State, and a number of other key entities headquartered in Washington DC. I think Nevada is making very positive steps forward in this arena.

AG CORTEZ MASTO:

Congratulations. And, congratulations to all the members of the team. Might I add, one of the team members, Mr. Lusak was a former employee of my office. He was a very good, very talented employee. It is a feat, and something we should be very proud of. So, congratulations from all of us. Thank you.

Agenda Item 4 – Presentation by Tom Kellerman, Laying Siege to Castles in the Sky, an analysis of current cyber threats

AG CORTEZ MASTO:


Item number 4 is a presentation by Tom Kellerman. He is vice president of security awareness and strategic partnerships, Core Security. He is also a professor at the American University School of International Service. I would like to add that Mr. Kellerman was a previous Chief Information Security Officer for the World Bank and is a current Commissioner on the President's Commission on Cyber Security. Welcome.

MR. KELLERMAN:

I am going to focus on three sectors today, energy, finance, and the dot gov space, or essential government services. It is important to note, given my background at the World Bank and on the Commission, as the Chair of the Threats Working Group, much of my discussion is not directly related to the corporation that hired me, but more importantly to the environment – the ecosystem

– the shadow economy – of adversaries that are constantly targeting these sensitive, critical infrastructures on a regular basis.

Agenda



www.coresecurity.com

1. History of the Threat
2. State of Play
3. Energy Sector Exposures
4. Financial Sector Exposures
5. Online Payment Systems: Money Laundering Online
6. Organized Hacking
7. Real World Attack Behavior
8. Cloud Computing
9. Challenges in IT Security
10. Relevant Standards and Best Practices
11. Critical Security Questions
12. The Future of Cyber Attacks

9/8/10 2

The agenda is self explanatory. What is most important is the focus is not just on threats, but on critical policy, procedural, and technological advances, or strategic opportunities you might delineate in order to progressively place Nevada in the forefront of this battle, this war, in cyber security.

History Repeats Itself



www.coresecurity.com

- Hannibal using the Roman Roads to cross the Alps



9/8/10 3


We have seen this before. In 213 B.C., Hannibal sacked Rome using the very infrastructure Rome created to extend its own power.

The problem was that the infrastructure was developed without fortifying it correctly.


The same thing has been done with the Internet. For those of you who are not familiar with the Internet, the ARPANET that was created in 1969 by DARPA was never meant to be a secure communications system. Yet, we have put our most

essential services within this system. Today's presentation will focus less on denial of service, or the disruption of services, and more on a discussion of the infiltration of critical services, the infiltration of command and control and integrity attacks. By that I mean attacks on the integrity of the data. These are much more pernicious and are much more visible from both a nation state perspective as well as from a critical, organized syndicate perspective. By "critical", I mean the eight major criminal syndicates of the world that exist here in Nevada.

Reality Check



www.coresecurity.com



- There has been a 200% increase in intrusions into U.S. government networks. --GAO, 2010
- 73% of the computer intrusions existed for over 9 months. --OMB 2010
- \$6.75M in losses associated per cyber-breach. --Ponemon Institute 2009
- \$1T in losses from Cybercrime in 2009 --World Economic Forum


9/8/10 4

Here are some fun facts.

According to the GAO, there has been a 200% increase of intrusions into U.S. government networks last year. More importantly, 73% of those intrusions existed for 9 months or more within those systems. This is highly problematic. It means these systems were polluted and were attacking trusted systems, critical systems, for over 9 months, according to OMB.


Regardless of the financial losses – and the Ponemon Institute, the go-to institute for cyber

insurers, insurance companies as they try to quantify cyber losses, which is why it is placed on this slide – that \$6.75 million per day is only associated with down time. It does not include loss of intellectual property, national secrets, or financial data, etc.

2010— Unprecedented Threats 

So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss. If you only know yourself, but not your opponent, you may win or may lose. If you know neither yourself nor your enemy, you will always endanger yourself.—Sun Tzu

- An 827% increase in compromised Web sites, the primary method for malware distribution, compared to 2008. (Anti-Phishing Work Group)
- Increasing numbers of spear phishing e-mails with malicious payloads target U.S. law and PR firms and their clients' IP. (FBI)



We need to pay respect to the adversary.

I think that is one of the critical problems of the U.S.'s perspective in cyber security posturing.

We do not play enough chess. We do not spin the board. We don't understand our own vulnerabilities; nor do we understand the tactics of our adversaries when we try to deploy cyber security solutions.

So, non-technical folks perceive it as a technological problem. They think we need technology to solve technology's problems.

The problem here is that many of these sophisticated actors are the protégées of the former chief scientists of the KGB that used to hack our systems – that is just from an Eastern European perspective.

From a southeast Asian perspective, we have governments that actually train and have competitions in high schools on a regular basis to generate the next generation of hackers, much like we train and generate NFL and NBA players here in the U.S.

With that cultural paradigm, we need to recognize and appreciate that the attacks have changed. There has been an 827% increase in web sites – trusted web sites – domains like CNN, Bank of America – systems being compromised. The Treasury's web site, Treasury.gov, was polluted two or three months ago. For the users, anyone who visits those sites, devices will be compromised immediately. This genesis of polluting trusted infrastructure and backdooring it, so that when you visit it as a user or employee, your system will become compromised, is something worth noting.

State of Play 



- FBI's #1 Criminal Priority is Cybercrime.
- Worldwide federation between various classes of cyber-criminals and malware developers.
- Nation-state, terrorist and politically-driven backing of targeted cybercrime efforts.
- 108 Countries maintain a Cyber-warfare division of their militaries.—FBI 2007

In addition, the FBI noted last year in a letter sent to major corporations in the U.S. that PR law firms and law firms – which you implicitly trust because of the contracts and the relationships that are espoused by modern society – are being targeted frequently to be the conduits, the transit points, by which systems can be attacked and successfully penetrated. This phenomenon was first noticed in the United Kingdom when major law firms were being targeted because their trusted communications channels were implicit. Most of these law firms had minimal cyber security practices in place.

As regards the state of play, The FBI's number one priority is cybercrime. More importantly, there is a worldwide federation of various classes of hackers that work in conjunction with organized crime syndicates to leverage various types of capabilities. There exists almost a pax Mafiosa – an underground economy that is exemplified in conferences like Black Hat Amsterdam. I know there is a Black Hat conference here in Las Vegas next week, a major cyber security conference that is held here every year. This one has been so commercialized, and there are so many law enforcement officials that go to it, that most of the best hackers do not attend in Las Vegas anymore.

The reality is that CanSecWest, in western Canada, Black Hat Amsterdam, and others like ShmooCon illustrate the phenomenon of information sharing and tactical superiority of the underground. They share far more information among themselves than we do.

There are 108 countries with cyber warfare capabilities. But what is more interesting about this reality is that many of those countries use those capabilities to enhance their comparative advantage of corporations that exist within their boundaries. They enhance the industrial espionage capabilities of major companies that exist within their sovereign boundaries so that they can leapfrog their competitors in the international market place.

Electrical Grid is a Prime Target

- Overseas attackers seek to infiltrate the energy grid, in order to:
 - Disrupt the American way of life;
 - Embarrass the U.S. government by compromising its Critical Infrastructure;
 - Cripple and weaken U.S. financial markets and other vital business operations, wreak economic havoc; and
 - Distract the public in order to attempt additional electronic campaigns or coordinated physical attacks.

Slide 7

Let's look at one sector in particular – the electrical grid.

Much of what I will discuss here comes from Mike Assante. He was the Chief Security Officer for NERC (National Electricity Regulatory Commission). He was also the head of Idaho Labs. I will discuss the importance of Idaho Labs in the recent Aurora test.

It is important to note that many of these systems have already been infiltrated and many of these systems are vulnerable to attack because of the smart grid revolution as well as the business continuity movement, which I will discuss.

Energy Sector Risk

- 2007 Aurora Project: U.S. Department of Homeland Security tested the security of emerging Smart Grid technologies.
 - Demonstrated the threat by exploiting a power grid network vulnerability to destroy a generator.
- Brazilian Cities Blacked out in 2007
- Estimated that a successful actual attack on one third of the North American power grid would cost \$700 billion over three months.

Slide 8


In 2007, the Aurora project of Idaho labs essentially tried to prove that, via cyberspace, they could blow up a generator. By using various free capabilities, they attacked a system to turn off the safety sensors that would essentially say that the oil slicks that were lubricating this giant generator are “on”, but they were not “on”. They had turned them off, but they faked the system out, indicating that the safety system and the oil slicks were running. It blew itself up. You can YouTube this later today. Type in “aurora project” into YouTube or Google, and you can see this image.

What is more important to realize is that we don't make these generators anymore. So, if there were to be effective, wide-spread attacks by a nation state, not necessarily China, but Iran, should we ever be involved in a conflict with these countries, it would take six to eight months to order these giant generators and these parts to be delivered to your communities.


It is also important to note that Brazilian cities were blacked out in 2007 – successfully blacked out – by organized criminal groups in these cities who were angry their leadership was arrested by Brazilian police.

Tom Donahue, who works for a 3-letter agency, touted the reality of susceptibility of attacks on the energy sector at a conference in New Orleans. So you know who Tom is, not speaking to his direct roll, he works for the Office of the President as an advisor to Howard Schmidt and the National Security Council on these issues.

There is a scientist named Jian-Wei Wang who actually produced a widely distributed report on how he could knock out the west coast power grid. This is still available on line. I would be happy to send it to you.


Additional Issues Emerging 

- The U.S. Department of Homeland Security has identified a report by a research scientist in China demonstrating how an attack aimed at a small power sub-network could potentially trigger a cascading failure of the entire West Coast power grid.
- Jian-Wei Wang, a network analyst at China's Dalian University of Technology, used publicly available information to model how the West Coast power grid and its component sub-networks are interconnected, increasing their value as a target.




Slide 3

The fact that this report delineates the perfect attack paradigm to knock out the west coast grid is highly problematic – particularly when it has been translated into four languages.

Cyber Vulnerability 

- Cyber vulnerability presents a growing and increasingly sophisticated threat.
- 85% of all systems relays are now digital.
- Industry purchased products can contain inherent vulnerabilities.
- “... a single exploitation of a vulnerability can be propagated across a cyber or power system network and potentially affect an entire class of assets at once.” (HILF report 6/10)



Slide 10


What we need to respect and appreciate is that some of these statistics and data come from the HILF report. The HILF report is a report released by the FERC and NERC folks, with Mike Assante before he left and was replaced by Mark Weatherford. NERC is the industry's self-regulatory organization.

They noted that 85% of system relays in the energy sector are now digital. This means that they are vulnerable to cyber attack.

More importantly, a single exploitation of a vulnerability can be propagated across the entire system in a nanosecond. Given that, why are there more points of ingress? This is a reality. The system can be taken down. But, how do you get into that system? How do you infiltrate that system?

Root Cause Issues 

- The U.S. electrical grid has long maintained an acceptable level of engineered resilience in the physical sense.
- Introduction of IT-based controls, specifically SCADA technologies now connected has created a higher risk of remote attack.
- The business continuity and resiliency movement following 9/11 has only served to exacerbate cyber-security concerns.



Slide 11

The events of 9-11 should have taught us that non-state actors will use technology against critical infrastructure. We should have learned that lesson.

But, what we really learned was business continuity and resiliency. You have to have business continuity and resiliency for all of your physical facilities from kinetic attack.

So, everyone ran out to build backup network data centers. They increased wireless uses and remote access and web 2.0-kind of portal technologies.

But in doing that, they increased the target. Back in the day, you had to be an insider to mess with the system. You had to be an insider to control the system. But now, you can hack a wireless transmission layer. You can hack a remote user. You can hack that remote data center. You have all these other points of attack because of the physical requirements of business continuity.

More importantly, the smart grid is highly problematic because it creates another node by which someone can ingress and attack that primary system at the house level.

You can now hack the system from the individual house level because the system is implicitly trusting the data coming from the house so it can control the amount of power released to the house. We have to respect and understand the fact that there is a bidirectional flow of

information. It is an aquatic environment. If you can compromise any one point in the environment, and ride the protocol or control the operating system or the application layer – sorry if I am getting technical – you can essentially backdoor and penetrate the system.

NIGHTMARE SCENARIOS

- Cyber intrusion into field engineering networks and the compromise of relays and Remote terminal units at multiple substations. The consequences range from simple breaker operations (open a line) to operations that cause equipment damage (aurora) only being one scenario.
- Man-in-the-middle attacks on data acquisition information allow attackers back to an interconnected control room or to swim up stream and compromise a front end processor.
- A push of bad firmware out to a significant number of remote field devices that can't be recovered by zeroing/reboot.
- Insider with access to several PCS systems for safety and protection.

According to Mike Assante, these are the nightmare scenarios.

The Aurora scenario illustrated scenario number one. Cyber intrusion into the field engineering networks, using the compromise in the relay and remote terminals, to, in the end, blow up a generator or take over a control station.


You have man-in-the-middle attacks, where basically you can allow attackers to backdoor something, push their way through the Internet, to interconnect with the control room.

You have the reality that many of these systems are implicitly trusting of the firmware and software updates that are pushed down to the systems. But you can pollute those software updates and compromise a multitude of systems at once.

Last, but not least, you have the rogue insider phenomenon, which everyone typically worries about when deploying these technologies.

NERC Letter

- April 2009 letter from NERC CSO Michael Assante:
 - Companies have not identified enough of their assets as critical thereby requiring additional protection.
 - NERC will "broaden the net of assets that would be included under the mandatory standards framework in the future."
 - "Assess the remote manipulation of Critical Assets via cyber-means"

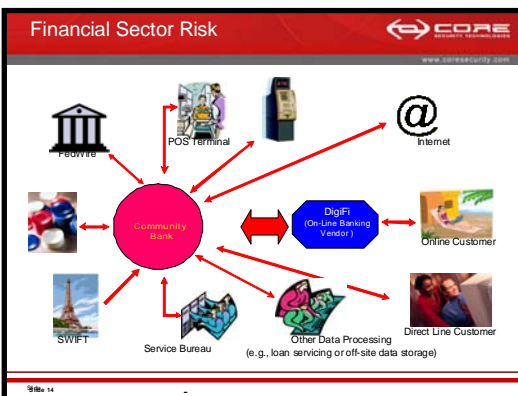


In April 2009, Mike issued this letter. It was this letter that got him in trouble.

The letter went against the grain. It was unorthodox. It stressed that the whole energy sector did not understand what the critical assets were.

They were so focused on the electrical engineering aspect of critical assets – what is critical from an electrical or mechanical engineering perspective – not a computer science perspective. Because of the business continuity movement and because of

the smart grid phenomenon, because of the mergers and acquisitions that have gone on in this sector, they really needed to assess the remote manipulation of those critical assets by cyber means. They needed to red team. They needed to scrimmage. They needed to penetration test. What could be compromised? What could be successfully attacked through cyber space, through cyber assets, to impact their critical physical assets? That was the paradigm that was lost.



Turning to the financial sector, everyone has been following the financial sector lead in cyber security for a long time. Having been a cyber security professional in a major, global, financial institution, I will tell you there are five critical gaps in how the financial sector has deployed its security.

There are five chinks in the armor, which have been widely utilized to compromise financial payment systems and in identity theft and in the compromise of banks globally.

More importantly, the financial sector has traditionally faced the most pernicious and sophisticated of adversaries because the Eastern European protégées of the former KGB guys are the ones that are focusing their attention on the banks because they are focused on “Money is God.”

That being said, look at this image, and notice all the different technological systems and networks that connect one community bank. Realize that you can compromise any one of those segments and you can compromise the primary bank. It is an aquatic environment. You can swim your way bilaterally through any of those systems.

Twenty years ago, there were only three connections to that community bank. You had the Fed, SWIFT, and the ATM machines. You have now increased all those connections. Because of those increased connections, you have to realize that they can all be compromised.

Organized Data Thieves Running Wild

- Organized cyber-criminals are using sophisticated, targeted attacks to steal mountains of consumer records.
- Kneber Botnet/ZEUS: 2,500 companies affected

According to the National Counter Intelligence Division in the Directorate of National Intelligence, last year was the first year that organized crime made more money through cyber crime than through narcotics, human trafficking, and other criminal enterprises.

That being said, if they did not have the capabilities before in house, they have coerced the capabilities, or they are using the service-based cyber economy to generate the capabilities I am going to discuss now.

So, first of all, where is the money? How do you make money? There are two ways. One is called cyber fraud. The other is service delivery.

Types of Cyber-Fraud

- Salami Slice
- Funds Transfer— 56,000 instances of wire transfer since 1997, more than half have occurred in the past two years. -FINCEN, 2009
- Brokerage Fraud
- Extortion via DDOS
- Extortion via crypto
- ID Theft— 2001 --Abraham Abdallah targets Spielberg, Oprah, Martha Stewart-- Fortune 100
- Market Manipulation
- Money Laundering

From a cyber fraud perspective, there is a salami slice approach, where you hack 100,000 accounts and take \$5 from each account once a month. No one notices this. None of the fraud detection mechanisms go off. The consumer doesn't even recognize it. But you are making \$500,000 a month! You have infiltrated the system, and you are just taking a tiny slice.

More importantly, there is large value funds transfer fraud. This has exploded. There have been 56,000 incidents of this in the past twelve years. More than half have occurred in the past two years. That is because large value funds transfers – 10 grand or more – are now taking place in real time – that day. They can no longer unwind the financial transactions like they used to. They only have two to three hours now to unwind fraudulent transactions, whereas, five years ago, they had a full day to review their books and say, “I don't know. We should never have sent that money to Latvia.”

To highlight this, the number one growth area in lawsuits in America currently are private businesses suing banks. This is because business accounts are being compromised and the banks are not making the affected businesses whole.

Brokerage fraud is self-explanatory. Extortion via DDOS goes something like this: “I am going to knock your system off line. I am going to tell you to pay me or I am not going to let you bring it back up.”

Extortion via crypto: “I am going to encrypt all of your sensitive data so that you are blind. It is all gibberish. I am only going to bring you back to life if you pay me money.”

Extortion via extortion: what this means is “I am going to compromise your partner systems or a trusted system that you cannot destroy a relationship with, but I am going to use your accounts to do it. And, I will prove to you that I have access to it.”

Identity theft we are aware of.

Market manipulation may have been what we saw a couple of months ago. [A precipitous, unexplained drop in exchange stock prices followed by an almost immediate recovery.] The investigation is on-going for the new circuit breakers on Wall Street.

Last, but not least, there is money laundering.



Beyond those ways of making money, the ecosystem is so diverse, that there are all these ways of making money.

The real hackers don't make money through what we have just described, other people do that. Other people do that for them.

Real hackers create things like detailed information on technical vulnerabilities. For example, “There is a Microsoft vulnerability that hasn't been patched. I am going to sell this to you. I will sell you the syringe you need to penetrate the system and

promulgate the exploit. You are going to pay me money.”

There is sensitive information on how these systems work. That is worth money. In a global recession, there are a lot of ex-financial people, a lot of ex-IT people, from sensitive organizations that know exactly what is critical, and what moves and how. They communicate in these channels to share this information for a fee – almost like reconnaissance.

How to defeat security and anti-fraud measures? This is a widely accepted form of employment now a days. You have basic infrastructure provision – hacking services, just intruding or maintaining a persistent presence; knocking people off line; custom malware development; spamming, scamming.

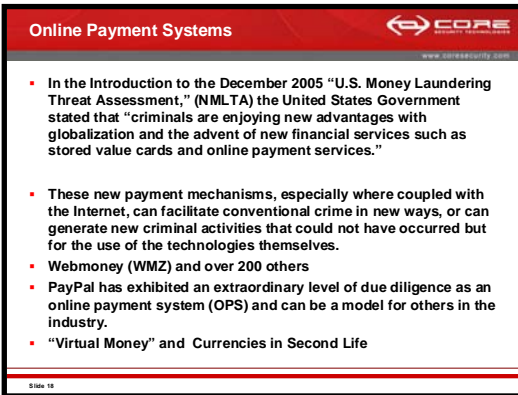
Bullet proof hosting is interesting. They know law enforcement and ISPs are trying to shut down command and control of all these systems that are either compromised or are being used for bad things. They create bullet proof hosting capabilities, specialized equipment for laundering funds, like card embossers and so on. They have even gone so far with identity theft that they have wholesalers of PII [personally identifiable information]. But these wholesalers can only justify the work – the bundles of PII that they sell – based on running FICO score checks. So, they say, “I have a bunch of high-value, great FICO score people that you can use to take out home equity loans. You can get platinum cards on their information. You want high-value folks?” They run checks. That is how robust the market place is.

Naming some of these service providers, you have the Russian Business Network, which was successfully engaged by law enforcement, but none of the members have ever been arrested. There are rumors that the leader of the Russian Business Network was essentially the son of one of Putin's favorite people. They still exist, using different IP addresses and names.

There is Hunaro, which is a South Korean group, which many think is actually a North Korean cyber crime group that generates money for the North.

There is Pigeon Hue, which is a great group in China. They have an agreement with the Chinese government where they will not go after the Chinese government. They won't attack any Chinese government systems or banks, but they will leverage these attacks against anyone else

Eurohost and Poison Box involve a fantastic hacker and his crew out of Turkey. They specialize in SCADA attacks, critical infrastructure attacks on those control systems. They sell that know how to others. Turkey has become prominent on the map of who is hacking what and how.



I have to pay homage and respect to the State of Nevada for SB 82 – specifically the forfeiture of electronic assets it relates to stored value cards.

I would challenge you to expand that to address alternative payment channels.

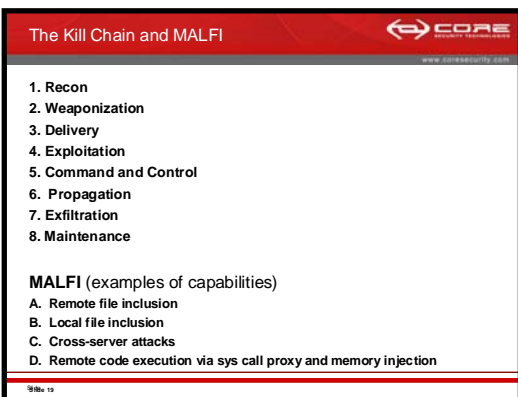
You have set the international and global precedent on forfeiture of the assets, and I salute you for it.

But, I suggest you take it one step further to deal with the Webmoneys, LibertyReserves, and Eagles out there that are blatantly playing in this game and

are non-regulated entities.

You also need to point to a standard of due diligence. Through my work for the Financial Coalition Against Child Pornography, I learned the way PayPal cooperates and collaborates with law enforcement, the way they investigate things, the way they vet their customers, the way they black list their customers should be the standard of care for these types of entities.

Last, but not least, turning to virtual money and currencies in Second Life¹, these are growing. Let's face it. I know it is not just a video game anymore.



Okay. How do you attack things?

I need to explain this to you so you can appreciate the level of sophistication we face.

They do not just push a virus into your system and take over stuff or knock it down.

Sophisticated crews that are going after sophisticated infrastructure in your State and in your State government itself are using the Kill Chain. The Kill Chain is not just one person. The Kill Chain involves three or four people. The chain

begins with a reconnaissance to determine who is the target and what is important to them and what you are connected to. The weaponization stage may involve, "I need zero day exploit code. I need exploit code that has never been seen before that can take over an operating system or an application at the root level, which is undefendable by firewalls, virus scanners and encryption."

Once I have that, I need to deliver it. I might deliver it through a botnet, through a zombie arm in computers that you know about. I need to exploit that system in a stealth fashion. I need to

¹ For explanation and background, see Minutes of the Board's Meeting on September 5, 2008.

maintain command and control in a persistent fashion, usually through memory injection techniques. Propagation: I need to move slowly through the system, and as I go, send out all the private keys and authentication and access control information that I can.

In exfiltration, the attacker uses ports that are already open for Internet access, email access, or SCADA-system access.

And, last but not least, showing the level of sophistication, is maintenance. These miscreants actually patch the holes that they came through. They patch the hole they came through in order to protect their hole for the community they just created. So, security experts can not find out that anything has been done because there is no hole that is apparent because it has now been patched.

MR. MORTENSON:

I am trying to understand why anybody would want to attack a system of electrical networks. What benefit would they get out of it? This looks like an extraordinary effort, and I don't yet see how an attacker gets anything.

MR. KELLERMAN:

Depending on the actor, from a state actor perspective, it is obvious to have backdoor command and control in case tensions arise with the United States. There is a lot of discussion around the term "soft power". Cyber power is a part of soft power as distinct from hard power. From a non-state actor perspective, or a criminal perspective, you could extort the owner of the utility by showing the utility you have command line access to their system. You could also, because energy is a commodity and it is traded, manipulate the system not unlike what Enron did through cyber means. Market manipulation of the energy sector could be accomplished by cyber means. Those are just a couple of examples. I am sure that I could give you a couple of more if I thought about it.

MR. MORTENSON:

Those are good examples, thank you very much.

MR. KELLERMAN:

From a real world perspective, we need to keep in mind that they are using what are called blended attacks.



"Oh, my web site doesn't touch my sensitive stuff." Well, it does. Because they can now push themselves through your web site, using techniques like SQL injection or cross site scripting attacks. They can then take over the web server and the data base server, and then they are in your network.

Once in the network, they kind of leapfrog around your network. Eventually, you may say, "Well, even that network is an outward facing network. It doesn't really touch my sensitive network. My sensitive network doesn't touch the Internet." That is what government agencies say many times.

But it does. There is always one box, one device, that is dual homed. That means that has two network cards in it. It means it communicates with the outward facing network and this inward facing network. Good hackers use what is called local information gathering in order to understand where that box is. Once they take it over, they control the bridge.

We need to respect that. They are playing chess, not checkers, with our systems. They are going eight to ten moves ahead, spinning the board the whole time.

Primary Attack Vectors

- Digital insider: APT
- Client-side applications
- Operating systems
- Web applications
- Wireless networks

APT Exfiltration--Tell Tale Signs:

- 1) Greater than 10 minutes
- 2) Greater than 5MB
- 3) Startup same time
- 4) DNSCache/Hackers use IPs

The primary attack vectors today include the digital insider – the advanced persistent threat you hear about. It is real. Most of the time they are hitting you from the inside out.

Client side applications are called spear phishing. You no longer need to click on the link or download the attachment to become compromised. They are actually attacking the QuickTime viewer, the Adobe Acrobat that runs on your system inherently. So, just having an email in your in-box can compromise your system if you have not patched those applications already existing on your home PC or

remote PC.

You will be well aware of flaws in operating systems. Problems with web applications are growing. Wireless exploits are growing tremendously.

I would worry about the Gaming Commission and the fact that when I walk through casinos, I see wireless everything. It is encrypted, but that is not going to solve the problem given the sophistication of the attacks we have seen.

More importantly, from the insider perspective, you will never see them in your system because there is no signature. No picture will have been taken of what their intrusion effort looks like. However, you can tell if you have an insider problem through four simple rules of thumb. One is the connection time of the device to the outside world. If it is more than 10 minutes, you have a problem. Another is if the device sends out more than 5 MB of data in a session. Another is if it starts up at the exact same time every day. No human being sits down and turns on a computer at the exact same time every day. Last, hackers love to use IP addresses to communicate. A DNS cache means there is a domain, like .CNN or a .Vegas or a .Nevada being recorded that doesn't really exist. When you look up a domain address, and can not find it, meaning it doesn't really exist, you have a problem. These are four simple rules that can be applied without knowing exactly what kind of attack is underway.

Modern Maginot Lines

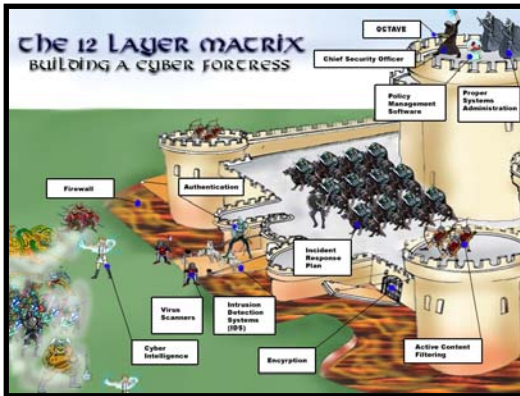
- Early 1990s: Virus scanners
- Mid 1990s: Firewalls
- Late 1990s: Over-reliance on encryption (PKI)
- 2000s: Over-reliance on IDS and Anti-virus

We should have learned something from the French.

Here is what we should have learned. Perimeter defenses, the firewalls, the encryption, the virus scanners, the IDSs are not going to stop the threat you are facing today.

The panzer tanks and the paratroopers will bypass and have bypassed those systems. This has to be solved through policy.

So, with apologies, forgive the childish nature of this slide, but we are over-reliant on the walls and the moat. And, yes, I purposefully misspelled "encryption" because if you can just compromise the spelling of "encryption" or take one of the letters, the private key, out of the picture, you can compromise the walls of the entire castle.

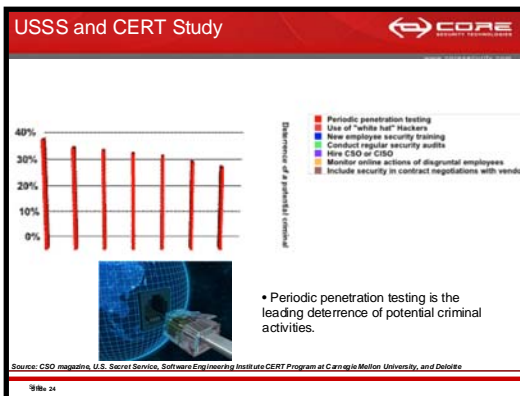


What is most important is that we are not scrimmaging enough. We are not actually assessing whether all of these policies, procedures, and technologies are working in conjunction, seamlessly with each other.

The reason why Chris and his team won that competition is because they scrimmaged well.

They have demonstrated a higher level of sophistication through their scrimmaging. The United States Secret Service and CERT released a study recently that noted the seven major things

you should be doing are periodic penetration testing (pen testing), use of white hat hackers, new employee security training, regular security audits, hiring a CISO [chief information security officer], monitoring on-line actions of disgruntled employees, and including security in contract negotiations with vendors.

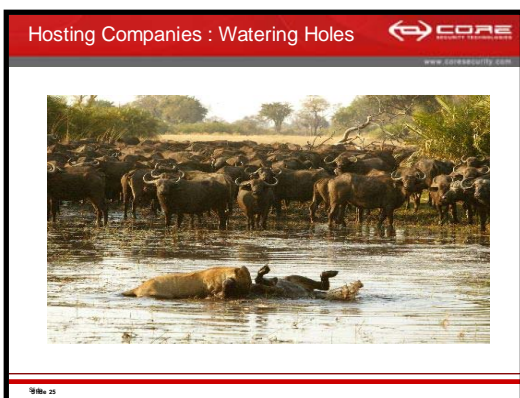


Let's speak to that.

With the cloud – you hear about this cloud thing – the cloud is going to be the Achilles heel of the American empire – unless properly secured through both contract language and through security assessments, and through various technologies, some of which don't exist yet.

The rush to join the cloud is the rush to move west. It became a wild west environment for a long time. I will speak to that.

The last two years in a row, the most credible, the most statistically significant report released every year is the Verizon business security report. I am sure you can attest to that. One third of breaches for the last two years in a row were due to strategic partners, who you trusted, whose systems were compromised in order to compromise the primary system.




The DHS system that was compromised years ago was compromised because Unisys was compromised.

The DOD major infiltration called Titan Rain was a compromise because Lockheed Martin was compromised.

So, given those realities, through mere contracts, how should you change the service level agreements that you have with managed service providers of managed security service providers to actually increase the level of liability. Right now,

they are just contracts of adhesion.² They do not really have any real liability except time and a guarantee of up time. Up time is not what we need to be focusing on.

² "For a contract to be treated as a contract of adhesion, it must be presented on a standard form on a 'take it or leave it' basis, and give one party no ability to negotiate because of their unequal bargaining position." Wikipedia.

Systemic Risk 

www.coresecurity.com

32% of Data Breaches occurred via third-party systems.
—Verizon Business


1. Verify that the legal requirements to which the service provider is contractually obligated are compatible with your organization's definition of adequate security (e.g., NIST 800-53).
2. Identify who in the service provider organization is responsible for security oversight (e.g., CSO or CISO). Their Information Systems Security Policy and incident response plan must be reviewed prior to movement of data or provision of service.
3. Confirm that their policies and agreements regarding security breaches include customer notification on a timely basis (within one hour). Maintain the right to test their incident response plan on an annual basis.
4. **On a quarterly basis conduct penetration tests of their network security posture, and verify whether they have layered security beyond firewalls, virus scanners and encryption.** (NIST 800-53A Appendix G serves as excellent guidance on this matter).

Figure 26

So here are some recommendations.

I am not going to read through these in the interests of time.

But let's speak to the cloud.

The Gathering Storm: Cloud Computing 

www.coresecurity.com

- Distributed, interconnected clouds also create as many potential risks as they may eliminate.
- Multi-tenancy and resource usage optimization driven by economies of scale introduce a multitude of security issues due to the blurring of lines of demarcation for data entering and traversing the cloud.
- Where does your organizations cloud end and begin?



Figure 27

The interconnected, distributed clouds that are coming, that we are being forced to use because they are more efficient, more green, more everything else. It is more resilient against denial of service attacks. True, true, true.

But they are also more susceptible to infiltration and integrity attacks.

Where does your organization's cloud end and begin?

There is an over-reliance on encryption. Encryption can be defeated and it is very difficult to deploy cloud-wide. Virtualization, which is the foundational technology that creates the cloud, has been exploited and is exploited today. There is a thing called "cloud burst" that was widely used in the underground economy to compromise major cloud providers in the last two years – just as an example of one.

5 Elements of the "Perfect Storm" 

www.coresecurity.com

- An overreliance on encryption: encryption can and will be defeated, by technical innovation and human error.
- Virtualization is still a security unknown: there are significant vulnerabilities in the systems people are using today.
- Outsourcing is a huge security risk: Organizations don't typically make security a major element of their SLAs and write safeguards into their outsourcing contracts. Unless they do so and invoke major penalties for breaches, a pass-the-buck approach to security will continue to dominate.
- The security perimeter becomes even fuzzier. With data constantly available in the cloud for user access, in multi-tenant environments, the opportunity for infiltration would seem to grow exponentially.
- SaaS Apps May Leak Data Even When Encrypted: their use of networks can cause "side-channel" leaks that might enable attackers to glean even the most sensitive.

Figure 28

Outsourcing is a security quagmire. You need to manage that through contracts. You need to test that entity and force remediation timetables on those entities that provide services to you.

The security perimeter, just like in a cloud, is constantly changing shapes. That is why it is called cloud computing. How do you protect that from integrity attacks, not denial of service attacks, you have to stop focusing on that. Denial of service attacks can be solved through technology.


Software as a service applications leak data even when they are encrypted in a cloud environment.

So, what am I trying to say here? What I am trying to say is that operational, reputational, systemic risk has metastasized due to a technological dependence of our culture.

We do not pay our adversaries enough respect. We do not fully appreciate that cyber crime and cyber warfare is the future of nefarious acting in this world. We need to begin to manage this risk like we do financial risk and traditional kinetic operational risk.

Challenges in IT Security

- The threat environment continues to evolve ...**
 - Growing opportunities for cyber-criminals
 - Increasing attack frequency and publicity
 - Widespread adoption of Enterprise 2.0 technologies including social media
- Organizations still struggle to keep up ...**
 - Shortages in skilled technical staff
 - Underscores the need to operationalize security as an ongoing, automated business process
 - Siloed security strategies present data overload with low visibility into real risk
 - Organizations can't measure overall security effectiveness or efficiently mitigate risk
- Mandates for security assessment and assurance continue to emerge ...**
 - Legislative, industry and internal regulations
 - OMB Directive 10-15
 - PCI, HIPAA, FISMA/NIST, CAG, multiple pieces of pending U.S. government legislation
 - Demand for due diligence by customers, investors and other stakeholders
 - Requires ongoing measurement, benchmarking and reporting of security posture




Slide 30

IT is going to evolve. There are not enough people. There are more stresses on the system. There are all kinds of regulations.

I think there was a dramatic paradigm shift in Washington DC two months ago when Howard Schmidt and Vivek Kundra mandated that not only OMB give the directive to DHS to run cyber initiatives for U.S. government agencies on the civilian side, but they also released a memo and directive known as 10-15.

OMB Directive 10-15- Overview

- What it entails:** "Provides instructions for meeting your agency's FY 2010 reporting requirements."
- Top-level message:** "Agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way."
- Practical message:** "CIOs, CISOs and other agency management need to have different levels of this information presented to them in ways that enable timely decision making."



Slide 31

That directive essentially said, "You can no longer check list your compliance exercises for FISMA [Federal Information Security Management Act of 2002]. We don't want to see that this year. We want you to prove to us on a regular, continuous basis that these controls you say you have in place, are actually working. We want you to benchmark the effectiveness of your security controls on a continuous basis."

That represents a significant paradigm shift. Essentially they were saying, "We want you to scrimmage everyday. Show us you are scrimmaging. And show us that you have learned something from your scrimmages because of the dynamic nature of the adversary."

OMB Memo - Implications


- How-to garner these enterprise-level metrics:**
 - "Agencies need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information."
 - "Agencies need to develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools."



Slide 32

One of the most seminal reports and guidance on how to protect ourselves was released in a joint effort by NSA, NIST, the SANS Institute, which trains most of the cyber security professionals in the U.S., Secret Service, and FBI. These organizations all collaborated. It is called the Twenty Critical Controls, or the Consensus Audit Guidelines.

Controls Verification and Effectiveness



Controls	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Typical Products	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Test & Measurement	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Legend: ● CAG Test Now ● CAG Test Future ● General Test Now ○ Never

Slide 34 - COMPANY

It was based on the CNCI, the Critical National Cyber Initiative, which was led by Hathaway under Bush, on why are we bleeding so badly as a country. From that we learned that there were certain types of attacks that were being leveraged, most frequently the blended attacks that I have discussed. The question was how do we manage them. So, if I am a CISO in a room right now and I need twenty critical controls to focus on in the next two months that will increase my security by 80% thereby eliminating a lot of the dangerous noise.

It was based on the premise of offense informing defense. One of those twenty critical controls,

which my organization does, and we actually train the people who do this, and that is more important, we are not just a product vendor, we are a training organization, is how to effectually red team and test your defenses before the enemy does.

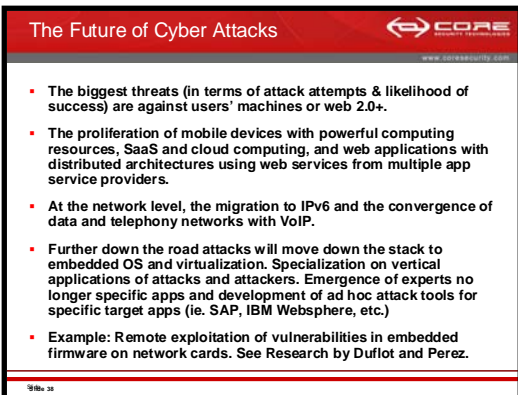
but the legal department, the PR department, the folks who do immediate communication with law enforcement, did their jobs so the right things actually happen.

Saying, "We are going to do a drill tomorrow," simply is not pro-active. If logs are kept, who is reviewing them and how often are they being reviewed. Logs are basically records of what goes on in a computer every second of every day.

Have we tested our web site for holes? It is different from testing your network systems and your third parties.

Particularly in the energy sector and critical gaming sectors and government sectors, can we just white list our environment? This means anything new that tries to run, isn't going to run. We will only allow these four programs to run on this box. That is it. The reason why is many times when hackers hack you, they try to start a new process, a new program, to run. That is what the virus scanners are trying to kill. But because there are so many of them out there, you could save yourself a whole lot of time and effort just by creating white listing. I only trust this group of people. I only trust these applications.

Last but not least, when was the last time you scrimmaged? And, who remediated what you identified as critical?



So, moving to the future of attacks; right now we are focused on web 2.0, not social networks so much as these new applications and web portals that allow you to be compromised through trusted communication lines.

Wireless devices, particularly hand-held wireless devices, are extremely susceptible to compromise.

So is the cloud computing environment I described.

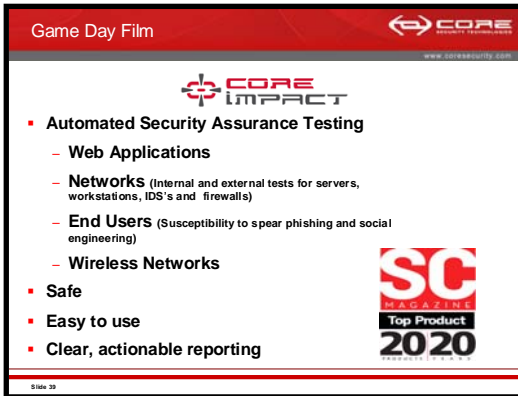
At the network level, IPv6, the next version of the Internet, so to speak, is vulnerable to attack. The

main reason is the hackers of the world used to use IPv6 before we adopted it. They liked it because it helped them protect themselves against malware service attacks. When hackers got mad at each other back in the day, they would black hole each other. They would basically knock each other off line. Because of that, they know IPv6 and the vulnerabilities inherent to that protocol far better than we do. They are at a much higher level of participation in that environment.

Voice over IP, oh, my God. None of us can even go out and buy a phone that isn't voice over IP enabled. Yet, that phone cannot have as many security things as a laptop because it does not have the memory space within the case of the phone to hold those. But, that phone can be compromised and used as a point of ingress to attack your whole systems and network. So, phreaking is back, right? But digital phreaking.

Last, this is really sophisticated. These two guys, Dufлот and Perez, work for the French Intelligence Ministry – actually one of the most pernicious adversaries directed against the U.S. in cyber space. They gave a presentation at CanSec West, the Canadian security conference about how they could compromise the network cards themselves remotely.

If you compromise a network card, none of your security will work. Ever. You can not defeat that. The fact that attacks for which there is no defense have been published and described and spoken about at conferences is troubling.



In the end, you game day film. That is what we provide.

That is what Chris uses. He uses our game day film. With his sophisticated personnel, he actually tries to create game day film on a regular basis on your systems. I applaud his work.

Last, but not least, we have to remember that we have to expect to be hit – and be prepared to survive. That is the mentality we need to get to. It is not about whether they will render our services unavailable, but whether they will infiltrate and

destroy the integrity of our data.

In closing, I would suggest this. Remember one thing about hackers. Hackers do not want to deny service to themselves. If they deny service to your infrastructure, they deny service to themselves. They would far prefer to go to a low and slow penetration attack on the integrity of the data, either steal it or control it. That would be the end game for them.

So, with that, I thank you for the honor to speak here.

AG CORTEZ MASTO:

Thank you, Mr. Kellerman. Are there any questions from Board members?

ASSEMBLYMAN MORTENSON:

When you say telephones are easy to compromise, are you talking about the hard wired telephones, or telephone systems that use the Internet?

MR. KELLERMAN:

The latter. But the phones are not what you think of as traditional phones anymore. They are using the Internet to communicate. This is what voice over Internet protocol means, voice over IP, or VoIP. That advancement has brought the phone rates down, but also increases the vulnerabilities of the systems.

ASSEMBLYMAN MORTENSON:

When I make a phone call, let's say to Japan, does that go through the Internet? Is that what you are saying?

MR. KELLERMAN:

The call touches the Internet at some point. It becomes zeros and ones at some point. Your voice becomes zeros and ones in the system.

ASSEMBLYMAN MORTENSON:

Okay. I was unaware of that. One last question. Could one of the secretaries here make a copy of your presentation, I would love to have it.

AG CORTEZ MASTO:

What I would ask be done, is if you would provide the presentation to Mr. Earl, he will get to all of the members. Are there any other questions?

For those members here who might be concerned about the integrity of the State system, something that Chris is intimately involved with, would you mind weighing in on what we have just heard to the extend you feel you can?.

MR. IPSEN:

Absolutely. I appreciate the opportunity. One of the largest challenges we have is communicating. If you are not absolutely frightened by what you just heard, then you do not understand the significance of what was just said.

This is something we in security have to live with day to day. It is something that can become so overwhelming that the human mind can not understand it, so we put into a compartment where it is not really addressed.

What I want you to know is that we are addressing these issues. I do appreciate those comments from Tom and from Core in terms of what we are doing. We are doing our best. Remember, we are in a fiscal crisis, and we are trying to do the things we can. We do have a consolidated security policy. It has been revised in the last month. You will see an adaptation to one of our standards. We do train on a regular basis.

One of the things that makes Nevada unique is that we talk on a county, city, and state-wide perspective. We are working together. That is an important point.

We do have some legislation that inhibits us from sharing resources among government entities. I am hopeful we can correct that in the next legislative sessions.

Additionally, we are restricted as an office from going out and pro-actively testing the entire state network because of laws that exist that preclude us from doing intrusive testing. Mind you, we never look at sensitive data. We simply want to make sure the security posture of the State infrastructure is sound.

This is a daunting task. I have made a number of presentations to the Board in the past, and I don't want to dwell on the thousands of points of ingress that we have.

We are trying to make the most of the resources that we have. We are fortunate that some of the tools, like the Core tool we purchased on behalf of the State, will be used state-wide. That purchase was not a budget item, but came from a department that said, "We need penetration testing. We need it because the feds require it of us, and because we believe it is the best way to validate that our security controls are good."

Rather than having that department buy it and keep it in their organization and use it only periodically, reflective of the global move of moving functions to the middle, we bought training with it. While we don't have training dollars internal to the State, the agency paid for training dollars so we can include people from every governmental entity that could potentially use a service like this. So, we are beginning to leverage this new DoIT capability outbound. What we are trying to do is take an enterprise approach with the zero dollars we have for these technologies to meet the challenges moving forward.

Another thing I want to point out, and I applaud Tom for saying this because it is so critical, from the standpoint of the Office of Information Security all of our training dollars are gone. They have been lined out of our budget. We did not have enough to begin with. We now have none. If we cannot move with agility to counter these threats – and we are not talking about hundreds of thousands of dollars, we are talking about 20 to 50 thousand dollars in the State budget – what we have to do is beg, borrow and steal training from any resource that we can. I don't beg on behalf of myself, but on behalf of the State. I think this is a problem that needs to be addressed from an enterprise standpoint. The ability to go out and do better testing, the ability to collaborate more effectively with government entities is highly critical. Finding training dollars, whether from federal grants, Homeland Security or wherever the money resides, to build a highly collaborative environment, I believe we can stave off some of the threats we face.

Everything Tom said is absolutely true. We are working with the federal government. Majority Leader Reid has asked for our input in the cyber security laws pending at federal level. Tom mentioned the change from FISMA compliance requirements to active testing. We are taking that same posture. We are encouraging this, not just to check the box and say that we have this control. We need to go out and verify it. We test it. We hammer on it using any resource that we can. We leverage the resources of anybody who is trusted and capable. And, we verify that our systems are secure. That is a significant change in the way the federal government is doing security. We are doing this as well.

Lastly, I want to say that Tom mentioned a number of individuals. One was Mike Assante. He was the former CISO from NERC. Mike is a friend. I presented with both Mike Assante and Mark Barret at the RSA Security Conference last year. Mike Barret is with PayPal, another organization Tom mentioned favorably. Both have committed to assisting the state of Nevada in whatever ways they can to make us more secure.

Additionally, the new CISO for NERC is Mark Weatherford. He is the former Chief Information Security Officer from the state of California. He is another trusted ally of Nevada. Mark has committed to coming in and talking to us in the future that is convenient to both sides. Mark will address our SCADA infrastructure, specifically the power grid.

If I could summarize, we have a number of resources. The challenges are daunting. The opportunities are great. The resources are very limited, but we are trying to think enterprisingly to do the best that we can. The number of national resources reaching out to the state are very significant. This is a very interesting time. I appreciate all the input Tom Kellerman and Core have presented now. We intend to work with them very closely in the future.

AG CORTEZ MASTO:

Thank you. Are there any other questions or comments from Board Members?

Actually, I do have one question after everything we have heard. Because this is a new frontier, and because it is so dynamic, from a State perspective, and we have heard a bit about this and seen your recommendations, it seems a daunting task to tackle this type of risk management, bringing everyone together to address it. I understand the federal government is passing some form of regulations, is that enough? Is it enough to pass the legislation?

What else can the State do to position itself, and to protect its assets?

MR. KELLERMAN:

Let's first view the protection of assets, security as a functionality of doing business rather than an expense.

That being said, the long term economic growth of the state of Nevada could be tied to cyber security in many interesting ways.

I have worked with Senator Reid and his staff on the new federal omnibus cyber bill. Actually, we went over it for 3 hours last week. That bill is going to recommend that type of testing among other things. It is also going to recommend that five critical infrastructures, finance, energy, essential government services, telecommunications, and managed security service providers not only undergo testing, but they improve their layered security posture. The first mover states that begin to do this will get the grant money from DHS and NSA for various government projects.

Inevitably, there is going to be a paradigm shift globally where major corporations – much like they wanted to outsource operations to India – decide to outsource to the U.S. for security reasons

I will give you an example. Thirty years ago, a company in Lebanon wanted an office in New York City, where they were going to pay \$100 per square foot because they had trust and confidence in the New York market place and they knew they had to be there to be in the U.S. market. I think that same phenomenon will occur in cyber space. We are the safest, soundest marketplace in the world. That will become relevant to a cyber marketplace in the long run for global corporations. The first mover states to improve their legal environment for security and testing and innovation, will be the recipients of those investments.

SENATOR WIENER:

I am going to ask this one question, if I may. I have been privileged to have been a Board member since we started in 1999. I have worked with other members and law enforcement to produce some successful cyber technology legislation. If there is something there is specific that you would recommend – something we could take to the next legislative session, I have bill draft requests left. Our legislature only meets every other year, we are in that stage at present. I would be happy to move forward to take the opportunity to remain on the cutting edge. We have done it before. Last session we did some pretty substantial work. I am poised to offer to do it again. Some of this was difficult, but we got the necessary legislation through. In addition to being on the cutting edge, any follow-on funding would be an additional carrot. I am here to say, "Let's do it." I will do whatever it takes to usher it through.

MR. KELLERMAN:

It heartens me that someone of your stature actually appreciates how the technological issues should become policy issues.

One thing you can do to ensure this on-shoring phenomenon comes from other states and organizations is to secure the managed service provider community here in Nevada, or force anyone who provides managed security or managed services – cloud and so on – to the state of Nevada and anyone else in those critical infrastructure communities, to adhere to, at a minimum, just contractually, changing the security level agreements that have these four elements on the slides would be fundamental to effecting that paradigm shift, as a beginning.

SENATOR WIENER:

If you could do me a big favor, could you provide suggestions, because you and Chris have the tech background, through Jim Earl that would get us started? I will put a bill draft request in so that we can move forward.

MR. KELLERMAN:

Thank you. That would be an honor.

AG CORTEZ MASTO:

Senator, if I might add, I know there were other concerns that Mr. Ipsen addressed as well that might require legislation. If we can put together a working group composed of Mr. Earl, Mr. Ipsen, and if Mr. Kellerman will assist as well, to work on potential legislation, that would be great.

SENATOR WIENER:

Because we are coming up on some deadlines, what would be most helpful now is some manageable language describing the BDR. They give us one sentence to describe the bill. It can be pretty long, but I need something to work with so that I can put the request in, and we can go from there to develop the more specific statutory language.

AG CORTEZ MASTO:

What is the time frame?

SENATOR WIENER:

I could put in a bill draft request today, but I have hit my quota for the September deadline, so it would appear after September. It would be reserved, it just would not appear in the bill draft book.

AG CORTEZ MASTO:

I think there was a question in northern Nevada.

MR. IPSEN:

Actually, I don't think I can top that. That really warms my heart as well. I look forward to working with you, Senator Wiener.

I was just going to comment that security is a business enabler. We encourage businesses to come to the state. That is an important economic issue for all of us, in addition to issues around personally identifiable information.

I am going to take you up on that offer. I cannot express with enough vigor, how much we appreciate having a legislator who is listening and addressing these very complex issues. If there is anything I can do to assist, you have me as much as you need me.

SENATOR WIENER:

I know your number too, Chris. Madam Chair, again to reiterate what we experienced last session with the landmark encryption legislation, we had the full force of the world against us. I can't even begin to list how many large voices were doing everything they could to kill the encryption bill. We had the team working for the best interests of the people of Nevada in our hearts. We made it happen. We will put that same energy into that legislation as well.

AG CORTEZ MASTO:

Thank you, Senator. Are there any other comments or questions? Hearing none, Mr. Kellerman, again, thank you very much. We really appreciated the presentation today. It was very, very informative.

Agenda Item 5 – Update by Robert Cooper, Senior Regulatory Analyst, Consumer Protection Bureau, NV Energy application before the Public Utilities Commission, Advanced Service Delivery Project

AG CORTEZ MASTO:

Agenda item 5 is an update by Robert Cooper on the NV Energy application before the Public Utilities Commission on the Advanced Service Delivery Project, which is the smart electric grid implementation.

Before Mr. Cooper gets started, let me say, he is an analyst in our Consumer Protection Bureau, who assists in putting together filings before the Public Utilities Commission that represent the interests of the state of Nevada. Mr. Cooper, thank you very much. This is a follow-up on the discussions we have had as a Board on the smart electrical grid implementation.

MR. COOPER:

Thank you, madam Chair. As you indicated, our office practices before the Public Utilities Commission (PUC). We represent the residential customers and small business customers of Nevada. We work with energy issues every day. I can not say strongly enough how Mr. Kellerman's presentation really hit the nail on the head regarding energy security issues in general, and, specifically, the importance of these smart meter applications that are currently pending before various public utility commissions all over the country.

I was invited to give a brief update on the status of the Nevada Energy smart meter application that was filed last February. The short answer to that question is that our utility commission will be making its decision next Wednesday at a public meeting that can be watched on the Internet. We will be getting a written order from the Commission thereafter that we will make sure we share with Mr. Earl.

In major decisions like this, the PUC is always very thorough in providing the evidentiary background and the context for its decision. I think that information will be helpful to this Board. Just to touch on some of that context, there were a number of parties that participated in this hearing. It involved several days of hearings in May and June with large energy consumers represented by private attorneys. Of course, our office represents the small consumers. The PUC staff also presented evidence on cyber security issues.

I want you all to know that we took the cyber security issue very seriously. We conducted a national search for consultant to assist us in arriving at our recommendations. We reviewed a lot of potential consultants. We chose Nancy Brockway because she had testified in seven prior proceedings involving smart meter deployments in other states. Also, Ms. Brockway was a former utility commissioner herself in New Hampshire. She was able to put herself in the shoes of our PUC as it makes this important decision – trying to balance several competing interests to arrive at a cyber security plan that will protect the energy consumers in Nevada. Ms. Brockway reviewed all the information, the filings, and data requests.

Her bottom line conclusion was that if smart meters are deployed in Nevada, basically, customer privacy will be at risk. She based this on a number of sources. She filed several pages of written testimony to support her conclusion. Her bottom line was really based on the work of the National Institute of Science and Technology (NIST) that Mr. Kellerman has just referred to. I believe you have also heard about NIST in prior presentations. Her citation was really to work being done by NIST. It involved an earlier version of a NIST document. I think it was called version 1.0, which is probably wise given the rapid changes going on in this area. The document she referred to was called the Roadmap for Smart Grid Interoperability Standards. That document refers to the greatest benefit of smart metering as all the data that the utility will be receiving. It also will be the Achilles heel of the smart grid network – protecting the privacy of that data and the security of that data.

We provided Mr. Earl with a redacted version of Ms. Brockway's testimony. I think you will be glad to know that a lot of the information has been kept confidential. Ms. Brockway did file a confidential version of her testimony as well.

I will say that a lot was accomplished prior to the hearing, and at the PUC hearings, regarding striking a balance between what should be open to the public and what has to be kept confidential for security reasons. Our office prefers that as much information as possible be made available to the public. We understand there are security concerns. Also, third party vendors will stress that their proprietary information be kept confidential. Some of the secrecy was lifted from some of that information. That was actually helpful to the process.

I think you will see a lot of helpful publicly available information contained in the PUC decision when it becomes available in the next several weeks.

The PUC staff filed testimony on cyber security, and certainly, the utility filed extremely important rebuttal testimony addressing some of our cyber security concerns. I think you will be heartened to know that the utility actually recognized a number of our cyber security concerns. In fact, the utility did not take them lightly at all. It filed testimony from William Olsen, their director of infrastructure services, who had submitted the cyber security plan to the Department of Energy (DOE). I think you heard at your last meeting the plan was approved by DOE. Mr. Olsen also addressed some of Ms. Brockway's concerns to the effect that no security system is guaranteed. He was very prudent, I believe, in indicating that by the very nature of the way a company must function, there will be some limited number of individuals with a significant amount of access that could potentially be misused. I think the utility is aware of Mr. Kellerman's precautions and Ms. Brockway's precautions that we filed. I think they realize this is an ongoing issue that they take very seriously.

Just to leave you with one last bit of information as we await the Nevada PUC's decision, I want to mention a decision we received from the Maryland Commission last month. That Commission expressed strong concern about the cyber security risks associated with smart grid deployment. In fact, that Commission rejected the smart grid application of the Maryland utility that was made under similar application to that of NV Energy, where there was over \$100 million of stimulus funds that were brought to bear. That Commission essentially told the Maryland utility to go back to the drawing board. They referred to cyber security as one of the areas of concern.

They indicated, and I am quoting now, "Smart meters are an enormous complex of interconnected networks. Such an extensive network is vulnerable to security risks in many different ways including physical tampering, intercepting or blocking the wireless signals that connect the smart meters to data collection points." They referred to the NIST standards, the NIST document from February of this year entitled *Smart Grid Cyber Security Strategy and Requirements*, and they indicated that these standards remain a work in progress. I think that is probably the best information we can all take from these decisions and from Mr. Kellerman's presentation today. This is all a work in progress. I think we have committed partners in Nevada that are working on this. It is certainly heartening to see this Board taking these issues very seriously.

One last piece of business I have today is to introduce our newest member of the Bureau of Consumer Protection, Dan Jacobsen. He has a wealth of experience – some 30 years of experience in telecommunications matters. Some of you may recognize Dan's name. He was former regulatory manager for Nevada Bell. He was also president of AT&T in Kansas. Dan is going to be a great addition to our smart meter team and also with regard to utility regulatory issues in general.

So, thank you very much for your time. I am happy to try and answer any questions you might have.

ASSEMBLYMAN MORTENSON:

I would like to do a little Internet searching on smart meter vulnerabilities. What is the last name of your consultant and how do you spell it?

MR. COOPER:

Her last name is spelled B-r-o-c-k-w-a-y. We provided Mr. Earl with a public, redacted version of her testimony, filed with the PUC in April. It is a 70-page document that is very wide ranging. I would be glad to help you get a copy of that document.

ASSEMBLYMAN MORTENSON:

Great. I would very much like to get a copy of that – any way you can help me out.

MR. EARL:

Assemblyman Mortenson, I will email you a copy as soon as we break up here. The other document I will provide to you, which is a fairly decent overview, although quite lengthy, is the NIST document that both Mr. Kellerman and Mr. Cooper referred to. That latest version summarizes a number of concerns that NIST has, lays out some of the ways at the national level NIST wants to try and consolidate advice and continue to generate guidelines in the future. You will get both of those as soon as I get back to the office.

ASSEMBLYMAN MORTENSON:

Thank you very much. I really appreciate it.

MR. EARL:

Madam Chair, having mentioned NIST, let me try and place some of these acronym agencies in context.

NIST not only plays in the smart electrical grid arena, it was the NIST standards that Nevada incorporated by reference in the encryption legislation that passed in the last session.

We also heard references today to other federal agencies, or agencies that operate at the federal level.

NERC was mentioned several different times. NERC is the North American Electric Reliability Corporation. It is a group of utility managers. Both Chris and Mr. Kellerman alluded to the fact that the new cyber security person at NERC, Mark Weatherford, has expressed an interest in coming and talking to us about continuing concerns.

One of the other agencies is FERC, the Federal Energy Regulation Commission, I think I have that right. It provides regulation and guidance at the federal level.

One of the large situational problems we face is that although NIST, FERC, and NERC operate at the national level, it is really the state public utility commissions that are responsible for issuing direction, guidance, and levying requirements on the providers of electricity and other utilities within the state. Although there are a number of initiatives at the federal level to provide guidance, and there is some legislation pending before both houses of Congress at the federal level with impacts on NIST, FERC and NIST, one of the things that sometimes gets lost, if you only look at the federal level, is the very important role that state public utility commissions play in the management of the utilities.

In attempt to bridge that type of gap, NIST, very recently, has set up a series of national briefings and participatory sessions. We were informed of the session closest to Nevada, one that will take place in southern California in August, through Chris and Mark Weatherford. I have sent information regarding participation in that event to both Mr. Cooper and the staff at the PUC. This represents an opportunity. Whether we will be able to take advantage given the scarcity of travel funds is another thing. But this is an attempt by NIST to reach out and explain where it sees the smart electric grid going and to establish contact with local providers and regulators.

MR. IPSEN:

Madam Chair, I have one last comment with regard to the submission by NV Energy. At the last meeting, I requested a copy of their cyber security plan. I want to go on record to say that I have received that plan. I am reviewing it. I look forward to future engagements with NV Energy. Hopefully, we can build that collaboration that we already have in the government space to extend to power company in order to work collaboratively to rectify any security issues we might have.

ATTORNEY GENERAL CORTEZ MASTO:

Thank you, Mr. Ipsen. Mr. Cooper, thank you very much for your presentation.

Agenda Item 6 – Presentation by Suzie Block, Network Manager and Information Security Officer – Office of the Attorney General and Teri Mark, State Records Manager, Risks Associated with Multi-Functional Devices [fax copiers] and the State Information Security Committee Response

ATTORNEY GENERAL CORTEZ MASTO:

Moving on to agenda item 6, we have a presentation by Suzie Block, the network manager and information security officer of my office and Teri Mark, the state records manager. They will be talking about the risks associated with multi-functional devices, fax copiers, and the State Information Security Committee Response.

Let me say, this came to my attention thanks to Senator Valerie Wiener. She sent me a very disturbing video. That video was a clip from an interview, and investigative report, done by Katie

Couric. Basically it showed that the contents of hard drives of fax copiers, present in most of our state agencies, when they are no longer needed or returned at the end of an expired rental period or sold some where else, will often contain sensitive documents, still located on these copiers. In particular, this video shows one of these devices was in a law enforcement agency. When the reporters pulled the sensitive information from the device, they found a lot of documents from the law enforcement agency that could be accessed by the public or whoever came in contact with this device.

So, I wanted to bring a presentation to the Board to discuss this. More importantly, Senator Wiener, on the forefront as usual on these issues, has already requested a BDR to address this issue in our state. Senator Wiener?

SENATOR WIENER:

We are in the phase of that one sentence description right now. Initially I looked at this as requiring protection of information stored on the hard drive for the entire duration of custody of the machine. That would affect both business and government. I could see this going to committee and people objecting that it would be impossible to do for the whole time. I am going to start with the issue of prior to releasing custody of the machine, all information on the hard drive must be removed or destroyed. So, if the agency or business could do what they wanted to in order to get it off the hard drive. The bottom line is not to release the machine with any information on the hard drive. I don't care if they dance on it or set it on fire. I am thinking about the public too. I have not seen the Attorney General go white quite that quickly. Her face went ashen when I expressed my concern. I had already put the request in for legislation, and had sent her a copy of the video I had seen on cbs.com.

I am also concerned about the Quick Copy store on the corner, the UPS store, or wherever. People do not have copiers at home and will go there to copy very important information on a public copy machine. This is just open to the universe for use and abuse because information remains on the hard drive.

I watched the video, and called Legislative staff with my next BDR because we have to do something about this. That was my incentive. I shared this with anyone who would listen. I think it is important. Thank you.

ATTORNEY GENERAL CORTEZ MASTO:

Let's hear the presentation first. Mr. Kellerman, if you like, we can ask you to respond as well. Suzie Block and Teri Mark are here to talk about what we are doing at the State level as well as to talk about the problem Senator Wiener identified. So, Suzie and Teri, if you would continue.

MS. BLOCK:

Thank you advisory board members. For the record and minutes, my name is Suzie Block, I am the Information Security Officer and Network Manager for the Attorney General's Office

I have been asked to speak to this Advisory Board regarding risks associated with Multi-Function Devices and the State Information Security Committee Response. I will do my best to explain the technical terminology as part of my discussion.

I would like to provide a definition first. Multi Function Devices (MFDs) are also called multifunction printers or all-in-one devices. These devices have many functions but the majority provide scanning, faxing, emailing, printing and copying functionality. They can help reduce organizational costs and increase employee productivity. However, there are security risks associated with the use of MFDs if not properly configured and secured.

While time and money is spent on securing computer systems, MFDs are often overlooked. Unfortunately, they are computers in-and-of themselves, running an embedded operating system, advertising a variety of network services, and sporting gigabytes of hard drive space. Possible

risks include information leakage from logs (e.g. fax numbers, long distance telephone codes, and filenames), SNMP attacks (a common monitoring protocol), poorly configured network services, and buffer overflows, to name a few. Beyond the network attacks, there is the potential for data recovery, which was mentioned earlier, from an MFD's internal hard drive.

While it might be a standard practice to secure wipe or destroy the hard drives from decommissioned laptops, workstations, and servers, what about MFDs that go in for maintenance or back to a leasing company after an upgrade?

Note that the administration and configuration of MFDs varies widely depending on manufacturer, model, and firmware revision.

I'd like to delve more into some of the security concerns associated with these devices.

MFDs often come with a wide variety of services enabled. Chances are that many of these services are not required in all environments and should be turned off to decrease the attack footprint. Services that these devices support can be broken down into management protocols and services protocols. Management protocols are used for configuring, managing, and monitoring the device, while services protocols are used for printing, faxing, and scanning.

Here are some specific issues. There are certain common web protocols on these devices. For example, a common web protocol for accessing web pages is HTTPM. Many modern MFDs often include an embedded web server for management. While this web server provides an easy-to-use, consolidated interface for managing the device, it is also the Holy Grail for anyone attaching to the device. Among the functions these interfaces typically provide are log viewing, fax and scan mailbox viewing, direct print of Postscript or PDF files, user management, access control list management, network configuration, and other administrative functions.

Just to briefly touch on two other exploits, Telnet is another technical protocol that many of these MFDs provide on their configuration interfaces. It is also used by some older management tools. Telnet access gives a printer administrator a text-based (usually menu-driven) configuration and management interface to that device.

Additional risks posed by Telnet include the following. Although telnet functionality is sometimes limited, compared to the web interface, it can still be used to modify network, password, and access list information, as well as monitor and manage print queues. So, all of the information sent to these devices would be able to be viewed remotely. Telnet is unencrypted and is considered an insecure protocol. Authentication and configuration information is sent in the clear, where it can be sniffed off the network.

Additionally, these devices have access to mailboxes, which are used to store scans, faxes, or templates on an MFD. Unless it is a strong enforced password protected mailbox, a hacker could obtain treasure trove of information. Here they might find entire faxes or scanned documents containing sensitive information.

I would like to briefly recap the challenges, to bring this home to what individual agencies are facing.

Each vendor has different configurations. This can be difficult to support if you need to be conversant on multiple platforms. So, for example, Ricoh, Canon, Kyocera and Xerox all have very different management consoles and configuration options.

Agencies typically purchase these through their fiscal/accounting/administrative staff who are non-technical. So many times the IT department isn't aware that these are being purchased and then staff want the device to be hooked into the network without having the opportunity to review the functional requirements.

Historically, the agencies haven't put into their contracts to retain the hard drives. So, there will be a fiscal impact for each device. That is estimated to be at \$250 per hard drive/MFD. Additionally, escorting outside vendors to work on these devices is required. Because they are technical in nature, we don't want the vendors to have administrative access if these devices are attached to the network. This could provide access into other network resources. A vendor representative could reset all of the security settings that have been put in place. Additionally, we do not want these vendors to remove faulty hard drives because the agency data is retained on these drives. This is why it is important for IT to be available to escort these vendors.

Therefore agencies will have to adopt some type of process into supporting these with IT. IT is extremely busy. I know you are all aware of this. We are always stretched thin and asked to do more with less. So, it will be difficult for agencies that support multiple MFD's in many remote/offsite locations

Next, I will speak to what the State Security Committee and the AG's Office in particular is doing.

We have a Standard that is currently in development at the State Information Security Committee. I believe Chris Ipsen has provided a draft in this meeting for you to see what this consists of. This standard addresses the procurement, configuration, administration and disposition of these type of devices.

The AG's office also has a process in development to address these concerns which includes the consideration of these security risks based on the provided functional requirements and appropriate mitigation strategies before MFD's are implemented. Our office is also including this information as part of our annual security awareness training to educate our staff on these issues.

That concludes my part of the presentation. I would like now to turn it over to Teri Mark.

ATTORNEY GENERAL CORTEZ MASTO:

Mr. Earl, before we get started, I am going to ask that a copy of Suzie's testimony along with that of Teri's as well, be provided to Senator Wiener for assistance in the bill drafting.

MS. MARK:

Thank you, madam Chair. My name is Teri Mark. I am the State Records Manager with the Nevada State Library and Archives, the Department of Cultural Affairs.

Listening to Mr. Kellerman this morning, I was very happy to hear him refer to information as an asset.

We frequently think of information just as records, and we get caught up with the information technology part of it. What is really important is the information and the records.

As the State Records Manager, I have found myself embedded in many IT committees, so that we can look at this not only from the technology perspective, but from the value and importance of the records and the information that is protected and preserved in the records.

Looking at this issue from a records manager point of view, I had to look at how important these MFDs are to our organization and what dangers they pose as well. We know that our personal information is being protected. We know that it is vulnerable to identity theft. As far as printers and copiers are concerned, we are used to being concerned about the printed copy: "Oh, my gosh. Who put blue copy paper in this machine?" Or we casually toss some information into the trash can. That is what we used to be worried about – what ended up in the trash can, and what personal information it contained. Now we are finding out that these MFDs are also maintaining personal information on their hard drives.

It is not just public agencies, such as the Attorney General's Office, that may have these devices in place. We have to look at places where we have public information, such as public libraries. We at the State Records Center have stored information on inactive paper records from all over the state agencies. People come into our agency. What do they do? They don't take the paper back with them. They take a copy of the information and refile the actual record. So, even within our MFDs, we have private information from all agencies. We have to consider how to protect that.

This is something we had not really thought about until the CBS information piece came out. This is a big concern to records management as well – how these devices are being managed and protected throughout our organizations.

We need to make sure that personal information in our care is being protected. That is my concern. If anyone has any questions, I would be happy to answer them.

ATTORNEY GENERAL CORTEZ MASTO:

Teri, thank you very much. Are there any questions?

MR. IPSEN:

I would like to give just a brief overview of what the State Security Committee does. The minute the CBS report aired, very much like Senator Wiener calling the Attorney General, I received calls from perhaps 6 different agencies. One of those calls was from Suzie Block, who identified the issue.

As an example of how the State Security Committee works, we immediately began the process of drafting a state standard to address the issue. The draft you have is very close to being voted on after obtaining input. One of the observations Teri provided in the process was that once information is on a state copier available to the public, we are responsible for that data.

Teri mentioned that she is on a number of technology committees. I end up being on a number of committees that deal with electronic records because there is a close link between us. We are working closely to determine who has the appropriate jurisdiction and who has the ability to manage the problem. That is what we are trying to do – manage the problem going forward. There are benefits to MFDs, but we need to mitigate the risks.

The draft standard you see before you is the most recent version of the standard the State – the Executive Branch and Constitutional Officers – are looking at as a state-wide standard. Both of the individuals you have just heard have been instrumental in pushing forward the standard to address the problem from an agency perspective. After identifying the problem, they moved forward in how to work collaboratively to address the challenge.

ATTORNEY GENERAL CORTEZ MASTO:

Chris, thank you. The final state-wide standard is, of course, something that can be provided to Board members. But more importantly, is that something that is available to the public as well, on your web site?

MR. IPSEN:

Once final, I will make sure it is available to everybody.

ATTORNEY GENERAL CORTEZ MASTO:

If there are no other comments or questions, Suzie and Teri, thank you very much.

Agenda Item 7 – How Implementation of Electronic Document Interexchange Would Be More Secure and Less Expensive

ATTORNEY GENERAL CORTEZ MASTO:

The next agenda item is a discussion of how the implementation of electronic document interexchange would be more secure and less expensive.

MR. EARL:

Thank you, madam Chair. I would like to very briefly provide some definitions and an overview of present Nevada statutory provisions.

In the 1999 Legislative session, the Legislature passed a chapter of the Nevada Revised Statutes entitled "Digital Signatures." In the following 2001 session, the Legislature passed another chapter, 719, whereby Nevada adopted the Uniform Electronic Transaction Act (UETA). That uniform act has subsequently been adopted by 47 states.

To give you a definition of what some of those terms mean, the Nevada statutory definition of "digital signature" means "an electronic signature that transforms a message by using an asymmetric crypto system." That's straight out of the statute. The definition of "electronic signature" means "an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." Clearly, when talking about digital signatures or electronic signatures, and electronic document interchange, we are talking about something much more technologically advanced than the copy of a real-life personal signature that is sometimes attached to or embedded in an email.

When we talk about digital or electronic signatures in the way Chris and I will use that terminology, we are talking about bits of code, which are embedded in, attached to, or associated with a particular document.

The good news is that Nevada has in place the fundamental statutory and legal framework to enable entities to exchange electronic documents and validate them through digital signatures. In fact, certain commercial operations within Nevada, are using this as a means of document exchange. I know, for example, that certain casinos are using electronic documents and digital signatures to exchange high level contracts.

Unfortunately, for a variety of reasons, State agencies and municipal governments have not entered into this particular arena. Chris is going to talk more about that.

There are two fundamental, underlying aspects to electronic document interexchange. First, the parties to the exchange of electronic documents have to agree. This is both a practical and a legal requirement. Indeed, there is a Nevada statutory provision that says, "the provisions of this Chapter apply only to transactions between parties, each of whom has agreed to conduct transactions by electronic means." This is important, for example, so a State agency can not simply decide that it will conduct an electronic transfer. The receiving party has to agree as well, and be set up to receive the electronic document.

The second underlying basis is that the way in which the electronic interexchange system in business has evolved over the past 10 years is that a third party, and perhaps several third parties, called "certifying authorities" are involved. These "certifying authorities" issue and manage the cryptography and identity management that lies behind each digital signature.

So, electronic document interchange is more secure and less costly than paper exchanges. Use of it can be made in commercial, judicial, administrative, and homeland security applications, where an originator wants to move information quickly, securely, and in an authenticated manner.

With that, let me turn to Chris to talk about the contacts he has had with agencies all across the State.

MR. IPSEN:

I want to take a step back. Having worked in technology, I know we can get engrained into the specific technology. We always have to ask, "Why are we even talking about this? Why is this important?"

One of the better examples I can state is that a recent conference, I believe it was last year, at a FEMA conference on protecting critical records. NAAR, the National Association of Archives and Records, put on this particular seminar talking about Hurricane Katrina. During Katrina, a number of records, for example, a deed to a home or an immigration paper that a person might store in their house, might have a duplicate record at a different location – a court or a recorder some where.

When Katrina hit, it wiped out the houses and it wiped out the courts. As a result, there was no record of who owned the property, what the disposition of the person living there was. How about the criminal records of individuals who were detained in jails? All of that information, when it was stored in a physical format was destroyed. There was no way to remedy the specifics of who did what, without extensive and quite expensive means of validating those records.

It really became evident to me that if we could digitize these things somehow and make sure they were authentic, and then share them in some way – maybe encrypt them so people could not see them, but also authenticate who can use them – we can address this problem electronically.

Commensurate with that, a number of agencies have stepped forward and approached me in the last year. They have said, "I know we have talked about digital signatures in the past. I know Nevada will never get to a point where we can use them. But, I still want to tell you my problem. I have a physical record." One of these agencies was the Clark County District Attorney's Office. They said, "Now that we are using federal tax information in some of our processes, the federal regulations say that if I have a physical document, I have to take it out of the file cabinet. I have to document that I took this PII and federal tax information out. I have to put it in a bag. I have to seal it. I have to put it in a second bag, and seal that. I have to transport it to the court, and then I have to take it out of the bags. I have to share it with the court. Then I have to put it back in the bags. I have to seal it up. I have to seal it again. I have to bring it back to the office and check it back in."

As you can see, this is a tremendously inefficient process – especially when the agency moved out of the building where the court was located. When they were in the same building as the court, they could manage it. The requirement for double bagging documents and logging them were not nearly as stringent. But when they moved out, the process became very cumbersome.

This is not just a problem and a process that resides with the District Attorneys, it also occurs in Health and Human Services when they communicate with federal agencies. As we deal with personally identifiable information, we have to come up with a solution.

One solution is to make those documents electronic. We do that because it saves money and because we know we can make it more secure if the proper infrastructure is in place.

One of the things I can not ignore is that when we have an opportunity in an economic crisis is to begin to work on the problem. That is the purpose of this item – to talk to you about the problem, some of the options, and engage the Tech Crime Advisory Board moving forward to effectively engage entities in sharing electronic records back and forth.

One of the opportunities is the Secretary of State's Office has authority over digital signatures. When I scan a document into an electronic format, there is the capability of my signing it to say

that I verify the document I say it is, actually there was legislation in the last session to allow for digital notaries. That was very forward thinking.

Secondly, I need to ensure that as we share these signatures back and forth, if someone is supposed to see it, they see it. And, people who aren't supposed to see the information, don't see it. That is where encryption comes into play. If we can manage encryption, if we can manage digital signatures effectively, and can deal with electronic document management, then what we have is an electronic solution, allowing us to bridge that gap, that deficiency, to provide services to the citizens. Right now, if it is too costly, we can't do it.

That is the fundamental challenge before us. By going to electronics, and doing it correctly, we can be infinitely more efficient. We can make information more available. And, we can ensure that only appropriate people can see the information.

Jim has previously mentioned a number of caveats. One is that there has to be agreement among State agencies to accept electronic records. That includes the court system. I have no jurisdiction over court IT, nor do I want to have that. I am hopeful that, through this Board or other committees, we can establish a framework for collaboration around electronic documents. I have spoken with the Secretary of State's Office. They have the authority to write regulations, but they need to know what those regulations are. If there are technical requirements, we need to know what those are. We need to look at industry best practices nationally.

I want to bring forward that there is a challenge and an opportunity here. When I heard, "We are never going to do this," I told the State administrator who said that, "Well, there is the Tech Crime Advisory Board, so there is a possibility." I see we need to establish best practices around the management of electronic records. We also need to establish legal requirements. If there are gaps in the legislation, they have to be bridged. Not only do we have agreement, we have fundamental requirements that allow documents to be exchanged in a safe and secure manner. I believe that if we capture these ideas, we enable government to do its job more effectively in the future. If we don't do this, we will continue to widen the gap between our capability to deliver services and provide the appropriate future functions of government.

ATTORNEY GENERAL CORTEZ MASTO:

Thank you, Chris. Thank you, Jim. I promised Mr. Kellerman an opportunity to comment. We would love to hear from you.

MR. KELLERMAN:

Both presentations were extremely important.

In the first, I think the legislation you would advocate would involve encryption and deletion. You can encrypt data and delete it to make it more secure when it leaves the hard drive. Or, you can force them to magnetize the drive. Big magnets destroy the data.

Relative to the last presentation, one of the five recommendations to be espoused by the Commission on Cyber Security for the President in a report issued September 1st is the need for two factor authentication, PKI and digital signature infrastructure.

But I would advocate that you follow the Asian model. Instead of having a private company become the certificate authority, have the DMV become the certificate authority. You could also generate revenue for the State if you have the DMV become the certificate authority. They are already in charge of identities state wide as they exist now.

Those are my two comments.

ATTORNEY GENERAL CORTEZ MASTO:

Thank you very much. That is great input.

Let me ask this of members of the working group. Chris, if we can identify a key stakeholder group for electronic documents that we can pull together to start exploring the issues you brought up, could that be brought back to the Tech Crime Advisory Board on what we can do for best practices and legal requirements, who would you be able to identify as stakeholders?

MR. IPSEN:

I think it absolutely essential that we include county, city and State government officials, the Secretary of State's Office, given their authority, Teri Mark as the State Records Manager. We probably want to reach out to a federal stakeholder, because we do want to do electronic interchange with the federal government. I think we also need to reach out to the private sector. Just a few days ago, we announced the kick off for the Secretary of State's business portal. It is a very important and positive move forward for the State. We should possibly also incorporate our interfaces with the citizens and the businesses. As the requirements are defined, we want to have the appropriate controls in place to ensure the data is maintained. Those are the entities.

If you like, I would be glad to get in touch with a number of stakeholders, reach out to them, and come back with a list of individuals, or supply it to Mr. Earl, and make some recommendations and proposals going forward.

ATTORNEY GENERAL CORTEZ MASTO:

Okay, that would be great. Do any Board members from the federal government have any thoughts on who we should be reaching out to? I don't want to put any of you on the spot.

U.S. ATTORNEY BOGDAN:

You probably want to contact ICE, the Marshall Service, the FBI, our office.

ATTORNEY GENERAL CORTEZ MASTO:

Chris, I think you heard that. Thank you Dan. If there are no other questions, let's move on to agenda item 8.

Agenda Item 8 – Board Comments

ATTORNEY GENERAL CORTEZ MASTO:

Are there any Board comments? If not, let's move on to public comments.

Agenda Item 9 – Public Comments

ATTORNEY GENERAL CORTEZ MASTO:

Are there any comments from members of the public here in the south that would like to address the Board? Seeing none, are there any members of the public in northern Nevada who would like to address the Board?

MR. EARL:

Yes, Madam Chair. Ira Victor would like to speak on one of the agenda item issues.

ATTORNEY GENERAL CORTEZ MASTO:

Welcome, Ira. I did not realize you were there.

MR. VICTOR:

Thank you, Madam Chair. I am here as president of the Sierra Nevada InfraGard Member Alliance and also as a subject matter expert on information security.

The issue of data on MFDs is very important to our members. We want to support Senator Wiener in her efforts to protect business and government in this area. I want to throw our hat in support of this initiative. We have InfraGard member from both the public and private sectors. I think we can help with expertise as this bill gets developed.

ATTORNEY GENERAL CORTEZ MASTO:

Ira, thank you very much. You have always been there to help us work through these issues. We really appreciate your continued support.

MR. VICTOR:

Thank you, Madam Chair.

ATTORNEY GENERAL CORTEZ MASTO:

Are there any other members of the public who wish to address the Board?

MR. EARL:

I see none, Madam Chair.

Agenda Item 10 – Scheduling future meetings

ATTORNEY GENERAL CORTEZ MASTO:

Item number 10 is the scheduling of future meetings. Are there any recommendations other than continuing to rely on Mr. Earl for scheduling as we have in the past? Sounds like we will continue to do so. Mr. Earl, do you have anything to add at this time with regard to future meetings.

MR. EARL:

I do have one issue – whether to plan on one meeting or two before the commencement of the Legislative session. I see two possibilities. Either we hold a single meeting, perhaps the first or second week in November. Or, alternatively, we hold two meetings, one of which would be in September and the other later in November.

ATTORNEY GENERAL CORTEZ MASTO:

We may hit Thanksgiving if we have one later.

MR. EARL:

Yes, that is true. Since the Legislature convenes in early February, one of the constraints we did not have last year is that these facilities are likely to be unavailable to us after the first of December. That needs to be taken into account as well.

ATTORNEY GENERAL CORTEZ MASTO:

Okay. Are there any other questions or comments? Hearing none, agenda item 11 is adjournment.

Agenda Item 11 – Adjournment

ATTORNEY GENERAL CORTEZ MASTO:

We are adjourned at 12:03 PM.

Respectfully submitted,

James D. Earl

Approved by the Board at its subsequent meeting on November 18, 2010.

Minutes of the Technological Crime Advisory Board

November 18, 2010

The Technological Crime Advisory Board was called to order at 10:03 AM on Thursday, November 18, 2010, Senator Valerie Wiener, Vice-Chair, presided in Room 4401 of the Grant Sawyer Building, Las Vegas, Nevada, and via videoconference in Room 3137 of the Legislative Building, Carson City, Nevada.

ADVISORY BOARD MEMBERS PRESENT:

Keith Munro, *meeting designee for 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
Russell Marsh, *meeting designee for Daniel Bogdan, U.S. Attorney, Department of Justice (DOJ)*
Special Agent in Charge Kevin Favreau, Federal Bureau of Investigation (FBI)
Assistant Sheriff Mike McClary, *meeting designee for Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)*
Captain Tim Kuzanek, *meeting designee for 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

ADVISORY BOARD MEMBERS ABSENT:

Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association
Resident Agent in Charge Greg White, U.S. Immigrations & Customs Enforcement (ICE)

TASK FORCE MEMBERS PRESENT:

Sergeant Kevin Skehan, Las Vegas Metropolitan Police Department
Sergeant Troy Barrett, Las Vegas Metropolitan Police Department
T.V. Davis, Attorney General's Office

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director

OTHERS PRESENT:

James R. Elste, Symantec
Paul Genco, Washoe County Sheriff's Office
Chris Long, Washoe County
Rick Vandenberg, City of Reno,

Jeff Seifers, Intuit
C. Kerry Nemovisher, C. Kerry LTD
Susan McCarthy, Prepaid Legal
Teri Mark, Nevada State Library and Archives, Department of Cultural Affairs
Mischel Kwon, Mischel Kwon Associates
Brett Windle, City of Carson City
Joe Gallegos, Attorney General's Office
Cory Casazza, Washoe County
Ira Victor, InfraGard
Del Roehrick, SAIC
Theresa Presley, Department of Health and Human Services, Health Division
Ernie Hernandez, Department of Health and Human Services, Health Division
Lois, Hale, InfraGard
Laura Fucci, Clark County
Joe Marcella, City of Las Vegas
Chris Wilding, City of Henderson

Agenda Item 1 – Call to Order – Verification of Quorum

SENATOR WIENER:

This meeting is called to order on November 18, 2001 at 10:02 AM. Mr. Earl, would you please call the roll?

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

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

SENATOR WIENER:

If there are any modifications of the minutes – we've had chance to review them. We do have several proxies present who are pinch hitting. If there are any modifications, would you please bring them to Mr. Earl's attention at this time.

If not, I will entertain a motion to approve the minutes.

Motion to approve the minutes by Mr. Norton and seconded.

The motion to approve the minutes was approved unanimously.

Agenda Item 3 – Reports regarding Task Force and Board member agency activities

SENATOR WIENER:

Item number 3 of the agenda is a standing item on our agenda since the beginning, asking for updates on what is going on in law enforcement. We normally start with the FBI.

SA SCHROM:

Good morning, Board members. My name is David Schrom. I am a special agent with the FBI in Las Vegas. I am the primary relief supervisor for the cyber squad. I am here representing Supervisory Agent Eric Vanderstelt. I am also the FBI coordinator for both InfraGard chapters within the State of Nevada.

Since our last meeting, we have had a number of accomplishments in our cyber crime related investigations.

Examples include, in July, a man was sentenced to 21 months in federal prison and ordered to pay restitution. He had gained unauthorized access to the computer network of a mortgage

lending company and utilized the stolen customer data to assume others' identities and obtain cash advance loans. Also in July, a man was sentenced to five years in federal prison after pleading guilty to receipt and possession of child pornography.

In August, a man was sentenced to ten years in federal prison after his conviction at trial on coercion and enticement of a minor. In August, a man was sentenced to more than 17 years in federal prison pursuant to his conviction for receipt of child pornography. This individual had a prior conviction for sexual assault of a child. In August, two men were sentenced to two years imprisonment and ordered to pay restitution for their involvement in criminal copyright infringement and trafficking in counterfeit slot machines.

In September, a foreign national was arrested on charges including conspiracy to commit access device fraud and aggravated identity theft. Also in September, a man pleaded guilty to coercion and enticement of a minor. He faces a mandatory minimum sentence of ten years in federal prison.

Lastly, in October, a man entered a guilty plea to receipt of child pornography and faces a five year minimum mandatory sentence. That is all I have.

SENATOR WIENER:

I have a question. I have done a lot of work as a legislator in identity theft issues. I have not heard the term "aggravated identity theft". Would you please explain what that is?

SA SCHROM:

Aggravated identity theft is a newer charge. I believe that Mr. Marsh may be better able to explain it. Whenever an individual commits an identity theft and, I believe Mr. Marsh may have the exact particulars, but it involves a mandatory sentence of two years in addition to whatever other crimes were committed.

MR. MARSH:

Madam Chair, this is a fairly recent federal law. It was passed and took effect in the last five years. It provides that, in cases where people have committed identity theft to facilitate other federal crimes, there is to be a consecutive two-year sentence, which can not be suspended. There is no allowing for probation. It has been a very effective tool for us on the federal side in combating identity theft.

SENATOR WIENER:

Any questions for the witness, committee? Thank you very much.

Again, history often sets the stage for us. We generally go to Washoe County to get a report about what is going on up there.

CPT KUZANEK:

Thank you Madam Chair. This is Tim Kuzanek with the Washoe County Sheriff's Office. Dennis Carry, a detective from our agency who normally reports to this body, is not here today. He was called away this morning. He reported to me that, since the last meeting, numerous warrants have been served. All of them relate, pretty much, to child pornography cases. There are a number of intrusion investigations that the Sheriff's Office is working in conjunction with the FBI. Forensic investigations have increased a great deal since the last report as well. They are generally related to proactive investigations that the Task Force has been involved in. That is all I have.

SENATOR WIENER:

Any questions? Thank you.

Are there any other interested parties who would like to come forward and provide updates?
Please come forward now.

ASSISTANT SHERIFF MCCLARY:

Madam Chair, I would like to call on Sergeant Kevin Skehan and Sergeant Troy Barrett from Las Vegas Metropolitan Police Department's (LVMPD's) computer forensic lab and our Internet Crimes Against Children (ICAC) Task Force.

SENATOR WIENER:

Thank you very much. Again, please identify yourself for the record and proceed.

SERGEANT SKEHAN:

Good morning, Board. My name is Sergeant Kevin Skehan. I am a sergeant with the computer forensics lab of LVMPD. My partner...

SERGEANT BARRETT:

I am Sergeant Troy Barred, LVMPD, ICAC¹ detail.

SERGEANT SKEHAN:

Historically, the unit I supervise has evolved – from the cyber crimes unit to the electronic crimes unit, and, as of March 1st of this year, we created the computer forensics lab.

What we noticed was that the primary function of providing forensics to the agency was having some issues when it came to dealing with some ICAC cases, specifically, in undertaking prosecution of these cases and waiting for computer forensics to be completed.

We noticed – and Sergeant Barrett will also speak to this – that there was a year and a half backlog of cases. This was unacceptable. We put together a fairly comprehensive plan in which we took existing resources from both my unit, which at the time also included SWIFT, the South Western Identity Theft Task Force. We left them in place. We took the forensic examiners from my unit and merged them with the forensic examiners from Sergeant Barrett's unit to create the computer forensics lab. Its charge was simply to keep up with current forensic case load and to eliminate the backlog.

We now have seven sworn examiners in the computer forensics lab, all working for the police department. We have one civilian examiner as well who provides assistance.

Turning to our year-to-date statistics, we have 202 individual cases that have come through the office. We have examined 580 devices, and have processed 30.2 terabytes of data. That is a significant increase over anything we have ever experienced.

We expect, in approximately three weeks, to be 100% complete with the backlog of ICAC cases. We are in the process of attaining our goal – a 30-day turnaround on the cases that come into our office that require processing for either forensics or intelligence purposes.

Our role is to fulfill a critical support function for the entire community, so that we can turn our cases – virtually any crime you can think of – back over to the primary investigator within that 30-day period.

We tell everyone that 10 years ago cyber crime was a novel concept. It was novel because it did not impact everybody. We have migrated away from using the term “cyber crime” because it really is just every crime. Every single section, bureau, division of our agency has been impacted by how technology changes how our work – how technology supplements bad guys in the crimes they are committing.

¹ Internet Crimes Against Children.

We have evolved beyond “cyber crime” to an “every crime” concept. We know it is a critical function of the agency to be able to provide this type of support, and get prosecutions using the evidence we are recovering.

We also provide technical assistance to the agency, and we put together a response team to respond to unusual circumstances that require immediate technological assistance for recovering evidence or intelligence as devices that access the Internet continue to converge, whether they are smart phones or whatever else. These devices really play a significant role in identifying suspects and potentially resolving deadly situations.

We pretty much think of the Internet as nothing more than an operational environment for bad guys. We look at these handheld devices as the instrumentalities of their crime. We are pushing in that direction. We are pushing to really support the ICAC mission, which is why we fall under the ICAC section. Troy will talk more about that.

SERGEANT BARRETT:

Traditionally, when you have a year and a half backlog, you will serve the search warrant, and, if you make an arrest, the District Attorney, or if you go federally, the Assistant US Attorney (AUSA) will require the examination be presented for the case. However, if the backlog is a year and a half, you can't provide that.

So, the arrests were being delayed. You can imagine a search warrant being done, and the subject remaining in the residence, free to do what he likes for up to a year before we could come back with some sort of consequences for his actions.

The perception of the bad guy is, “I got away.” He might get another computer. We have multiple cases where, in the interim, the subject got a second computer and started committing their acts again.

The perception of society is, “If they are dangerous, why are you letting them be out there?” So, working together, we have addressed this issue and have reduced the backlog down to an unprecedented 30 days. If you do any type of research throughout the nation, a one-year backlog is not unheard of. So, we are setting a standard and holding those accountable, and having some serious repercussions for those that choose to go ahead and do these acts.

The additional benefit is for the computer examiner. My examiners were looking strictly at child pornography. This is an easy term to say – “child pornography.” But when you think about what they have to view and the details they have to record, for instance, “at minute 1:03 into the video, the adult then touched the child in this manner” – that is a lot for someone to have to deal with.

As a result of teaming up, having a big team available, Sergeant Skehan is able to take a forensic examiner out of child porn images for a little bit to, maybe, work on a robbery or a homicide. This gives them a mental break for the constant viewing of children being raped. As a result, the burn out factor for computer forensic examiners is greatly reduced. Remember, the training to get a computer forensic examiner up to speed is 2 years. We are not going to lose that individual now. Due to what we have done, we are able to keep those computer forensic examiners on the team and continue to be productive detectives.

SENATOR WIENER:

You mentioned that cyber is just part of bad guys doing business in every environment. Early on, a lot of our work had been done in the child pornography arena. In the new normal, where you have alternative crimes for examiners, how much is still child pornography of the work you are doing?

SERGEANT SKEHAN:

Twenty-four percent of my current caseload is child pornography. The majority of our cases, what we are seeing because of the convergence of devices, are such things as homicide cases that are being put together by very good investigators that are bringing us GPS units that the bad guys are using to navigate to the victim's addresses. Although a lot of this data is encrypted, we are working with the manufacturers, and after getting appropriate court orders, we are able to decrypt this data and look at log files and track files. In several cases we have had this year, we have been able to put the suspect at the scene of the murder exactly at the time it occurred because of these technologies. So, we are seeing an enormous increase in requests from units like homicide, robbery, vice – given the way these bad guys are doing business these days, they don't bother keeping the old written things. Everything is going to these devices. They are able, not only to take down information, but they are able to access the files that they are storing on the Internet. They are able to immediately upload video. You are going to see another explosion in the amount of use of these devices as the networks get faster and faster.

Right now, we are only limited by bandwidth. Most of the major carriers will allow sufficient speed to do some limited video conferencing. Other carriers require that you have a faster pipe – through a Wi-Fi connection, for example. That is all changing. With the latest networks and the latest network architecture, you have the ability to do real time, full 30 frames a second, digital video conferencing back and forth. On the fly. Anywhere.

As this matures, you are going to see these devices used for all types of criminal activity, from the planning and commission of simple robberies to more complicated robberies. We have a case now where a suspect actually recorded the homicide he committed. You will see more and more of this.

It gets more complicated. It is not just local device storage we are talking about. It will involve taking these images and uploading them into what we call "the cloud". That is essentially an array of servers. Tracking that down for police and evidentiary purposes becomes a challenge.

SENATOR WIENER:

I noticed that earlier in your statement you mentioned how many cases you had and how many devices you had gone into. Even now, you have cases where you have multiple devices?

SERGEANT SKEHAN:

Absolutely.

SENATOR WIENER:

So, even at this primitive stage, you are often dealing with multiple equipment for each crime?

SERGEANT SKEHAN:

Yes.

SENATOR WIENER:

Any questions, committee? If I slip into the "committee" terminology, that is how I am used to serving as a chair. I am not used to being on a board as a chair.

ASSISTANT SHERIFF McCLARY:

Can you briefly address the change in the operational environment when we did computer crime, or cyber crime, 10 years ago? Contrast that with what you are dealing with now – going away from desktop PCs to more hand held devices. You have spoken a little about the current operational environment from both the ICAC and overall criminal perspective. Can you give the Board some sense of what you see coming in the near term – the next year or two? What will the operational environment be for law enforcement?

The second thing I would ask you to do is to provide to the Board the very well crafted document you provided to me that explains the operational environment of stand-alone forensic labs today, and why that is best practice? This goes both to what we are seeing in litigation, but also it includes some of the things Sergeant Barrett mentioned – particularly giving ICAC investigators a chance to take a breath and step away from a very emotional investigative venue.

So, if you would expound a little on the piece about where we are headed, and, second, I ask you to provide to this Board the document you supplied internally to LVMPD so we can make it part of the record, allowing Board members to look at that in the future.

SERGEANT SKEHAN:
Absolutely.

Here is where I see things going in the future. A lot of it has to do with expectations that the public has. When we have a major event in Las Vegas – and this year we have had several significant events – major crimes, uses of force, or whatever. The public expects that the police department has the tools, skills, and abilities to retrieve evidence across multiple different platforms. This could be electronic evidence stored on cell phones, or electronic evidence as digital video. Every major corporation has embraced the concept of using digital video because it is fairly inexpensive as compared to what it used to be. It helps when it comes to loss mitigation – when someone makes a claim that they were injured on the property, for example.

The other side of this is that this information is now critical to investigations we undertake. These may be violent crimes, unusual circumstances, or whatever it turns out to be.

Any police agency, not just the lab I run, but the entire agency needs to have the knowledge and skills to identify digital evidence, to be able to know how to properly handle digital evidence and preserve it, and be able to process it so that it can be brought into court in a way that does not compromise it as evidence.

As technology evolves, many things will get a lot cheaper. As technology gets cheaper, it gets more widely adopted.

We see an evolution from a few guys running a cyber crime office to an entire agency of technically astute, technically literate, capable investigators that know the difference between a phone number and an IP address. They need to know how to identify where the best source of evidence or information resides. They need to understand that bad guys are just like everybody else – if they have easier ways of doing things, they are going to use them. We need to be able to exploit that.

Gone are the days of just being able to go out and take a crime report, take a few notes, and prosecute a suspect.

If you are not looking at the digital evidence associated with the crime, you are not doing your job in the best manner possible. We will see, probably over the next year or two, a lot of emphasis put on training – particularly relating to the technical side of law enforcement. This just has to take place. We have to embrace this. It is a phenomenal source of information and intelligence.

SENATOR WIENER:
That training would be down to the first responder because that is where the information gathering occurs?

SERGEANT SKEHAN:

Absolutely. And it really has to be at that level. The reason is that concepts we never heard of years ago, such as Faraday containers², and being able to remotely wipe devices – these are all commonplace now. If you buy a standard smart phone, it comes with the ability to send a command to the phone to remotely wipe it. As law enforcement, we want to preserve this evidence, just as we preserve any crime scene. The way we do it is by placing the device within an electrically shielded container to prevent the signal from getting to that device.

Understanding basic concepts like this – going to how to properly preserve evidence – is going to be critical.

SENATOR WIENER:

Thank you. Are there any additional questions or comments?

SERGEANT SKEHAN:

Another consequence of the computer forensic lab deals with personnel. Before, I had two active investigators, and my other two detectives were forensic examiners. With a year and a half backlog, I had to pull in the reins on the proactive side. If they continued to be active, they would just create a larger backlog.

Now, with the creation of the computer forensic lab, and the turn around time of 30 days, the reins are off. My proactive investigators can go out and get as many bad guys as they can get their hands on. This provides wonderful encouragement for these detectives. They became cops because they wanted to get bad guys. They love getting guys who prey on children. So, our new method of operations has opened up everything for us.

I know we have told you before, the amount of work out there is utterly amazing. Just in my area of jurisdiction, Clark County, I took a snapshot of 20 hours, and asked, in that window, how many people are going to be going on the Internet and sharing child pornography? I had over 50 contacts in 20 hours. This involved 50 different IP addresses, at different physical locations, were looking for and sharing child pornography in 20 hours.

The questions this raises are: How many bad guys couldn't get on line in that particular 20 hour time? How many would be working, or not have the day off?

If you gave me ten additional detectives, I would have work for them. We are presently dealing only with those at the top of the list. I don't think we are going down far enough. But, due to the creation of the lab, the reins are off, and my two investigators are doing a smash-up job. That's what all of us are here for.

MR. IPSEN:

First of all, I would like to say, with as much veracity as I can, I really applaud this effort. That is a significant achievement. My hat is off to LVMPD – particularly in light of how much work is required to do effective forensic analysis. It is also important to note that when you do good forensic work in the digital world, it sticks. I just want to say "great job" in light of your achievement.

Second, a couple of other points occurred to me. I do not know if they have been emphasized sufficiently. Criminals are becoming aware of the fact that IT is a business enabler. It makes their

² A Faraday container, cage, or shield, is a device (perhaps an entire room) to block or greatly attenuate a static electrical charge or field. In context, a Faraday container is used in police and intelligence work to prevent a cell phone or similar device from receiving a signal. This is often necessary after a cell phone has been seized to prevent a signal being sent to the cell phone that causes the erasure or corruption of data contained in storage or active memory within the cell phone.

job a lot easier. The more IT criminals use is reflective of the greater world that emphasizes IT. It also reflects the importance of cyber security in all aspects and lines of business.

I think the FBI would likely concur that the types of crime, the amount of white collar crime, will not decrease, but increase. I am proud to be a Nevadan, knowing that you have the capability you do.

From the Office of Information Security standpoint, we would love to collaborate with you. This is a great achievement. Thank you for your work.

SENATOR WIENER:

If there are no additional questions, thank you, gentlemen, for the good work.

If no one else wants to speak to Agenda Item 3, we will move on to Agenda Item 4.

Agenda Item 4 – Presentation by Teri J. Mark, State Records Manager, (1) Securing public records during Government Transitions, and (2) Issues associated with allowing state agencies and local governments the option to declare the electronic copy as the official record for retention purposes.

SENATOR WIENER:

Teri, thank you for the work you have been doing and the work you continue to do, although I kind of loaded you up a bit with one of my bill drafts. We know we are moving forward on several measures. We look forward hearing what you have to say.

MS. MARK:

Thank you very much, madam chairman and members of the committee, for inviting me here today.

I a couple of issues as you said concerning public records in Nevada.

First, I would like to talk about government records during transition. As you are aware, government executives create and maintain public records as part of their official responsibilities. These materials may appear in paper, electronic, or other formats. Regardless of the physical form, however, or characteristics of the record, the recorded information is a public record if it is produced, collected, received, or retained as required by law or in connection with the transaction of public business.

By state statute, NRS 378.290, the

...records of the Governor's Office, which include correspondence sent or received by the Governor or employees of the office in the performance of governmental duties, are the property of the State of Nevada and must be transferred to the [State Archives] before the Governor leaves office.

The transfer of these records ensures that the accomplishments of this governor and previous governors' administrations will be documented and the material preserved for history.

Traditionally, we expected the records to be paper records; however, we are experiencing the great shift to electronic formats. For example, four years ago when Governor Guinn left office the State Archives received well over 900 boxes of paper records. The State Archivist, Jeff Kintop, and I met with Governor Gibbons's transition team a few weeks ago, and while they have a large quantity of paper records, they will also be transferring 70 – 90 gigabytes of unstructured electronic records and emails to the State Archives.

While Governor Guinn's staff printed out every official email and filed the communication in a file folder, Governor Gibbons's staff electronically preserved each email account and every email sent or received within each account for transfer to the State Archives. This adds a new level of complexity for the State Archives and highlights the necessity for the establishment of a digital archive within this State.

While we do not have a statute requiring the transfer of records by Constitutional Officers or department heads, these individuals do have an obligation to protect and preserve records that provide evidence of their decisions and of their agency's functions, organization, policies, programs, and activities, compliant with NRS 239.080, which states that

official state records may be disposed of only in accordance with a schedule for retention and disposition approved by the [State Records] Committee.

It is the advice of the State Library and Archives (NSLA) that state officials know and understand the importance of proper record keeping, thus ensuring a smooth transition and adequate maintenance of the public records within their offices. In the next couple of weeks, NSLA will be distributing a memo to all government officials reminding them of this obligation. This memo will highlight the best practices of transitioning out of office, specifically dealing with issues of wrapping up the business of the present administration and then turning to the tasks necessary for preparing for the new administration.

Generally, any records created or received in an official capacity are public records and not the private property of the office holder or appointee. The statutory definition of a public record in Nevada is rather vague, stating that

all public books and public records of a governmental entity, the contents of which are not otherwise declared by law to be confidential, must be open at all times during office hours to inspection, NRS 239.010.

On the other hand, NRS Chapter 239, for the purposes of records retention, does define Official Records, albeit in a rather antiquated way, as

any: (a) Papers, unpublished books, maps and photographs; (b) Information stored on magnetic tape or computer, laser or optical disc; (c) Materials which are capable of being read by a machine, including microforms [also known as microfilm] and audio and visual materials; and (d) Materials which are made or received by a state agency and preserved by that agency or its successor as evidence of the organization, operation, policy or any other activity of that agency or because of the information contained in the material. (NRS 239.080(4))

NRS Chapter 239 establishes the records retention requirements for state government. There are approved retention schedules for most of the types of records an office maintains. We have the general retention schedule, and the agency-specific retention schedules. Most of these records may have continuing value to the officer or his or her successor.

In addition, there are groups of records that are identified in the retention schedule that have historical value. In the last couple of years, we have seen and over the next few years we will see more government restructuring. All of the records that document this restructuring will be of significant interest to future officials and researchers. They are going to want to look back at what worked and what did not work. What happened? We need to have those records available. It is extremely important that the official records documenting this are collected and preserved by the agencies so that the records remain persistently accessible.

Since most of these records are born digital and will more than like be maintained and preserved digitally, it is extremely important that government officials ensure that the records of their agency

are organized, categorized, identified and tagged according to their retention value. These records will explain how the agency formulated and executed significant program policies, decisions, actions, or responsibilities.

Government officials have a legal obligation to ensure that the agency establishes and follows appropriate records creation and maintenance procedures – this includes the paper record AND the electronic record. That should be transparent. It does not matter what the format is. We will look at the record and the content. Good recordkeeping best practices include:

- Contributing to the smooth operation of an agency's programs by making the information needed for decision making and operations readily available, facilitating transitions between administrations.
- They want to create a complete record of the official actions that will remain within the agency for future use by agency officials and eventual transference to the State Library and Archives as a historical record.
- To ensure accountability to the administration, the Legislature, and all Nevada citizens.
- To ensure that electronic records will be available to all authorized personnel
- To protect records from inappropriate and unauthorized access.
- And, to facilitate authorized removal of materials by avoiding the need to separate public records from extra copies of records and personal materials when a director leaves office.

The next part of my presentation deals with a BDR we have before the Legislature. Do have any questions for me regarding securing records in transition?

SENATOR WIENER:

Teri, you mentioned early in your remarks that since a lot of information coming to you is electronic, what would it entail for you to establish facilities to retain this? You are used to paper records – the nine gillion boxes you received – now, you are getting a mix. You mentioned you need more capacity, would you explain that? What might that entail?

MS. MARK:

Yes. We have to start looking at the digital archive. We know we are going to enter a digital dark ages if we do not start protecting the digital record in the State of Nevada.

The digital archive is a process that retains the record electronically. It has multiple redundancies of the copy. Also, it provides for the forward migration of that copy, or, at least protecting it in a format that can be read by future generations. Unfortunately, none of us has a crystal ball that will allow us to peer 20 years into the future to determine what type of format records will be in and how we will want to see these records.

We can look back 20 years in the past, and we know we have lost a lot of the digital records that were created 20 years ago because they were not properly retained. Or, perhaps, they were retained in such a format that they can not be accessed today. We have records in all sorts of formats that are unreadable today because they have been abandoned by past technologies.

The digital archive protects a record through redundancy. Unfortunately, our State Archives does not have the capacity to do this. We are working with the Washington State Archives. They have developed a digital archive. We are partnering them with several other states, including Oregon and Indiana, to store digital records. We would either protect the record in a manner accessible to the archivist or accessible to the public, depending on the type of record it is.

Did that answer your question?

SENATOR WIENER:

Yes, but I am still concerned about that crystal ball and whatever protections we offer today that will allow us to avoid having to say "Oops, we can't read this." Any additional comments or questions?

MR. MORTENSON:

I am surprised to hear you say you have lost digital records from the past because you don't have the equipment to restore it or bring it forward or something. That old equipment exists everywhere. I'll bet I have equipment that will go back as far as anything you have digitally. So, it's hard for me to believe that you have lost any digital data irrevocably.

MS. MARK:

Unfortunately, the format may not persist because it is written on a CD where the CD is damaged. CDs are not permanent formats. You can pull out a commercially produced CD and find that it is skipping over things because it has not been well maintained.

It could be in a format that we no longer have the software for. You may have the old zip drive, but you may not have the software to process it. You may get a data dump if you are lucky and the magnetics are still good. So, often it is the sustainability of the media itself that determines whether a record can be accessed.

MR. MORTENSON:

I understand how CDs can be damaged. Thank you.

MR. IPSEN:

I have a question that goes to the authenticity of documents in electronic format. Do you see any challenges going forward with respect to verifying whether the documents you have are authentic?

MS. MARK:

Yes, and I will be addressing that in the second part of my presentation. Is it OK if we hold onto that thought?

SENATOR WIENER:

Why don't we let you go ahead then and proceed with the second part?

MS. MARK:

Thank you, Madam Chair. Currently the Department of Cultural Affairs has a Bill Draft Request (BDR) before the Legislature to address an on-going concern of State agencies and local governments – recognition of the electronic record as the official record for retention purposes.

We are specifically looking at NRS 239.051, which allows governmental entities to take a paper copy, convert it to microfilm and then to preserve the microfilm as the official copy, or as the statute calls it "microphotographic film" or, if the information is entered into a computer that permits the retrieval and reproduction of that information. This basically means taking data and entering it into data processing as was done in the 1980s, and recognizing that the official record is then the electronic version – although it is not looking at the imaged copy or the born digital record as the official record.

More local governments and State agencies are looking to us to allow them to retain the electronic record as the official record. The concern is always the authenticity and the integrity of that document. We must ensure it is retained in a system so that at the point of transaction, when the document is signed, when the correspondence is sent, when the contract is signed, when the report is published, no one can thereafter go in and modify any of the information after the fact.

What we have proposed is updating the language in NRS 235.051 by adding the following text at the end of the first subsection:

only if those records or writings have been placed on microfilm and may be reproduced as an image in an electronic recordkeeping system which permits the retrieval and reproduction of the records or writings. A reproduction of that film or image shall be deemed to be the original.

2. The reproduction shall be durable, accurate, complete and clear, and maintained in such a manner and place as to protect it reasonably from loss or damage; and so reproducing the original shall have the same force and effect for all purposes as the original record whether the original record is in existence or not. The reproduction shall be deemed for all purposes to be a certified copy of the original record. Such reproductions shall be preserved in the place and manner of safekeeping prescribed by the Nevada State Library and Archives Administrator under NRS 378.255.

We, the State Library and Archives, will then write the regulations that will identify how to protect the record so that it preserves its authenticity and integrity. So, we are looking at the authority the State Library and Archives Administrator has under NRS 378.255 in order to write standards and best practices.

We would go on to add a new subsection 4 to the effect:

4. Images reproduced in an electronic recordkeeping system must meet the standards adopted by the Nevada State Library and Archives Administrator under NRS 378.255 (1).

That is our proposal – to recognize the electronic record with the caveat that good record keeping practices must be maintained as well. As you know, so many records are now scanned or resaved, and there is no record keeping police overseeing the records to ensure their authenticity. Chain of custody may be lost for some of these records. We want to make sure that we have an audit record of anyone who has modified or changed a record. We want to know when it happened and who has authorization to do anything with that record.

Many of the electronic record keeping programs that are available have a module that can be added so that when the record goes from a document, and it is in version control, and is preserved as the official record, it is an uneditable copy. So, no one could edit it without the proper authority to do so. And, there needs to be a retention schedule attached to it so we know how long we need to retain that record and how we have to protect it. If it is a three-year retention period, we can probably keep it in almost any type of format, and it will still be accessible for its life time. If it has a 30-year retention period, you have to exercise some additional care to ensure it will be accessible for the full 30 years. Or, if it is a permanent record, we have to ensure it is transferred to a proper record keeping agency. State agencies can transfer it to the State Archives to ensure the record is persistently accessible for the life of the State.

Are there any questions?

SENATOR WIENER:

Teri, authenticity is critical. You mentioned editing late in your remarks. I have grave concerns about editing a document that has already been authenticated. If it has been edited, it becomes a new document.

MS. MARK:

Exactly.

SENATOR WIENER:

If there is a capacity to edit, I have very serious concerns about that occurring. I would think that if you are tracking a document, and it changes, then you have two documents. This might come to a committee I might be serving on in the Legislature.

MS. MARK:

Right. That was a misstatement by me. I apologize for that.

SENATOR WIENER:

I was just very concerned. Any additional comments or questions?

MS. MARK:

That is true for the paper record as well. We want to ensure the paper record is authentic as well.

SENATOR WIENER:

Again, if it is changed, it is changed. That makes it a new document, and, there could be 16 new documents, but each is authentic as it is presented.

MR. MORTENSON:

What is the archival duration of microfilm? How long will it last?

MS. MARK:

If it is kept under proper conditions, humidity and climate controls, the lifespan has been tested out to 500 years. But, if it is tossed into your basement without any good environmental controls, it could last just a few years. So, we want to make sure that if there is a permanent record, we still look at microfilm as a good preservation tool. It will preserve the record as long as the microfilm is maintained properly.

MR. MORTENSON:

Five hundred years is pretty good. Thank you.

MR. IPSEN:

At a previous meeting, we had a discussion around electronic data interchanges and utilizing those, with digital signatures, to authenticate documents and building business efficiencies internal to the State. Can you speak to digital signatures? Is this an acceptable format? Can you speak to non-repudiation of documents in the future and the State-wide capacity that would be required?

MS. MARK:

That involves the public key/private key issue to make sure the on-going access is maintained. Is that right?

MR. IPSEN:

Yes and no. There are a number of ways to sign documents with non-repudiation. To use them might involve a public key/private key interchange. But, not necessarily just to create and sign documents. The reason I ask is based upon the IPER project going on with the federal government to keep and protect critical records.

A great example is the post-Katrina environment when both sets of physical records, one at a county clerk's office and one held at a home, a deed, for example, were destroyed simultaneously. Wouldn't it have been better to have had an electronic version that involved non-repudiation in multiple locations? This would be a more effective way to store documents. Can you see what we would need to do in terms of technology to build that capacity? Is it your impression that this would be a better business efficiency for the State?

MS. MARK:

I agree with you. The requirement of duplication – many copies is clearly better than having only one copy – and having all your eggs in one basket, so to speak. You want to make sure you have multiple copies and geographic redundancies of those copies so that you are backing up in both the north and the south. Katrina was a classic example where lots of official records were lost – deeds, wills, criminal records, and all sorts of things. Sometimes there was nothing left but the front steps of the courthouse. We are still looking at a number of small counties in Nevada that do not have the capabilities that some of the larger counties have to protect electronic records.

Yes, they are creating electronic records, but they may not be undertaking protection of those records through redundancy. This is a concern. An electronic record, held in multiple locations, helps to ensure the protection of that record in the event of a disaster.

SENATOR WIENER:

If there are no further questions or comments, thank you so much for the great explanations and bringing us up to speed. We will move onto Agenda Item 5.

Agenda Item 5 – Presentation by Mischel Kwon, former Director, US-CERT (United States Computer Readiness Team), What I learned at US-CERT and implications for the future.

SENATOR WIENER:

Ms. Kwon, I believe you are in Carson City. Thank you so much for travelling here from Washington DC. Hopefully, it was an uneventful trip. You have very strong credentials. If you would just give us a brief review of your history with these issues, that would help us understand and appreciate what it is you are about to share with us. Again, thank you for joining us today.

MS. KWON:

Thank you for having me, and thank you to all those of you who helped me get out here. It was a very nice trip. This is a very beautiful state.

I am the former Director of US-CERT. As the Director, my mission was to help protect the federal civil departments' and agencies' IT systems and networks. In addition to that, I was also tasked to lend assistance to private sector and state and local governments. My presentation is going to be about what I learned and what my "lessons learned" were from being the Director of US-CERT and where we have to go from here. What are some of the solutions as we look out into the future?

I will have to start by saying that this is an evolution. This is a long road map. We got really excited at the end of the Bush Administration with talk of the CNCI, the Comprehensive National Cyber-security Initiative. We thought we were going to be able to come up with some solutions that were going to be immediate. Unfortunately, there are no immediate solutions. This is a long evolution. It will always be a job that needs to be tended to. This isn't something we can solve overnight, and it is not one issue. It involves a lot of issues.

I think one of the biggest things I learned is that we are not very far down that path. We are really in a very immature state. We have a very young technology. I know that seems a little crazy, sitting here in 2010 – to say that IT is a new technology. But, in the realm of our history as a country, IT is a relatively new technology. Security of IT technology is a new idea and a new place to work.

So, today, I am not going to tell you a lot of nightmare stories about different kinds of attacks and spooky things that will happen to your networks. I am going to tell you more about what I learned about where we are in terms of our adversaries, in terms of the health and well being of our networks, and in terms of trying to move to a place where we can defend our networks, ensuring that our mission-space owners, who are the users of our networks, can feel safe and secure.

I want to talk more about the collaboration that is necessary in order to accomplish these things.

As I moved into the position of Director of US-CERT, I realized we were in a very disorganized state. US-CERT, at the time of my entry, was basically a ticket-taking organization based on the legislation called FISMA.³ The federal government was required to report all computer incidents to US-CERT, and they were doing just that.

We were getting multiple reports: “Yes, we had an incident.” But we weren’t getting much more than that. Just watching the craters form and measuring how large they were was not making things get any better. In fact, it was just causing a lot of frustration.

We needed to step back and ask what it was we really wanted to know. I will keep coming back to this mantra, over and over again. You will see that as the Director of US-CERT, one of the biggest accomplishments was changing the concept of operations for US-CERT – directing it from a ticket-taking organization to an organization that could clearly understand the threat to the federal government, the attacks those threat actors would then use, the vulnerabilities those threat actors would exploit with their attacks, the mitigation process necessary to correct the damage, and a reflection process – including compliance – that would allow us to ensure our networks were created and maintained so that this attack would not happen again.

That is a really different mantra than what we had worked with before, and I am happy to say we are still moving along in that direction.

It is important to understand that it really doesn’t matter if it is the federal space, or a private sector network, or a piece of our critical infrastructure, or a network here in the State of Nevada. We are running blind. I often say that the bravest people in the world are the Chief Information Officers (CIOs) and the Chief Information Security Officers (CISOs) of the world. I say that because they are having to make decisions with very little actual information about their networks.

IT is a very stove-piped organization. Although it is young, we have learned how to cordon ourselves off into separate groups and not collaborate, and not share. This has become not just a shame, but a money problem. It has become a management problem. And, in the end, it has become a security problem.

When we have an incident, we look at the information we have on that incident – whether we detect it through our security operations center or someone telling us that we have had an incident. We go back and try and collect the information. Very few organizations have that information in one place – what I call a single pane of glass. Very few CIOs or CISOs have something that says, “My network status is this...” or “My patch status is this...” or “My configurations are hardened and good, but in this organization, not so much.” “I need improvement here.” “I have this many users and they do this kind of work.”

Very few CIOs or CISOs have all of that information at their fingertips – all of the statistics they need – that single pane of glass, to understand the health, well-being, and status of their systems and networks. Without that, it is very hard to understand how to use your money, how to procure the proper equipment, how to hire the appropriate staff to maintain this network and create a defensive posture.

Many people will say, “The cyber problems today are technical problems.” I beg to say that we have a lot of good technology. And, I will talk about this later in my conversation. This is not to say that we don’t need improvements in our technology. I was talking to the CISO of the Department of Justice several weeks ago. I asked him how much money he was spending on security products in any given year. He said it was about \$30 million. I asked, “Kevin, for \$30

³ Federal Information Security Management Act of 2002.

million, what do you get for that?" He said, "I have no idea." This is because Kevin doesn't see the results of those security products. He has good people working for him that get those results, but the results are spread across several different organizations. There is the server group, the network group, the architecture group, the security operations group. Each one has a bit of information and is using a security product to do the job. Each product creates a log. Is there a way to pull this together so that you can have a single pane of glass – a vision of the health and well being of the network? That is one of the places we need to go. We need – not just to get rid of our stovepipe organizations technically – we also need to get rid of them as an entire staff.

I was talking about this to Chris earlier. We need to move toward cost savings not by getting rid of people or getting rid of products, but by repurposing – taking all of these separate entities and making them one joint entity that has a common mission: to not only to protect and defend the system, but to keep that system in good hygiene.

Most of our problems today are hygiene issues. That is another main thing I learned. About 80% of what ails us today has a fix for it. It is a problem that our networks are in such disarray, that we are so vulnerable to these attacks.

So, putting together our organizations and also putting together our products in such a way that we can use this data to help us understand and manage our networks and systems is critical and important. Having said that, we are dealing with more than just a patching problem. It is not just a configuration management problem. As soon as we patch and make things better, we will have another patch to install next week. And, we will have another configuration setting to change, because our adversaries are nimble. I will also say that the technology base we have chosen to use is an open technology. With an open technology will come vulnerability. We have that problem. We have to look for another solution beside just patching. I will talk about that as well.

One of the other large lessons I learned as Director is that we have a shared infrastructure that we all use. We need to take advantage of that share infrastructure. We all use Internet Service Providers (ISPs). The Internet is made up of joint missions among many companies. But it is an infrastructure, and we need to learn how to clean up some of the noise, some of the rote and mundane problems we see in cyber. We need to get rid of some of those vulnerabilities at the infrastructure level – whether it is at the ISP or web caching company or another part of the Internet infrastructure. We need to learn how to do this. We need to learn how to do it while at the same time preserving privacy and civil liberties. That is one of the largest concerns and challenges that we as a nation face going forward. This is such a productive place to do defense, but such a dangerous place because of the information that flows over the Internet.

What is most important to know is that, although we seem disorganized as a nation in cyber right now, we are moving in a good direction. We have a good roadmap of where to go. I think the fact that we understand that this is more than a technical problem – that this is a management problem – this is an "understanding what we are dealing with" problem – is good and important. It is most important because our adversaries understand that this is our problem.

I think our adversaries understood that managing our networks was our problem before we understood that managing our networks was our problem.

You can see this by reading a lot of their open policies and open discussions on IT and how they have restructured their governments to incorporate IT into every aspect of their government.

It was interesting to hear some of the earlier testimony about how this has become just another part of life. As we have our IT stovepiped into its own organization, we have to realize that IT is a part of everything we do today. There is very little we do today that does not have an IT aspect to it. The only reason these systems and networks are here is to serve a particular mission. They

are not here to have the biggest, fanciest systems, or the greatest SLA⁴, or the fastest network performance time. A lot of us in IT like to tout these things. But, we are here to support the missions of our law enforcement. We are here to support the missions of our record keepers. We are here to support the missions of our Defense Department. We have many important missions, and without them, we would not be here at all.

To understand how we protect their missions by protecting IT is critical and important. By coming back around and understanding how to manage what we have, and manage that in such a way that we protect our missions, is absolutely critical and important.

As we look at how we manage that, we also have to realize that the status quo is expensive. How we do it today is expensive. Of course, the losses we feel from data loss, or even monetary loss in the financial sector is huge. The “whack-a-mole” process of patching is a very expensive process. Continuing forensic processes, not necessarily for law enforcement, but for purposes of understanding what happened, when the same thing is happening over and over again in our networks. The constant checking of security controls that we call best practices, but when you read those security controls, they are the same security controls from 1982. This tends to be a bit of a problem.

When we look at our SIM⁵ tools in our security operations centers, we have what we call “alert frenzy”, where we have so many alerts that we do not have the staff or the time to look at them all. In essence, we have an inability to manage or control our systems and an inability to show any return on investment for any of the products that we buy. This becomes a major problem. It is all created because we have stovepiped our way apart from one another, and we do not have a way to manage our processes. We have to go back, take this by the hand, we need to create this management process. We need to pull our tools together. We need to create the “single pane of glass”. We need to look at not just the vulnerabilities. Many of us CISOs realize we are drowning in patching. We are drowning in the vulnerability.

Not every vulnerability is your vulnerability. We have to go back to the mantra: It is the threat. It is understanding the attack the threat actors are targeting on your organization. Prioritize the vulnerabilities those attacks are going to use so that you can create the mitigation strategy and create the reflection process. This is a methodical management process that needs to be put in place.

We also have to understand that most of the attacks today are not single onesie-tuosie attacks. It is not just one piece of malware. It is a multitude of malware that is exploiting multiple vulnerabilities on the system, some which are not even technical. Some that are social engineering tactics. Some are a part of the mission. Understanding the attack pattern is even more important than understanding the vulnerabilities on our systems. This means we can prioritize the work that needs to be done, whether it is social engineering training, whether it is fixing an actual vulnerability, or changing an application, or changing an architecture. We need to know what we need to do in order to defend our systems.

With all that being said, and that sounds like a lot is wrong, when you hear that a lot is wrong in this case, you have to realize that a lot is right. That is because we realize that is where we are today. We realize that some of our technologies are not doing what we want them to do. We realize that signatures⁶ are not helping us as much as we would like them to. If you triggered [detected] a signature, you are probably already toast. You want to try and catch the problem before that signature triggers.

⁴ Service Level Agreement.

⁵ Security Information Management.

⁶ Here “signature” refers to a characteristic marker identifying specific malware or a method of attack.

We realize that patching is hard. We realize we have all these problems. If we have moved to a place in our evolution where we realize we have to stand up, turn around, and try something new, what is it that we need to try that is new?

We need to embrace the fact that security equals good management. We have to put our team back together and not allow our staff to become stovepiped. We need to understand our governance structure within our organization and the authorities that each entity brings to the table to help get this job done. And, I say that very carefully – to help get this job done – not authorities to stovepipe themselves away from one another, but to get the job done.

You see this governance process problem on the national level, on the agency level, on the sub-agency level, on the sector level, and in companies – as many companies merge together. And, I am sure you see it here in the State of Nevada at times. Pulling the governance structure back together and pulling that team back together is critical and important. I know you hear “information sharing” all the time, and I know that many of you are tired of hearing it because we have not gotten very far with “information sharing.”

But we need to where we can share information in an unclassified way – at least through the TTPs⁷. We are hurting ourselves more by not sharing than we are by sharing. Yes, we will lose a few secrets here and there, but we will protect a lot more by sharing in an unclassified manner – at least on the tactics, techniques, and protocols level. We need to be able to understand what is happening in these attacks and share that information quickly.

We need to understand what metrics we need to use to measure whether we are being successful or not in protecting our networks. This has been a challenge. This is one of the harder problems we have had to face. We need to show we are making improvement. Basically, we need to start from where we are all afraid to start from – that is our incident level. If our incident level is going down, we are doing better. If it is going up, we are not doing so well. It is a scary place to start, but we need to start looking at how to create a defendable network.

We need to understand how to report on all levels. This is information sharing too – whether it is sharing information all the way to the top executive, whether it is sharing information to the CIO or CISO, to the manager, to the network administrator. But understanding how an incident or what the state of the health of the network is throughout all those strata is very important. That communication and information sharing, and the flow of information, should be good and actionable.

We need to create compliance programs that are based on our incidents, so that we understand that what we are checking when we check for compliance is that we are defending our networks and that we are fixing the most critical problems that need to be addressed – not that we are fixing the best practice, low-hanging fruit, but that we are fixing what is ailing us most. I think the federal government is moving in that direction with their continuous monitoring programs, and I think that is one of the bright shining stars that is happening today in cyber. It is not often that you hear a compliance program described as a bright shining star. But, moving to continuous monitoring, where you are marrying your compliance program with your defensive posture is absolutely critical and important.

We have to be able to pull all of the data together to help these stovepiped entities. We have to be able to take the patch management information and the idea of signature hits and the level of operating systems and where our third party software is and how many incidents we have had and where it has affected those areas and pull it all together in an understandable, non-technical way so that our CIOs and our CISOs understand the health and well being of their network at any given time. That is just critical and important moving forward.

⁷ Trusted Third Parties.

With that being said, I did talk a little bit about ways to take our current technology and pull it together to create a single pane of glass as a positive going forward.

But what new technologies do we need to help us combat this problem?

I think one of the things we understand is that monitoring our IT networks with a security operations center is really expensive. We are finding that a lot of security operations centers are turning their SIM tools down to where they only have ten triggers to look at, at any given time. My question about that is, "What is happening to all of the other stuff that is hitting you? You just don't look at it?" That is a problem. It means that the technologies we are using today and the methodologies we are using to monitor our networks are not quite correct.

Instead of looking at the onesie, twosie hits, being able to look at those attack patterns and to develop an attack pattern strategy, looking at behavior across the network, understanding what your user behavior is supposed to look like, who your users on your network are supposed to be, and how traffic on your network is supposed to move, in order to understand when something has gone awry, and be able to see the entire attack instead of just the one piece of malware that was exploited. It becomes a much more efficient way of managing an incident. The only way we are going to get to that attack pattern process though is through some good information sharing where we all share information about the attacks and the patterns we see.

Having some sort of change resistance technology, understanding our environment today as it stands. This is what normal looks like, and understanding when it changes so we can then do something about it – whether it is an automated change or whether it is some type of physical change. That is going to be one of the new interesting technologies coming in the future that I think will help us a lot.

Also, creating change in the environment to keep the adversaries from being able to do what they need to do. Even if there are vulnerabilities in the environment. I call this a "fault-tolerant" type of model, where you are moving more and more to virtual machines. As you move to the virtual machines you can roll the virtual machine back to its original state periodically. In doing that, you rid yourself of all the attacks that were in the service at the time of the roll back. This is another technology that is important to look at for going forward.

More importantly, automating the analysis and reporting, so that this reporting all the way down from the executive level all the way down to the actual administrator on the floor is cohesive and automated. Automated compliance – so it is based on real data from the system and not just inter-view is critical and important.

I also think it is critical for us to look at new ways of doing old technologies. I see cloud as one of those new/old combination technologies coming forward. I think we have to embrace the thought of doing. I see cloud as a collaborative type of solution. It is an opportunity for us to learn how to do the reporting and the management.

We actually knew how to do this at one time. We all had network operations centers where we were concerned. We all had SLAs for up-time and how fast the traffic would move. That is the same type of monitoring that we need to do. It is expensive to do on a onesie, twosie network basis. But, in a cloud environment, it becomes much more cost effective when you are sharing that kind of monitoring across many entities.

In addition to that, security operations become a lot more cost effective if you are doing it in a centralized security operations center, or even hiring out a security operations center to do the work for you.

So, looking at new models of doing old types of technology will allow us to have good cost savings, maybe better management reporting, and, in addition to that, help with some of the

information sharing since some of that will be in one center. It is a matter of getting better at trusting each other so that we can do these collaborative efforts together. I think that is very important.

In summary, my strongest lessons learned, my very strongest lesson learned, was that it is knowing your threat actors – knowing what your threat is, specific to your organization, and knowing what attacks are going to be coming at you so that you can prioritize and understand what vulnerabilities you need to concern yourself with, understanding the mitigation processes and what those will cost, and understanding how you can reflect on what has happened to you so that you can ensure it will not happen again. This is a clear management issue. And, it is ours to solve. We need to reduce the noise on the infrastructure level, and that is a hard problem we are all going to have to come together and figure out how to solve. We have to understand this from the attack pattern process. We need to worry about vulnerabilities, but only as those vulnerabilities apply to us. We need to have better situational awareness through better information sharing.

I would love to see a non-profit information sharing portal where non-attributional information on attack patterns can reside. I think that would be one of the biggest contributions to cyber today.

I also think declassification of TTPs is absolutely critical in order for us all to defend our networks.

And, knowing our systems and knowing our users, knowing what the mission of our users is, knowing what happens on a network, and knowing what normal looks like, is really important to be able to defend and to get back to normal.

Last but not least, looking at new technologies. We have had the same base of technologies for at least 10 years. It is time to look at new technologies and new methodologies, thinking outside the box – a new way to defend out networks.

That is what I have learned. I hope I didn't just give you bad news, but I gave you some thoughts for some solutions going forward. With that, I would like to know if there are any questions.

SENATOR WIENER:

Thank you very much for making the trip and for sharing your insights. Even for one who does not work with this daily, I learned an awful lot. It is good information to take into a Legislative session. I appreciate that very much. Are there any questions or comments from the Board?

ASSISTANT SHERIFF MCCLARY:

Thank you for the information you provided. Let me say a couple of things. And, please, if the words I use aren't the right ones, consider the source – I'm just a cop.

One of the comments you made really resonated with me. At a number of the boards I sit on at the national level, the whole concept of cloud computing and where we are going to be in a very short period of time has really been framed in the context of "Oh, gosh!" This presents a lot of challenges from a police perspective – in traditional ways that we have collected electronic intelligence and a number of other things.

The comments you made about the fact that cloud computing provides opportunities to us as well was informative. That is the first positive comment I have heard from my world about cloud computing. It will allow me to say, in the next meeting I go into, that not everything that is happening is bad.

One other question I have for you – and hopefully I can frame this in such a way that it will make sense to you – and you may have an opinion, and, in fact, ma'am, you might not. One of the other committees I sit on here in the State is our Nevada Homeland Security Commission. We are

having a great deal of discussion about where State and local law enforcement fit in the overall national model to detect, prevent, respond and mitigate either terrorist or criminal threats.

We had some guidance two years ago from the Department of Homeland Security that recommended to States that they establish something called a cyber initiatives – and there was not a great deal more definition of that. And that best practices for communities to protect themselves would include whatever those are. So, we have had this on-going debate for the last two years in our State about what our role is at the State and local levels vis-à-vis the overarching national mission.

If you have an opinion you can share with us about where you think we fit – what's our lane in the road – that would be helpful.

MS. KWON:

So, first of all, in regards to the cloud statement, I will tell you that it should be seen as a positive, but it is not all a bed of roses. I think we do have some problems we need to address and overcome before it is perfect. But, this is our opportunity to do that. This is our opportunity to address how do you handle data that is going to be used for prosecution. How do you handle forensic evidence? These are things that have to be determined. Unfortunately, at this time, it is being left at the contract level of the person who is buying the cloud services. Having informed customers at this point in time is absolutely critical as we move to the cloud. So, whatever you can do to inform people that they have to keep aware of keeping that door open for you in their contracts is really important.

As far as were do State and local fit into the larger cyber arena, I alluded a little to this. Again, I tried to keep it on the positive side when I talked about governance structure. I think we are still struggling with that. We are still struggling with how does everything fit together. If you look at the national level, they are still struggling to figure out what their cyber czar does. They are still struggling to figure out what ODNI's⁸ role is, what Homeland Security's role is, what Commerce Department's role is. They are still trying to figure out the role of Secret Service versus the role of the FBI.

These are all governance structure issues. I believe we all have a very critical and important role. Especially as you get closer to the crime, as you get closer to the users, as you get closer to our citizens, your role becomes even more important. It may not make the newspaper all the time. It may not be at the top of the national news, but it is where we are making the arrests. It is where the action is really happening.

What we have to ensure is that we turn that table upside down – where the national level is supporting what is going on at the ground level.

So, I can't tell you how it is going to be. I do not have any visibility or vision into how a governance structure can be put in place. I know that is one of the hard problems today to solve.

ASSISTANT SHERIFF McCLARY:

Thank you, ma'am. I appreciate your comments.

MR. IPSEN:

I have just a quick question. First, thank you for being here. I genuinely appreciate your views from a national perspective. Rarely do we get a chance to peek up over the wall to see what is happening globally. In order for Nevada to embrace cyber issues effectively, we need to be mindful of the global picture as well our own individual pictures.

⁸ Office of the Director of National Intelligence.

One of the things that is particularly important for me is developing enterprise approaches to cyber security. Can you speak briefly about the business efficiencies of enterprise approaches to security? Do they work better? Do they cost less? In general, if we could develop a collaborative strategy, and I am heartened to see everybody in the crowd that is here, because I think we do have a great collaborative environment, could you speak to those business efficiencies? Are we on the right track moving forward if we approach cyber security in this manner?

Ms. KWON:

Absolutely. Not only from a US-CERT perspective, but also as the former Director of the Justice Security Operations Center for the Department of Justice, I can tell you that their roadmap has been to create an enterprise security operations center. And to create an environment that allows them to have enterprise licensing for all of their IT products in general because there is so much cost savings.

You will see that rolled up again, where, on the national level, today, DHS is trying to put together national level contracts that will allow not only federal government, but state and local, to buy security products on a larger contract, so as to be able to find money saving in buying in a bigger lot. So, that's only one part of the savings.

When you look at the amount of data that you have to put together and the number of professionals you need to do this, it is hard to find that many people. It is hard to administer on a smaller network level. The more you can do on an enterprise level, even on a co-sharing enterprise level – which we are beginning to see now, where companies are sharing security services and even IT services. Again, moving more and more toward that cloud model.

You are seeing lots of cost savings – and not just cost savings but efficiencies, in that you get a higher level of professional staff and more information sharing because you have more data to cross pollinate.

So, there are a lot of savings and a lot of efficiencies created in going to an enterprise – or even higher – level of merging.

MR. IPSEN:

Thank you. If I had to speak to the State's perspective, two of the challenges we are facing right now that I think we need to address, and we are looking at addressing, are (a) the framework that allows us to share contracts. In the past we have had initiatives like NSITS⁹ and collaborative organizations working together to come up with those enterprise license agreements, where we can effectively leverage economies of scale. But then also (b) we need to look at the ways we can procure against federal contracts, because I know there are some limitations right now in terms of the State purchasing against very good pricing on the federal level because those contracts do not necessarily meet all of the P's and Q's of our individual procurement agreements. These are two areas I think we can save a lot of money moving forward – against an appropriate architecture and framework for acquisitions.

So, thank you very much for your comments

Ms. KWON:

I agree. Chris, I also know there are several initiatives to include state and local in the procurement, so that once it is procured, you have the benefits of the product without having to go through the procurement process. We can talk some more about that later. Those types of threat information purchasing processes – when it makes sense to buy for a bigger lot, and the federal government has the money and can do that – going with initiatives like that is even better.

⁹ Nevada Shared Information Technology Systems.

ASSISTANT SHERIFF MCCLARY:

I'm sorry, ma'am. I just wanted to make sure I had this written down correctly. It is your official, and your educated, opinion that we need to turn the paradigm upside down – and the federal government needs to support State and locals.

Ms. KWON:

You're going to hold me to that, aren't you?

Yes. That is my personal opinion.

SAC FAVREAU:

With that in mind, I just wanted to comment quickly, Ms. Kwon, on your remarks. They especially rang true with me, because what you learned during your time at US-CERT, we at the FBI and kind of been going through the same exercise. You said you went from ticket-taking to trying to better understand the adversary, the vulnerabilities, and then come up with mitigating strategies. In a post 9-11 environment, that is exactly what the FBI has been trying to do as well.

I really applaud your effort in trying to get the cyber security community to understand this as well. I think it is a great roadmap you have left for the cyber community to follow.

Ms. KWON:

Thank you very much.

SENATOR WIENER:

If there are no other questions, thank you, Ms. Kwon, very much. We certainly appreciate everything you have shared. I am sure we will be tapping into your intelligence, your wisdom, and your experience, and your perspective. This is the beginning of a process. Thank you so much for coming far west to help us understand this at a greater level of detail.

Agenda Item 6 – Reports on (1) the InfraGard/GMIS Cloud Computing Conference in Carson City and (2) the Cyber Seminar in Las Vegas, Ira Victor, President, Sierra Nevada Chapter, InfraGard, Alan Rogers, President, Nevada Chapter, GMIS, and, Christopher Ipsen, State Information Security Officer.

SENATOR WIENER:

Gentlemen, before you share your comments and give us your report, I want to thank you on behalf of the Board, the Attorney General, and myself, for sponsoring Ms. Kwon's participation in today's meeting. Without your financial assistance, this would not have been part of our agenda. We received a lot of new insights that can inspire us to go in different directions. With information, we are armed. That is critical for us doing the right thing. So, thank you very much for your participation and your support at many levels.

Ira, of course, you are a regular as well. You have helped us along the way. But, let me turn to Mr. Rogers first and then we will come back to you for any comments you would like to make.

MR. ROGERS:

Thank you madam chair. I am the President of the Nevada Chapter of Government Managers Information Sciences International. That is where the GMIS comes from.

GMIS is an organization structured for IT entities within the public sector. Our members come primarily from the State, county and city governments and their IT agencies. So, we are represented here in Nevada by Sparks, Reno, Washoe County, the State of Nevada Department of Information Technology, State of Nevada Department of Personnel, and State of Nevada DHHS, Carson City, and I think that is all of our membership.

Those are the entities that participated in financing Ms. Kwon to come here today, and I appreciate their support. We are a collaborative body. We get together to share information, to share ideas, and to work together on initiatives for Nevada in the IT area. With that brief introduction, I will pass it on to Ira, unless there are any questions.

SENATOR WIENER:

Mr. Rogers, do you want to talk a little about that Cloud Computing Conference, and then we will bump over to Ira? However it works for you.

MR. ROGERS:

That conference was a joint conference between InfraGard and GMIS, so Ira is going to present some information on the conference.

MR. VICTOR:

Thank you Madam Chair. I am the President of the Sierra Nevada InfraGard Member Alliance. As we like to say I-N-F-R-A-G-A-R-D. The only thing that is missing is "U". I want to thank you for the kind introduction. We were pleased as a group, InfraGard was, to sponsor Ms. Kwon here to help provide the information to help protect the critical infrastructure here in the State of Nevada.

That is why we, along with GMIS, co-presented what I believe is the State's first cloud computing security conference ever. Hopefully, we can make this somewhat of a regular event because it is so important. We did do an entire day session with three tracks here at the LCB building in Carson City.

We had excellent attendance and excellent feed-back from the members. Some InfraGard events are closed to the public because the information is sensitive. We made this conference intentionally open to the public. So, anyone from the public sector, the private sector, law enforcement, all of them were invited to attend, and we did have a good, broad spectrum of attendees from the different areas in the State to help tackle these issues – and they are tough, indeed.

Our speakers talked about the challenges, as Ms. Kwon did, of the contractual issues. In brief, companies, and both the public and private sector, decision makers, will sign up for a cloud service. It seems easy. The data gets transferred. The management gets transferred over, and then no one knows what to do with the issue "Who owns that data?"

There are law enforcement issues, forensic issues, both from a civil and criminal perspective, trying to track down a bad guy – Who owns that data? That was one of the many issues that was covered in the cloud computing conference. There were storage issues. All your data is stored in the cloud. How do you manage that from a technical and from a contractual stand point.

I know we are touching on the right areas here. I attended the Paraben Forensics Innovators Conference in Park City, Utah last week. Some of the most attended events at that conference dealt with cloud data from a forensics standpoint. When law enforcement seizes someone's laptop, or their GPS, or their cell phone, the standard operating procedure is to grab all the data off that device to use that to determine what happened in the past.

Well, what do you do when that data is in the cloud? What are the jurisdictional challenges? What are all of the problems when the data that we need is in the cloud?

We began the discussion here in Nevada last week. It was confirmed to me that we only began the discussion because, even at a pure forensics conference in Utah, they were admitting that we were only scratching the surface of what needs to be done for an entire dedicated conference. So, there is a lot of work that remains, and a lot of education that needs to be done for technical and non-technical decision makers to help guide us through these challenges so that businesses

and the public sector can help protect their information and do the things that need to be done to help Nevada grow.

That was our goal at that conference, and we will continue our efforts in that area. As a segue to that, I want to thank you again, Senator Wiener, regarding your comment on my being present. As a president of InfraGard, I want to offer up our board members and the members of our group as subject matter experts for the up-coming legislative session.

There are a lot of bills that will have cyber implications in the next session. A lot of times, if you just look at the surface of the bill, it might sound like, "Oh, this is a good idea" or "Oh, this is a bad idea." But often there are a lot of nuances when it comes to cyber. I want to offer the expertise of our organization to help members of this Board and to help members of the Legislature to dissect all of these terms and understand the ripple effects of what a bill can do – either to help us or to hurt us in Nevada. We offer expertise in those areas. That is my presentation for today. I am available for questions.

SENATOR WIENER:

Let me state for the record that you have always been an important person at the table as I have worked on technological legislation. We have had great success because we have created the clarity we needed to produce good policy. So, I thank you for that. I probably have a bill or two that I will call you on. We are drafting them now.

Did you have anything to say about the Cyber Seminar that was held here in Las Vegas?

MR. VICTOR:

Thank you. I...

SENATOR WIENER:

Chris was there as well. That was another event we wanted to take a look at.

MR. VICTOR:

My apologies. I will say a few words, Chris, and then toss it to you. I did not bring that up, even though it is staring me in the face, right in front of me.

There was a meeting in the south, in Las Vegas, regarding cyber crime and critical infrastructure issues last month. Again, it was very well attended, although, the bigger emphasis was on the public sector for that event. But, there still were private sector attendees. It was an entire day event on cyber security issues.

I think it is a good sign that these issues are rising in importance. It used to be that the issues of cyber crime, critical infrastructure, forensics, were fringe issues. Now, members of the general public and non-technical decision makers, the non-geeks, are starting to understand how these issues ripple throughout. That is what a big part of that event in Las Vegas was.

The one area I want to bring up, because, today, it was in the news again was discussion about Stuxnet and industrial controls security – that's the electrical grid, the gas and water systems. We had a speaker from the federal side come to us via Skype and talk with us about the real dangers that we face.

Yesterday in Congress, there was testimony regarding Stuxnet, and how that worm has the potential to do a lot of damage to critical infrastructure. So, the word is getting out here in Nevada. There still is a lot to be done in that area nationally and locally. But, I think the attention that is being focused on it is healthy for us and will help us to tackle those issues.

SENATOR WIENER:

Thank you, Ira. Chris, did you want to add something?

MR. IPSEN:

I just wanted to say thank you. Both InfraGard and GMIS really stepped up with Mischel. I also want to complement Irene Navis in Las Vegas. She did a fantastic job on the conference. And thanks too to DHS for funding people to travel. They are actually solving some of the challenges we have. Even though the costs are minor, I think the outcomes from these types of presentations and collaborations are significant. As you know, the State is extremely financially strapped. Often these travel dollars are the things that get cut. So, by having organizations like InfraGard and GMIS stepping up to help with speakers – and also down in the south with DHS funding for our travel to go down and discuss these issues – I think we are head and shoulders above where we were before. I think we are a model for the United States in terms of collaboration. I can't thank all of you enough. It has just been fantastic.

SENATOR WIENER:

Are there additional comments from the Board, north or south? Thank you very much for the update and what is in process as we move forward with the educational opportunities that are being offered to people who need them and want them. Thank you so much.

Agenda Item 7 – Identification of issues and concerns relating to possible statutory changes allowing increased collaboration among DoIT and county and municipal IT Departments in the procurement and use of Information Technology (IT) and IT security goods and services.

SENATOR WIENER:

We have heard the word “collaboration” several times in the last presentation, and we have heard it throughout the morning. This is a very important mindset for us to consider and move forward with in ways we have never done before.

This particular collaboration would be with DoIT and county and municipal IT departments. So, we are looking at procurement and use of IT, some of that relates to security in terms of goods and services. So, we do have representatives from several of the local jurisdictions.

Hopefully, I will get these right. In Las Vegas, do we have Laura Fucci, the CIO of Clark County? Then, Joe Marcella, Director and Chief Information Officer from the City of Las Vegas should be with us. Then, Chris Wilding, the Chief Information Officer from Henderson, should be here. OK. If you would all please come forward.

Then, in Carson City, we have Cory Casazza, Chief Information Management Officer from Washoe County, and Richard Vandenberg, Director of Communications and Technology, City of Reno, and Chris. Chris, are you going to join them at the table?

MR. IPSEN:

I think I want to minimize my involvement and not give up my cushy seat up here. Well, I'll come on down.

SENATOR WIENER:

I understand you have had the opportunity to look at the proposed legislation from the Attorney General's Office. What we want to look at are the advantages of collaboration and some of the highlights you think we need to address.

But also, if there are considerations that are disadvantages as well, we need to be aware of those. Let's start in the south and then go north. We are going to hear from all of you, but if you have a lead presenter, please identify yourself.

Ms. FUCCI:

I will go ahead and start and then pass it on to my colleagues. I am the Chief Information Officer for Clark County. I want to express that we have had a very long and rich collaborative relationship with each other in the south and also participating with the State of Nevada Department of IT. That has been expressed explicitly with a Governor's initiative, which we refer to as NITSITS. It is the Nevada Information Systems Sharing Technology... I can't remember the exact acronym, but that allows us to work together in collaborative efforts.

More recently, we have been working together in response to AB 494 [2009 Legislature] within the south, looking for opportunities to collaborate on various infrastructure and other projects for technology. We have worked for years on GIS, wireless technology, and various other efforts. I know that we also ride on various State contracts.

What the State of Nevada is proposing are some legislative changes to better enable them to work collaboratively with the south and offer State services in the south. There is some legislative language that may currently preclude them from doing so. They are trying to open that up and more freely provide services – not just to the south but to other local governments within the State.

We are very open to the idea. We think we can save money and do things more collaboratively for the best interests of our citizens by joining forces together.

SENATOR WIENER:

Because money is obviously going to be a big consideration the session, in looking at the measure that the Attorney General has proposed, do you see that this could benefit government at all level, therefore the people of Nevada, while being cost-effective and efficient?

And, are there any downsides to this that we need to be aware of?

Ms. FUCCI:

I think that as long as it is an option for governments, and not mandatory that we have to take DoIT services, then we can look at what is best in every situation. The opportunity that is at the table is clear. Right now, the way things work, we ride State contracts. For example, the State negotiates the contract, puts it all in place, and then local governments review the contract that is already negotiated, and we then write it.

With the opportunity that they are talking about, we would join them at the negotiating table. We would identify what our use would be. So, there is an opportunity for better discounts. So, Clark County may be using 5,000 licenses of something. We could add that to the volume discount during negotiations, thereby getting better discounts from a vendor.

Right now, we don't have that opportunity, because we ride on that contract after it is already negotiated.

SENATOR WIENER:

Thank you. Great information.

MR. MARCELLA:

I am the CIO for the City of Las Vegas. I just want to provide a framework around the purpose for moving forward, and having the opportunity to do purchasing in some collaborative fashion.

With AB 494, which asks for the research and analysis for collaboration with the local governments as well, and with NSITS, the Nevada Shared Information Technology Services, where we had looked into collaboration in southern Nevada of the IT organizations in local government, where there might be some opportunities for not only sharing excess capacity, but establishing contingency and records management in some fashion that was not only

collaborative but also efficient and effective. Then, we were looking at giving us the opportunity to have multiple organizations and multiple sites where, in the event of a catastrophe, we had some place to go.

The framework that is necessary for that is, obviously, the cost of doing that, the procurement of certain goods and services. This proposal actually starts to lay some of that foundation that is necessary.

AB 494 asks for several things from local governments. One of which is to take a good look at services that we provide, and, if it is at all possible, portal ready – or do them in some sort of collaborative fashion. An example would be business licensing, where multiple jurisdictions have different rules, codes, and obligations for someone to get a business license that they need. The Nevada business portal is still in its infancy, and would allow someone to get a State business license as well. If that could be done in some collaborative, consolidated fashion, then it would make perfect sense for citizens because they are dealing with multiple governments. Obviously there is a revenue issue that goes along with that. But there is infrastructure that is necessary.

As Ms. Fucci mentioned, one of the concerns has always been, when you start talking about consolidation, you start talking about consolidation of data centers. There is such a disparity, or difference, between how certain governments do certain things, sometimes based on charter, that it becomes difficult to marry or merge those organizations.

What we have found is that in some collective fashion – almost like virtual consolidation rather than brick and mortar consolidation – after the identification of these services are made, we can actually do that, and prepare for those things, as they either get agreements within the local governments to move forward – to do those kinds of things. Then, the infrastructure is waiting and ready from the IT organizations doing this kind of collaboration. The ancillary benefit is, as I mentioned before, contingency and shared resources and efficiencies in products that we currently deliver.

So, this literally does two things with one event. We are really anxious and feel that this is important because it helps with that infrastructure and it does set the foundation for collaboration with the State, which was never before at the level and possibility that it is today.

MR. WILDING:

I am the Chief Information Officer for the City of Henderson. As you can tell from my dialect [spoken with obvious English accent], being a local, born and bred – not really.

I am here to express Henderson's support for the language being proposed in the Legislative session. The more we can collaborate with a broader set of entities, that kind of makes sense. My colleagues in the south and I collaborate; we look for opportunities very frequently. It would be very appropriate and necessary for the State DoIT to be able to collaborate and provide services, if, indeed, they can, and, if, indeed, we request them.

I don't see too much of a downside to the language being proposed. Just to speak briefly again on AB 494 – I concur with my colleagues that collaboration and sharing is most successful, in my opinion, when it is voluntary.

I have been a public servant for only two years, so, with my private sector background, I look at a lot of these initiatives with some sort of ROI¹⁰ in mind. Is there some kind of payback here? Is this really worth while? I believe if we can continue in an opportunistic manner, that as something happens, we seize it and work together to try and drive down costs and create savings, that is, overall, more effective than trying, perhaps, to be encouraged or forced into some brick and mortar consolidation.

¹⁰ Return On Investment.

I don't believe that bigger is better necessarily. We are a small, agile city. The services we provide enable us to be sort of out there at the front edge. We are very, very proud of where we are.

I do believe that are definitely some opportunities to look at data centers and sharing bandwidth, but I would like to do that on a voluntary, kind of ad hoc basis as the needs arises. We will be having conversations, for example, with the City of Las Vegas about some new opportunities we have around agenda management systems, permitting, land control, business licensing. I think if we can get our heads together as issues arise, to look for these savings, it is far better than being directed to do so in some other way.

So, basically, to summarize, we are supportive of language in the bill draft, and supportive of these voluntary studies under AB 494.

SENATOR WIENER:

You mentioned in your remarks that two distinct and different words: collaboration and consolidation.

I can not speak for the Attorney General on her intention for the BDR, but, in the notes that I have, the word "collaboration" is the one that is consistent. That looks like the direction rather than consolidation. That has seemed to be the theme of our meeting today, and it is carrying through all the way to this agenda item.

Before we go north, are there any questions of these witnesses in the south. Then, let's go to the north, and please, proceed in whatever order you feel is appropriate. But, let's wait for Chris to go last.

MR. CASAZZA:

I am the Chief Information Officer for Washoe County.

Similar to the south, I think we completely support this effort. We are very appreciative of the effort the State has made to include us in the past – especially with the virtualization software. That has saved us a significant amount of money.

In a similar fashion to the south, Washoe County, City of Sparks, and City of Reno have consolidated and shared services. Well, maybe not consolidated, but shared services as far as 800 MHz, GIS. We share a lot of network together, and we also have some jointly owned fiber with the City of Reno that connects city and county buildings together. We continue to look for consolidation and shared services opportunities.

Going beyond AB 494, the City of Reno and Washoe County have hired a consultant to come in and see if there are further consolidations and shared services opportunities. So, we are looking to see, even beyond shared services, if there are places where we can consolidate functions. We may not save money currently by doing it now, but are there cost avoidances in the future?

That pretty much sums it up.

MR. VANDENBERG:

I am the Communications and Technology Director for the City of Reno.

I came here to listen about this. I was a little bit surprised that I would get called up here.

But, I agree with Cory. I think, given the state of the economy, especially in the northern region – I don't know how it is in the south, I am more concentrated on Reno – doing things the old way is no longer doable. We have to look at new ways of moving forward on this.

Initiatives, from what I am hearing, and moving forward with the State, only make sense.

But they make sense if we go in with our eyes wide open. I think our shared services that we are looking at with Washoe County makes a lot of sense. But, we have to go into it with our eyes wide open. We have to go into it taking a look at a business model perspective – not necessarily the idea that, well, “I heard it works. So, therefore, let’s go forward that way.”

I think there are lot of issues that are going to come forward that are going to bite us on this, but I think that every single one of them can be overcome.

With that, to summarize, I’d say, I am absolutely in favor of this – and looking at any options that makes us become more efficient and effective in the jobs that we do.

SENATOR WIENER:

Thank you very much. Let’s turn to our very own Chris. You now bring up the State side, so please share your thoughts with us.

MR. IPSEN:

Actually, I think this is a really good example – the collaboration model manifest. The individuals who have spoken before me have done such an eloquent job, it is difficult for me to add anything more than the State perspective.

As I provide the State perspective, I am not the Chief Information Officer for the State of Nevada. I am the Chief Information Security Officer, and I am acting on Daniel Stockwell’s behalf on this Board. So, I speak only for myself, but I can tell you what I see in this proposal.

One of the limitations the State has is that, by NRS, we are restricted from collaborating with counties and cities. It is a little easier for counties and cities to collaborate with us than for us to collaborate with them – primarily based on the language in the NRS, which basically states that we can only collaborate if we have excess capacity.

Well, you know the financial state of the State, and having excess capacity – well, we could never be in a position, where, even if we did have it, we could freely manage it and give it out to others, because it would be planned for some other use.

What this initiative does, is it gives the State the opportunity to more effectively collaborate with counties and cities. I think from a leadership perspective, we need to consider the State participating with the counties and cities and collaborating.

I don’t want to be the odd person left out. I think we all have one citizen we are trying to serve, and if there is a capacity that exists that is effective and efficient anywhere, I want to leverage it. If we can reduce the costs of IT and services, and improve those services going forward, I think it is a no-brainer to look at enterprise agreements. We should all stand together. We should build those economies of scale. I think it is in the citizens’ best interest for us to look at that.

So, if there is existing legislation that precludes us from doing that, then we need to address it, and I believe that the Attorney General’s legislation addresses that very effectively. From my perspective, I am wholeheartedly in agreement with it, and I am really glad to sit here with everyone and say that, “We, in Nevada, are going to be Number One. We are going to be great in this regard.”

I have to commend you, Senator Wiener, for your leadership. You have had the fortitude to look at these types of legislation. A lot of times when you talk about IT, people just glaze over. They say that it is hard and scary, or that it is really difficult. To be able to sit down and look at legislation that makes sense, I think the citizens are well served by this.

That's all I can add. I think it is a great idea. I am proud to be a part of it.

SENATOR WIENER:

Chris, thank you for the kind words, but one question. It seems as though there is a collective thought around "it being at the request of the municipality, or the more local jurisdiction". Does that work well with you? That collaboration from DoIT be by request from locals?

MR. IPSEN:

I think it is essential. The same question was asked at me at NASCIO¹¹ just a couple of weeks ago in terms of the role of the CISO. Do you want the authority, or do you want the opportunity?

What I want to do, is, having a lot of faith in the people in the room, we can come up with a collaborative plan that makes a lot of sense.

What is often understated – and I think that Laura stated it well in the beginning – in some cases there are technical challenges that make it not a good idea just to mash everything together. It becomes more costly. I think Rick said that as well.

We have the right people here to be able to analyze this from a business perspective. I think that collaboration is really important. I think we have a mandate though. I think the citizens have created that mandate. I certainly hear it from the Governor's Office – in terms of reducing costs. So, we have to do this. I think it is important to engage all the parties in a collaborative sense, and challenge us to come up with a way to save money – and then capture those costs on the back side once we say we are going to do it.

So, not say, "Oh, we are going to save \$10 here, and then not recover it." I think we need to do that. I think that is the right thing to do.

SENATOR WIENER:

Any additional comments or questions, Board?

Thanks to all the presenters. And thanks for your willingness to take a look at this measure and give us the thumbs up to go forward in the next session with it. It's a huge piece. Sometimes, as Chris said, these aren't headline grabbers, but they are essential for us to do the best work for the people of our State.

So, thank you for coming forward and bringing your willingness to the table. We appreciate that.

We will move on then.

Agenda Item 8 – Board Comments.

SENATOR WIENER:

Are there any Board comments or thoughts. "Collaboration" seemed to be the word of the day, and that's a great one to bring to our meetings.

Agenda Item 9 – Public Comments.

SENATOR WIENER:

Are there any public comments? Anyone wanting to come forward from the public?

¹¹ National Association of State Chief Information Security Officers.

MR. ROGERS:

Madam chair, thank you. I just wanted once again, to thank Mischel Kwon for coming and being here with us today. I also wanted to let you know that she has graciously agreed to stay this afternoon.

She is going to meet with us here in Carson City. So, anyone here who would like to stay, I think we will reconvene at 1:30. It will be in this room – room 3137. So, anyone watching on the Internet who would like to come down and participate, we would like to invite you.

SENATOR WIENER:

Thank you. Any additional public comment from the north?

Agenda Item 10 – Scheduling future meetings.

SENATOR WIENER:

With regard to scheduling future meetings, I know sometimes it is difficult to get us all together. So, Jim, if it is OK, if you would do what you have done in the past? I don't have dates in front of me. With the Legislative session, I am not sure what the Attorney General had in mind. If you would coordinate with Board members for the next, best date, we would certainly appreciate that.

MR. EARL:

I will be glad to do that. It will probably be after the Legislative session, given the fact that it is much, much easier for the Board to operate in these facilities. Thank you.

SENATOR WIENER:

Yes, there is the logistics of that.

Agenda Item 11 – Adjournment.

SENATOR WIENER:

There being no other business coming before this Board, the meeting is adjourned at 12:12 PM.

Respectfully submitted,

James D. Earl
Executive Director

Approved by the Board at its subsequent meeting on September 9, 2011.