

# Minutes of the Technological Crime Advisory Board

September 9, 2011

The Technological Crime Advisory Board was called to order at 10:03 on Friday, September 9, 2011. Attorney General Catherine Cortez Masto, Chairman, presided in Room 3137 of the Legislative Building, Carson City, Nevada and via videoconference in Room 4401 of the Grant Sawyer Building, Las Vegas, 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  
Special Senior Agent Eric Vandersteldt, *meeting designee for Special Agent in Charge Kevin Favreau, Federal Bureau of Investigation (FBI)*  
Assistant Sheriff Ray Flynn, *meeting designee for Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)*  
Assistant Sheriff Tim Kuzanek, *meeting designee for Sheriff Mike Haley, Washoe County Sheriff's Office*  
Chris Ipsen (*Rep. for David Gustafson, Director, NV Dept. of Information Technology*)  
Dale Norton, Nye County School District Assistant Superintendent

## **ADVISORY BOARD MEMBERS ABSENT:**

Daniel Bogdan, U.S. Attorney, Department of Justice (DOJ)  
Nevada Assemblywoman Irene Bustamante Adams  
Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)  
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association

## **TASK FORCE MEMBERS PRESENT:**

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

## **STAFF MEMBERS PRESENT:**

James D. Earl, Executive Director

## **OTHERS PRESENT:**

Jack Homeyer, PSC Consulting  
Brook Doty, NTAC  
James Elste, INOV8V CYBERCQRT  
David Gustafson, Department of Information Technology  
Jeff Rauh, Legislative Counsel Bureau, Audit  
Tim Cary, NDEM

Bob Cooper, Bureau of Consumer Protection, Attorney General's Office  
Lois Hale, InfraGard  
Ira Victor, InfraGard  
Mark Weatherford, Vice President and Chief Security Officer, North American Electric  
Reliability Corporation

### **Agenda Item 1 – Call to Order – Verification of Quorum**

AG CORTEZ MASTO:

Good morning, everyone. We are going to go ahead and get started. I am going to call to order the Nevada Technological Crime Advisory Board, September 9<sup>th</sup> at 10:03 AM. We are going to do a quick verification of our quorum.

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

### **Agenda Item 2 – Public Comments**

AG CORTEZ MASTO:

The next item on the agenda is public comments. We now have public comment both at the beginning and end of this meeting. I would like to invite members of the public if they want to make any comment to the Board, either north or south. Is there anyone? I do not see anyone in the north. Is there any member of the public in the south who would like to address the Board at this time? Alright, seeing no one, we will move on.

### **Agenda Item 3 – Discussion and approval of minutes from the last Board Meeting**

AG CORTEZ MASTO:

I am assuming everyone has received a copy of the minutes. Is that correct Mr. Earl?

MR. EARL:

That is correct.

AG Cortez Masto:

I will entertain a motion at this time.

*Motion to approve the minutes was made by Senator Wiener and seconded by Mr. Norton.*

*The motion to approve the minutes was approved unanimously.*

### **Agenda Item 4 – Reports regarding Task Force and Board member agency activities**

AG Cortez Masto:

Are there agencies that would like to provide information to the Board.

SSA VANDERSTELDT:

I would like to share some information regarding southern task force activities on behalf of the FBI representing the southern task force. Since our last meeting, we have had a significant number of accomplishments in cyber crime related investigations.

Five individuals were arrested federally in various computer intrusion related matters. Approximately two dozen individuals were arrested pursuant to federal child exploitation laws.

Cyber crime prosecutions concluded during this period included the following. In November, a man was sentenced to 97 months in jail for receipt of child pornography. In December, a man was sentenced to 10 years for coercion and enticement of a minor. In January, a man was sentenced to 97 months for receipt of child pornography. In February, a man was sentenced to 10 years for coercion and enticement of a minor. In March, a man was sentenced to 12 years for coercion and enticement of a minor; he had a prior conviction for receipt of child pornography. In April, a foreign national was sentenced to 18 months in prison after pleading guilty to conspiracy to commit access in vice fraud. In May, a man was sentenced to 10 years in jail for coercion and enticement of a minor. In June, a man was sentenced to 78 months in jail for receipt of child pornography. In July, a man was sentenced to 97 months for receipt of child pornography.

These are examples of cases that have concluded prosecution where we worked closely with LVMPD and the Henderson Police Department here in the south.

AG Cortez Masto:

Thank you very much. Just to clarify, that is just in southern Nevada, is that correct?

SSA VANDERSTELDT:

That is correct.

AG Cortez Masto:

Thank you, and thank you for being here. Are there any other comments or reports? We do have someone here in northern Nevada.

MR. CARRY:

I am Dennis Carry, Washoe County Sheriff's Office (WCSO). I want to discuss briefly the northern Nevada task force activities. Similar to the south, we cooperate with the FBI, WCSO, the Attorney General's Office, Carson City Sheriff's Office, Homeland Security Investigations, and other law enforcement entities in the north.

Last year, we conducted well over 30 search warrants involving child pornography leading to the same number of arrests. I do not have specifics on sentences. I do want to touch on a few of these individuals who are still pending sentencing.

We came across one individual through a child pornography investigation that led us to multiple contact offenses in the past where this individual had been kidnapping and raping small children throughout California. There are at least five incidents where this appears to have occurred until we captured him.

Besides child pornography, we are seeing an increase in individuals involved in network intrusion. We are coming across individuals who are associated with groups identified in the media, the hacking groups Anonymous and other similar groups. Individuals are starting to look at how to participate. We recently investigated an individual from this area, in Carson City actually. That case is still pending so I can not describe too much. However, he had an active interest in the hacking group Anonymous and was taking an active role in targeting what the group was suggesting to target. This was not a child pornography investigation, and indicates that cyber crime individuals are involved in many other activities. Some believe that this will not happen in our back woods, but these individuals are in the State, just like everywhere else. Thank you.

AG Cortez Masto:

Thank you, are there any comments or questions? Are there any other comments from task force members? Seeing none, we will move on to Agenda Item 5.

**Agenda Item 5 – Update by Robert Cooper, Senior Regulatory Analyst, Consumer Protection Bureau, regarding the Cyber Security Findings Approved by the Public Utilities Commission on NV Energy Application, Advanced Service Delivery Project [Smart Electric Grid Implementation] Regarding Cyber-Security**

AG Cortez Masto:

This is an update by Robert Cooper, a Senior Regulatory Analyst in my office, regarding the cyber security findings approved by the Public Utilities Commission on NV Energy's Application, which, if you recall, is called the advanced service delivery project or the smart grid implementation, regarding cyber security.

We had a presentation by NV Energy last year regarding the smart grid and some follow-up. Mr. Cooper is here to give us an update. Thank you for being here.

MR. COOPER:

Thank you Madame Chair and members of the Board.

My name is Bob Cooper. I am an analyst with the Attorney General's Bureau of Consumer Protection. Our office represents the residential and small business ratepayer customers of Nevada utilities before the Public Utilities Commission. I do not have a formal PowerPoint today. I am here mainly to give an update on the status of the smart grid application process in Nevada and some of the updates that have been made to that application.

By this time next year, NV Energy will have replaced nearly every electric meter in Nevada. That is almost 1.4 million meters that will have been replaced by smart meters. Almost half the cost of this replacement was covered by a matching grant from the federal Department of Energy. Those grant funds were made available under the American and Recovery and Reinvestment Act, ARRA. A number of utilities took advantage of that matching grant funding opportunity. Therefore, we have a number of utilities that are facing cyber security challenges similar to what NV Energy is dealing with this year.

Because NV Energy is somewhat at the end of the chronological process that DOE is bringing utilities through, NV Energy has been able to learn some of the best practices that have been developed around the country as other utilities confront cyber security challenges. We are getting the benefit of those best practices in terms of updated filings that have been made with the Public Utilities Commission (PUC).

To back up a little bit, your agenda description has it just right. NV Energy is calling the whole smart meter deployment "advanced service delivery" because of the number of different broadband technologies that have to be integrated in order to bring these advanced services together. Examples of some of those services include someone reprogramming their thermostat from their office, or from their smart phone, or even from their home area network, right down the hallway from their thermostat. Given those different levels of broadband deployment, there will be a number of cyber security complexities that the utility is still working on.

I would like to briefly update you on the PUC status. The PUC approved last year the entire advanced services deployment, the \$160 million that Nevada ratepayers will be asked to pay and the \$140 million that the Department of Energy is contributing. All of that was approved by the PUC.

The only extend of their approval of the cyber security part of that application was to acknowledge that it would be the federal Department of Energy that would be passing judgment on the cyber security on the cyber security aspect. That was one requirement of the federal matching grant – that a satisfactory cyber security plan be filed and approved by the Department of Energy.

So, at paragraph 260 of the Commission's order of last year, in docket 10-02009, the Commission acknowledged that approval had been received by the Department of Energy.<sup>1</sup> But the Commission did go a step further. It held the docket open as the informational body for cyber security matters. So, these updates have been coming in, in that docket, and they are publicly available. The Commission is going to be requiring additional updates as the technology evolves and the systems are tested.

There was an update last year on the privacy aspects of cyber security that the company made. Basically, they promised to follow the NIST standards, the National Institute for Standards and Technology. Under cross examination last year, the cyber security witness for NV Energy, Mr. Gary Smith, indicated that they were very conscientiously following all the NIST guidelines to the best of their ability and they would be providing updates to the Commission as those guidelines evolved.

We were encouraged to see that. We were encouraged to see the NIST monitoring on the privacy aspect, and, most recently, an update was made last month on the AMI<sup>2</sup> network and the security testing for several aspects of their AMI network, including the home area network component of the broadband deployment.

They hired a third party to do that test, World Tech Labs, in Vancouver, Canada. They tested in Canada, they tested here at NV Energy. They found some bugs that they are debugging. They performed a number of simulated malicious attack scenarios. I think we will hear more about that later this morning from Mr. Weatherford. They are in the process of debugging some of the problems they encountered. They indicated last month that they will be filing an update to last month's report regarding some of the steps they will be taking to remediate those problems.

So, we are optimistic that things are being looked at. They have hired a third party to review the work of World Tech Labs, so there is kind of a second level of checking. Again, we will be receiving additional remediation documents. We will be sharing those documents with Mr. Earl and member of the task force when they become available. With that, I am available for any questions you might have. I appreciate the opportunity to provide this update.

AG Cortez Masto:

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

MR. IPSEN:

I have a quick question regarding the validation testing. You mentioned there were a couple of entities, one of those being World Tech Labs as a validator of the security controls that Nevada Energy has put into place. Do you know who the second entity is, and, secondly, are they validating to any standards? Are they producing a report? You mentioned that those validation reports would be available?

MR. COOPER:

We haven't yet learned the name of the second validating entity. Some of that work is being done and will be filed, we understand, in the next couple of months. The only standards I am currently aware of are the NIST standards.

---

<sup>1</sup> Paragraph 260 provides:

*In response to a request from the Presiding Officer, the Companies submitted their Cyber Security Plan that was approved by DOE. The commission acknowledges the receipt of this Plan. Such receipt shall not be construed as Commission approval of this Plan.*

<sup>2</sup> AMI: Advanced Metering Infrastructure, electrical meters that measure more than simple consumption and an associated communications network to report the measurements. (Wikipedia)

AG Cortez Masto:

So, Mr. Cooper, just to clarify. The PUC has retained some sort of oversight with respect to the cyber security issues involving the smart grid, is that correct?

MR. COOPER:

They have retained an open docket for the purposes of filing and transparency. They have signed off on the cyber security plan that was approved by the DOE by simply acknowledging it was filed and met the DOE requirements. They have not gone any further than that in regard to cyber security matters other than leaving the docket open, which is kind of an extraordinary step for them to provide that extra level of transparency. But, as of right now, I am not aware of any adjudicatory process that is contemplated by the Commission in respect to cyber security matters.

AG Cortez Masto:

Are there any other questions or comments?

SENATOR WIENER:

Madam Chair, thank you. As I hear about the reports that are being made public and this on-going transparency, I am curious as to the level of information that is being provided publicly. At what point is it protected information? We don't want to put out data and reporting results that could actually jeopardize the system.

MR. COOPER:

That is a great question. A lot of the material has been redacted. The company is working with a third party vendor called Sensys as well as IBM and some of the other vendors I mentioned in addressing their cyber security issues. I think they are working hard to keep matters protected where that is appropriate because of the risks that are involved.

That being said, our office enters into confidentiality agreements all the time with the company, and we do strive to provide an extra level of review of the confidential documents.

AG Cortez Masto:

Thank you, and just one follow-up to Senator Wiener's question. Literally, other than the Department of Energy, there really is no oversight for NV Energy's cyber security program, or the means they are using to try and protect the information.

MR. COOPER:

That is exactly correct.

AG CORTEZ MASTO:

Okay. Thank you. We appreciate your presentation.

**Agenda Item 6 – Presentation by Mark Weatherford, Vice President and Chief Security Officer, North American Electric Reliability Corporation (NERC), Introduction to NERC, its Mission, Relationship to Other Government Agencies and Private Providers, and Cyber-Security Issues Confronting the Electric Grid**

AG CORTEZ MASTO:

Moving onto Agenda Item number six, we have a presentation by Mark Weatherford, Vice President and Chief Security Officer of the North American Electric Reliability Corporation (NERC). He is going to provide an introduction to NERC. Welcome, Mr. Weatherford.

MR. WEATHERFORD:

Thank you, Madam Chair, and thank you for inviting me here to Carson City today. It was good to get out of DC. We have had so much rain the past week that I received some photos from one of

my staff this morning, showing that he had been “islanded” and could not get to work. He was surrounded by water.

I’m one of those lucky people in life whose work is his passion so if I run past the two hours Jim has given me, please forgive me. Just kidding.

My name is Mark Weatherford. I am currently the Vice President and Chief Security Officer for the North American Electric Reliability Corporation. I will talk a little more about NERC when I actually start the presentation.

As background, I spent a career in the United States Navy where my last job was leading worldwide Navy Computer Network Defense operations and directing the Naval Computer Incident Response Team. In 2005, I was hired by Colorado Governor Bill Owens to stand up the state’s first information security program and following the 2006 elections, was asked by Governor Bill Ritter to continue in my role as the Colorado Chief Information Security Officer. In 2008, I joined the Schwarzenegger administration in California as the state’s first CISO and built the enterprise state government security program there. I am also the former CEO of the Denver InfraGard Members Alliance.

While in both Colorado and California I worked with Chris Ipsen quite a bit on a variety of security issues and continue to seek his counsel on important issues today. Chris is one of the thought leaders in the security community and very well respected across the nation. I think that is kudos to Nevada. In fact, I’ve tried to hire him on two different occasions but he declined to leave Nevada.

Coincidentally, and sometimes timing is everything, SysCon Media just announced yesterday their Most Powerful Voices (MPV) in Security. Your very own Chris Ipsen is in the Government Top 10 Most Powerful Voices in Security along with US Senators Susan Collins and Tom Carper, US Representatives Darrell Issa and Mac Thornberry, and DOD Deputy Secretary William Lynn. So, that really is a big deal.

MR. IPSEN:

I didn’t prompt this. [laughter] I think Mr. Weatherford is on that list as well. He’s definitely a respected voice and a person I use quite a bit.

MR. WEATHERFORD:

I’m going to tell a few scary bedtime stories today but not for the purpose of creating fear and uncertainty. Rather, they are part of the message about where we are from a technology perspective and how we need to create cultural momentum across the nation to come to grips with the new normal as related to cyber security.

What I mean is that, until technology matures to the point where cyber events are the exception rather than the rule, and people like Chris and I no longer have full-time jobs, our primary organizational cyber security goal should be to become targets of opportunity rather than targets of choice. I don’t mean to sound un-empathetic but we don’t have to outrun the bear, we just have to outrun our buddies. To do that we need to be working to raise the security barrier so high and make it so resource intensive that bad guys go somewhere else looking for easier prey. That doesn’t mean we gold-plate everything we do, but rather that we manage to an appropriate security risk posture for our specific organizations. Because state governments transact and possess so much sensitive citizen information, I believe we have a higher level of responsibility and can collectively be called negligent if we don’t understand and actively address the security risks.

When I worked in state government the two most frequent questions I received from both executive branch leadership and legislators were:

- If we give you a budget and funding for these products and services, will they eliminate our security problems? And;
- Is the state safe today?

The answer to the first question is “No”, money doesn’t solve the problem. And the answer to number two, unfortunately, was always, “I don’t know how secure the state is today.”

In attempting to answer why spending one-time funds on security doesn’t eliminate the problem, my explanation was, and continues to be, that security is a journey not a destination. As technology changes and creates opportunities for greater efficiencies in our government and private sector organizations, the threats also change and new vulnerabilities are introduced. Very simply, the security things I worry about today are not the things I was worried about 12 months ago.

Regarding the second question, I don’t know of any state government security program that is mature enough, with all of the necessary security controls in place and with visibility across the entire enterprise that can confidently say, “Yes, we are secure today.” There are simply too many variables and the cost is too high to mitigate our risks to zero. I’ll talk about it a little more later but when we see very mature Defense Industrial Base companies and advanced security companies that have security events – very high profile security events – it makes me concerned about where we are.

I am happy to see Nevada making so much progress. It is very encouraging to see pro-active activity like your Senate Bill 82.

That’s enough of an introduction so I’d like to now launch into my actual presentation. What I’m going to very briefly talk about today is NERC and the role we play in the electricity industry, and then, more generically about some cyber threats, and the things that we are doing and what others can be doing.

**Who is NERC?**

- NERC is an international, independent, not-for-profit organization
- Mission is to ensure the reliability of the bulk power system in North America.
- Electric industry’s “self-regulatory organization” for reliability
  - Balances the interests of all stakeholders
  - Represents industry consensus
  - Independently acts in the best interest of reliability

NERC is an international, independent not-for-profit organization. Our mission is the reliability of bulk power.

My being here today is quite coincidental with the power outage in California yesterday afternoon. I spent probably 8 of the last 14 hours on the phone dealing with a variety of related issues. We talked earlier about the impacts of that. The FBI and DHS released a joint product yesterday talking about al Qaeda and potential attacks related to the upcoming 9-11 anniversary. There were many people quick to tie the power loss event in San

Diego together with a potential al Qaeda event. We get involved in all that. I work very closely with Department of Homeland Security and the FBI in Washington DC.

We are the self-regulatory organization for reliability for the industry. What I mean by that is we are the electrical reliability organization for the United States. NERC essentially sits between the federal government and the private sector to ensure that industry is managing to and meeting the compliance requirements of the standards as part of the ERO. Unfortunately, sometimes the federal government doesn’t think we are being strong enough on the private sector, and the private sector always thinks we are being too strong. This puts NERC in an interesting position quite often.



### Importance of Bulk Power System

- Electricity is arguably the most critical of all critical infrastructures in North America.
- As important to modern civilization as water was to ancient Rome\*—impossible to calculate our dependency on electricity.
- An extended loss of electricity could result in unprecedented human suffering, economic devastation and profound gaps in national security.

\* For an interesting historical perspective, read [...shameless plug...]  
 "4 Things The Roman Aqueducts Can Teach Us About Securing the Power Grid."

Electricity is arguably the most critical of all critical infrastructures. When you think of your day-to-day lives, and you try to think how you would operate without electricity, I think you would quickly conclude that, in fact, modern society is completely dependent on electricity.

I get into interesting conversations with my colleagues in other critical infrastructures as to who is the most important. Perhaps water, and the delivery of water is important, but, obviously, they need electricity to deliver the water.

I now have a shameless plug. Mike Assante<sup>3</sup> and I wrote a paper a couple of years ago about the Roman aqueducts and how important water was to ancient Rome. That paper created an analog to electricity in modern times. I think this is an appropriate analogy.

### The "Largest Machine in the World"

**The North American power grid**

- 3 Major Interconnections
- 8 Regions
- 135 Balancing Authorities
- more than 5,000 companies
- more than 160,000 miles of high-voltage transmission lines
- more than 1,000,000 miles of distribution lines
- representing more than \$1 Trillion in assets.
- real time capacity more than 4B kilowatt hours (KWh)
- delivering electricity to more than 334 Million people
- who spend more than \$365 Billion per year for electricity


Electricity is called the "Largest Machine in the World" – the grid in North America. When I say "North America", the northern American power grid includes all of Canada as well as a small slice of northern Mexico. This is in Wikipedia. You can look it up, so it has to be true. Right?

The North American power grid has 3 major interconnections across the continent. There are 8 regions and 135 Balancing Authorities. It is important to note these entities because, as we speak, there are thousands of people across the nation making minute changes to generation and

delivery of electricity to ensure we electricity is level on the grid [without peaks and troughs, or surges and drops in power].


### Fundamental Principle of the Electric Grid is **BALANCE**

**Generation**  
(fossil, nuclear, hydro, renewable)



+

**Transmission**  
(Hi-voltage lines)



NERC's mission is to ensure the reliability of the Bulk Power System which includes all generation and transmission in North America

Electricity obeys the laws of physics, moves at the speed of light, and must be consumed the instant it is produced – called the "millisecond industry"

There are more than 5,000 companies that play some part in bulk power. There are more than 160,000 miles of high-voltage transmission lines and more than a million miles of distribution, representing more than \$1 trillion in assets. Electricity is a big deal and a big business in North America.

The fundamental principle of electricity is balanced generation and transmission of people's distribution. There is a lot of activity that happens in real time to make sure that power flows are in fact balanced.

Power is called the millisecond industry because the electricity powering the lights in this room right now was generated two or three seconds ago somewhere in the country. It may have been in Canada. It may have been in Tennessee. But, somewhere in North America, the electricity powering this room right now was just generated.

<sup>3</sup> Mike Assante is currently the President & Chief Executive Officer of the National Board of Information Security Examiners (NBISE) and Chair of NBISE's National Board. He was formerly Vice President and Chief Security Officer at the North American Electric Reliability Corporation.

As I mentioned, NERC's mission involves bulk power. This does not include anything on the distribution side of the grid. This presents an interesting conundrum as we talk about the smart grid. Much of the activity regarding the smart grid at present is on the distribution side. Certainly the meters, the AMIs and the smart meters, are on the distribution side of things.

While I have no responsibility for, or authority over, smart meters, I work closely with – and am working more closely with – the Public Utility Commissions in the different states because PUCs generally have the authority and control over the distribution side of the power network.

The world has changed...

“...it is necessary to consider whether the rapid adoption of the Internet has provided so considerable an asymmetric advantage to our adversaries that it can change the course of American history.”

Steve Chabinsky  
Deputy Assistant Director, Cyber Division  
Federal Bureau of Investigation

The world has changed. I saw this quote. Steve Chabinsky is the Deputy Assistant Director of the Cyber Division of the FBI. I work with Steve quite a bit. He wrote a paper a while back. This quote really goes to the heart of technology in general and not just technology as it relates to critical infrastructures.

We have come so far so fast, that some of us often wonder if technology hasn't gotten too far in front of our ability to protect what the technology runs.

This is part of my daily life – dealing with issues in the media. There is a lot of it. Almost every day I receive multiple inputs from both print and voice media. The result of this is lots of legislative activity. I have been involved with legislation at the state level, but being in Washington DC has given me an entirely different perspective on the legislative process.

Power Grid Threatened...Really?

We have testified four times before Congress, both the House and the Senate this year alone on a variety of different bills. At last count, there were over 20 different pieces of legislation introduced so far this session that had some component dealing with cyber security. Many of them are focused on the electricity sector.

Proposed Cybersecurity Legislation

- NERC has testified four times since February to four different congressional committees.
- Bills address cybersecurity emergencies and vulnerabilities as well as information sharing, defense facilities and GMD/EMP.
- Senate Energy and Natural Resource Committee passed the Senate Grid Cybersecurity Act on May 26<sup>th</sup>.
- House Energy and Commerce Committee is considering action on "The GRID Act."
- House and Senate Homeland Security Committees considering comprehensive approach with DHS as lead agency.
- White House cybersecurity bill

The White House sent a bill to the Congress. I believe Senator Reid has it now. It is new legislation that is very comprehensive. We are working with a variety of congressional staffs to see how these various pieces of legislation might fit together, and how they might be distilled into an omnibus piece of legislation. We are still waiting to see what happens to that. The Congress has been a little distracted with other things lately.

I want to talk now about some cyber specific topics. Until about 4 months ago, I tweaked this slide every now and then. I added just one more thing. Then, I grew more concerned. The Google attack happened in January 2010. This is a lot of high level activity that happened in a relatively short period of time – less than 18 months. This is unprecedented in our business – to see these large attacks occur so quickly. Many of these are unrelated, but just the fact that they happened concerns me greatly as a cyber guy.

### A disturbing trend... 4 months ago

	<b>Google</b> (Operation Aurora)	They proactively and publicly identified an intrusion. The primary goal of the attacker was to access and modify source code
	<b>Stuxnet</b>	Highly sophisticated attack on control systems hardware. Target specific through common USB attack vector
	<b>WikiLeaks</b>	Takes advantage of data breaches and the insider threat. Exposes national security and diplomatic information
	<b>Anonymous</b>	Retaliated against HBGary by defacing website, plundering internal e-mail and then publicly posting it online
	<b>Night Dragon</b>	Sensitive IP stolen from energy companies. Attacks appeared to originate from computers in China
	<b>RSA SecurID</b>	Security of over 40M 2-factor tokens at risk after cyber-attack

The last 4 months have taken us to an entirely new level. The things that concerns me most, and we have read about all these attacks, is that they are very high level events. I am also concerned about what we don't know. These are the ones that are reported on and discovered through various means. It is the unknown issues that have always scared us. Chris and I have talked about this. It is one of the things I worried about in both Colorado and California – the events that were occurring that we did not know about because we did not have the visibility of them. We did not have the tools, the services, or the necessary talented people to

discover some of the things that were happening below the radar.

You only report what you know about.  
What don't we know about?  
... last four months

Most of these events are associated with Anonymous, mentioned in one of the earlier reports this morning. In fact, all of these are associated with the Anonymous hacktivist group and LulzSec, a branch of Anonymous. I don't like to talk about this very openly because I am afraid that I could become the next victim. I have already said more than I ever say in public. It is something for us to be concerned about. While these events did not cause any catastrophic outages, they caused these companies a lot of money to remediate and also from a public perception about them.

Here is another interesting thing. I don't want to take a lot of time, but I believe it is important. The world's largest legitimate cloud provider continues to be Google. Amazon and Rackspace are the second and third largest.

### The enemy within...

The biggest *legitimate* cloud provider in the world is **Google**, made up of 500,000 systems, 1 million CPUs and 1,500 gigabits per second (Gbps) of bandwidth.

**amazon.com** is the second largest cloud provider with 160,000 systems, 320,000 CPUs and 400 Gbps of bandwidth.

In third place is **rackspace** with over 65,000 systems, 130,000 CPUs and 300 Gbps of bandwidth.

The **Conficker** botnet controls 6.4 million computer systems at 230 top level domains globally, more than 18 million CPUs and 28 terabits per second of bandwidth.

<http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/>

The Conficker botnet actually controls more actual computers than the legitimate cloud service providers. I had a conversation about two weeks ago with Rodney Joffe, who is the leader of the Conficker working group. This number is a little out of date, but he told me that there are over 4 million botnets that are active. The disturbing thing he said was that, as they do investigations and forensics, they consistently find computers that are compromised not only with Conficker, but with a variety of other things. Most of these "other things" are malware or vulnerabilities that standard computer hygiene would fix. We have patches for these things. We have antivirus signatures for. The

computers are simply not being taken care of. They simply are not having hygiene applied to them. That is concerning – when you know the answer to the problem and people in the private sector, and in government, quite frankly, are not taking advantage of available solutions.

NERC is a compliance organization, as I mentioned before. This has been a bit of a challenge for me, as a cyber security guy coming from California and Colorado. My role there, much as Chris's role here, was to help state agencies raise the security bar, float the security boat a bit higher.

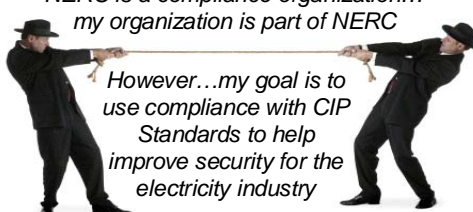
Since I am part of a compliance organization, people want to keep me at arms' length. They are very reluctant to share information with me. One of my challenges has been to break down those

communications barriers with the private sector within the electricity industry. I don't know that we will ever completely get over that hurdle as long as I am part of the compliance organization. But, we are making progress on this problem. This involves constant evangelism on my part.

**Security vs. Compliance**

*NERC is a compliance organization...  
my organization is part of NERC*

*However...my goal is to  
use compliance with CIP  
Standards to help  
improve security for the  
electricity industry*



NERC  
NORTH AMERICAN ELECTRICITY RELIABILITY CORPORATION  
1000 M STREET, N.W. WASHINGTON, D.C. 20004  
703.286.7000

The electricity in North America is one of only two industries that has mandatory and enforcement compliance standards as directed by the federal government. While NERC has been in the compliance business for a long time, it has not been in the cyber security business for a long time. In fact, we just developed standards for the electricity industry, bulk power specifically and not distribution, that became enforceable only in 2010. So, we are just beginning the compliance process across the sector regarding the CIP<sup>4</sup> standards. These are the product of an evolving standards process. This has been a bit of a hurdle, as you

can imagine. Organizations that previously had no oversight, at least no federal oversight, no do have federal oversight.


NERC has very broad authority to issue fines to the private sector entities that are not in compliance with the CIP standards.

**Building on Critical Infrastructure Protection Standards**

We know - That mandatory reliability standards are necessary – self regulation doesn't work without an economic incentive

So it's inferred - That compliance equals good security

The reality is - That standards are not sufficient since they only tell you "what to do" and not "how to do it"



STANDARDS

The last bullet is really the important one. From a cyber security perspective, standards are not sufficient since they only tell you what to do and not how to do it. This is really the right way standards should be followed.

Here are some of the things that I have been working on and leading within NERC. These are the critical infrastructure protection initiatives – obviously starting with standards. This is our highest priority. It is the thing that forms the basis of daily interaction with the federal government.

**NERC CIP Priority Initiatives**

CIP Standards

ES-ISAC


- Threat research, analysis and industry information sharing
- DHS/DOE/DOD information-sharing relationships

Security Training, Exercises and Outreach

- National cybersecurity security exercise (GridEx 2011)
- Electricity sector security conference (GridSecCon 2011)
- Sufficiency Review Program (SRP)
- Cyber Risk Preparedness Assessment (CRPA)

High Impact, Low Frequency Events

- Cyber Attack Task Force
- Severe Impact Resilience Task Force
- GeoMagnetic Disturbance Task Force
- Spare Equipment Database Task Force



Then there is the Electrical Sector Information and Analysis Center (ES-ISAC). The ES-ISAC is one of a number of different ISACs. Each critical infrastructure has an appointed ISAC. The ISAC role is pure information sharing – from both a push and a pull perspective. Over the past 6 months, I have raised the visibility of the ES-ISAC. We continue to do that with a very robust information sharing portal that is evolving. It is getting more and more complex. We are able to create communities of interest with very rigid access control for the different communities. This is much like the initiative Jim has mentioned to me, and I can't recall its acronym.

<sup>4</sup> Critical Infrastructure Protection.

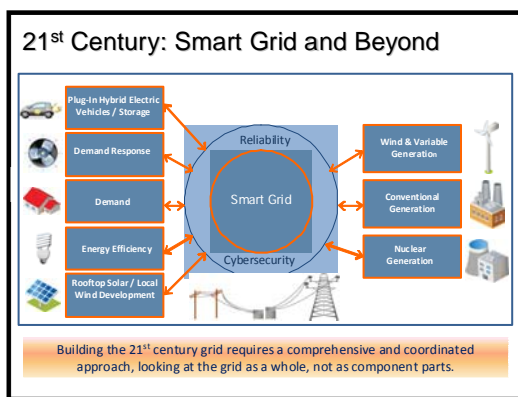
The point is that the ES-ISAC is one of several, and we do share a lot of information among the various ISACs. We have relationships with the Department of Homeland Security and a variety of other government organizations.

As I mentioned earlier, evangelism is a huge part of my job – getting out there and providing training to industry. I still find that we still have, and this number is a little bit fuzzy, fewer than 20 large electricity companies that provide the majority of electricity in North America. So, if about 20 companies provide the majority of electricity, this means there are about 4,980 companies providing the minority of electricity in North America. Some of these companies are very, very small. They do not have a lot of resources to devote to cyber security. Their job is to run their business.

I have taken it as part of my job to help these smaller companies, much as a state CISO would help some of the smaller agencies, boards and commissions improve their cyber security posture. One of the things I have done is to begin to reach out to some of these small companies with training and exercise initiatives. I list here the Sufficiency Review Program and the Cyber Risk Preparedness Assessment. These are things my staff is working on with individual companies in order to help these companies understand not only the standards but how they can go above and beyond the standards to mitigate risks above and beyond what the standards call for.

In June 2010, NERC and DOE issued a joint high impact, low frequency event report. That report identified four major occurrences that would be considered very high impact even though they may have never happened. These are things, from the perspective of the electricity sector, we should be thinking about and planning for. Those four things were a coordinated cyber attack against the electricity sector, a coordinated physical attack against the electricity sector, geomagnetic disturbances and a pandemic.

I joined NERC in July 2010. I received the report. We have established task forces that are working on developing white papers and recommendations for the electricity sector on how we can best address some of these high impact, low frequency events across the sector. All four of these task forces should wrap up in December of this year. I am expecting the delivery of public white papers some time early next year.



I am going to talk a little about smart grid even though I really have no authority or responsibility for the distribution side of things where most of the smart grid activity is taking place right now. But the smart grid is important to me for a couple of reasons.

As I mentioned earlier, electricity is a very simple model. There is generation, transmission, and distribution. Generation involves a relatively limited number of finite entities. There are fossil fuels, nuclear power, hydro power, and we are now adding in renewables. Renewables add a completely new complexity to electricity generation. First, they are very variable. The wind blows during the day, and, typically, does not blow a lot at night. Sun shines during the day. There is no solar activity at night. Planning around variable energy sources is an entirely new challenge for the electricity sector.

From a cyber security perspective, the smart grid adds new challenges because it greatly increases the attack surface. The smart grid aggregates many new end points. It forces us to take actions based on things that we had no control over previously.

So, where previously, we had very few generation sites, a very small number of touch points into the grid, the smart grid creates millions and millions more access points into the grid.

One of the things that concerns us from a bulk power perspective is that while we don't have any reach-back into the distribution of electricity, the simple fact that we are now creating all of these new end points in the distribution system can affect the load. It can affect the feedback into the bulk power side of things.

For example, if you have a million smart meters that go off line because they were hacked, then, all of a sudden, the bulk power side has to adjust immediately how much transmission and generation should take place on the grid. So, there are increasing dependencies across distribution and bulk power. In the future, we will see more interaction from a pure cyber security perspective between these two disciplines.

**Smart Grid presents new opportunities for a secure and resilient network**

- Build Security In!
  - Confidentiality, Integrity and Availability - best practices
- Apply network security lessons-learned from the past 40 years
  - Need innovation in technology, process and people
  - Authentication and authorization of all transactions (no anonymity)
- Holistic Approach – Make security an integral part of the smart grid



That's the bad part of smart grid development. As we heard earlier, the good part is that with the smart grid we have an opportunity not only to capture the efficiencies on offer but to draw lessons learned from the start so we can build cyber security into the infrastructure. When smart meters first came out 3 or 4 years ago, there was a rush to market. We got a little ahead of ourselves from a security perspective. Now the vendor community as well as companies deploying smart meters recognize that there can be significant vulnerabilities if one takes a willy-nilly approach by just throwing smart grid appliances out there. So, there is a much higher level of awareness that we

need to do this right. We need to ensure that the appliances and devices we are putting out there do have security built into them or have their security vulnerabilities mitigated before deployment.

As was mentioned, the NIST smart grid standards are, so far as I know, the only standards for smart meters right now. This is what most people are using.

**Cybersecurity Challenges in all Critical Infrastructures**

1. All networks are contested territory – **BELIEVE IT!**
  - Lack of vivid nature of the risk
2. Are we protecting the correct assets properly?
3. Is funding appropriate to mitigate cyber-risk?
  - Unfunded mandates can result in significant cost impact to businesses, industries, and society
  - Mandates with cost-recovery may require public trade-offs
4. Compliance rarely leads to good security, but good security almost always leads to compliance.
5. No one can afford 100% risk-free security environments and they **DO NOT** exist



Cyber security challenges must be faced by all critical infrastructures. One of things I tell people all the time is that all networks are contested territory. Historically, there has been a divide between what we call our business/administrative networks and the control system that works in our SCADA networks. That line is beginning to blur a little bit because of the efficiencies that can be realized. I am still not an advocate of tying our control system environments to our business environments. In fact, we are starting to see a little bit of pull back from that because of the vulnerabilities that are introduced. The last thing we want is the same

vulnerabilities we see on the Internet that affect all the computers in this room being transferred to the control system environments where it really matters and people can die if things go wrong.


Bullet number 3, "Is funding appropriate to mitigate cyber risk?" has two components. I worry, on the legislative side, about placing unfunded mandates on industry. The money has to come from somewhere. Nothing is free. I can't say the industry is struggling, but companies have to account for things. They have to account for how they spend their money. So, there are unintended consequences to legislation that requires the private sector to spend money that can not be recouped in some fashion.

On the other hand, mandates for cost recovery require a public trade off. In many cases, if a PUC or a standard requires an industry to spend money, the industry will seek to recoup those costs. Typically, this results in higher fees for the public that is paying for the electricity.

I am sure Chris has said this more times than you care to hear, but we can not afford a 100% risk-free security environment. They simply do not exist. Our job is to take a risk management approach and identify what is most important to us and manage to that risk.

**Things That Keep Me Awake...**

- Network convergence of IT and control systems
- Internet "everything" means "Cyber" everything
- State-sponsored hackers and organized crime
- Insiders and greater reliance on third parties
- More sophisticated malicious code (Stuxnet)
- Complex and indecipherable supply chain
- Over publication of sensitive information
- Explosion of wireless communication
- The myth of perimeter defense
- Over-reliance on the Internet



Things that keep me awake are the same things that keep every cyber security person awake. Our IT and control systems environments are converging. That bothers me, although, as I said a second ago, I think we are seeing some pull back on that.

Internet "everything" means "cyber" everything. So, anything connected to the Internet accepts the same vulnerabilities as everyone else.

I would include hackers in state-sponsored and organized crime – Anonymous and similar organizations.

Insiders continue to be a problem. In fact, many studies done over the years – and I continue to believe this – show the majority of our security-related events are the results of insiders, whether malicious activity or simple ignorance.


Sophisticated, malicious code includes Stuxnet. This was an eye opener for us last year. We continue to worry about Son of Stuxnet. Stuxnet code was released into the wild very quickly. We haven't seen any follow up yet, but we expect it.

Complex and indecipherable supply chain: we don't know where all the components that are embedded into our electronic devices come from. The intelligence community is very concerned about this.

A lot of things keep me awake. These are some of the more important ones. I suggest that no one in the cyber security business would argue with any of these.

**What to do?**

- Don't give up
- Train your people
- Don't ignore the cyber-threats
- Know your cybersecurity resources
- Include security in all state government technology planning
- Take a brave pill and ask hard questions



So, don't give up. Keep spending money and training your people. Do not ignore the threats. Know your resources. I think that is one of the things the security community is good at. I still talk to Chris on a regular basis even though we are in completely different geographical locations, and, now, even different sectors. But we share information all the time.

Include security in all of your technology planning. This continues to be a struggle. I know it certainly is in state government. In California, at one point, we had over \$8 billion of on-going IT projects in the

state. It was everything I could do and more to keep my fingers (or some one on my staff, or some one I knew on some body else's staff) involved in all these projects to ensure the right security questions were being asked.

The worst thing in the world is to deliver an IT project and have some body say, “Jeez, you know what? We didn’t think about the security implications of this.” It makes everybody look bad, and it certainly doesn’t look good on a resume.

Finally, I think we need to take a break and ask hard questions. We really do need to ask those kinds of questions that are sometimes uncomfortable – from both the executive side and from the technology side.

That is all I have and I would be happy to take questions.

AG CORTEZ MASTO:

Thank you, Mr. Weatherford. Are there any questions or comments?

MR. IPSEN:

First of all, Mark, thank you. It was a great presentation and reflective of why you are so prominent in this industry. It is certainly an eye opener. It makes me feel proud to know you are there guarding the electric grid.

I do have one question for you. You presented an interesting paradigm we face all the time. That is the standard versus law and regulation, the enforceability of those standards. Can you expand your thoughts a little bit on that? I know that with the passage of SB 82 – and we will have a report on that in a little bit – it has changed my mind set. You mentioned that you have a little bit more authority to move forward with some of the standards. Can you talk about some of the challenges and opportunities that presents?

MR. WEATHERFORD:

Well, yes. Thank you, Chris. Standards are interesting. This is the first job I have had where I actually dealt with standards relating to cyber security. It has been challenging. I will not hesitate to say that.

Standards are normally thought of as static and long standing. You create a standard for something – the size of the light bulb is a standard that never changes. In the cyber security world, standards do change. The threat changes. I think we have to be very careful. As I said earlier, there are unintended consequences for going down the wrong road with standards.

The other thing we have to be very careful of is creating a compliance mentality where all people want to do is check a box to address whatever the standard said they had to do and nothing more. This is something I have to deal with regularly within the electricity industry. Standards are very explicit. If an auditor or an operator is looking at complying with a standard and it says, “Do A, B, and C,” but D might add more security to the overall posture, they may not do D. There may be as cost associated with it. There may be other resources associated with it. There may be compliance requirements associated with it. So, while doing D may make security better overall, they are hesitant to do it because it goes above and beyond what the boxes on the form call for.

One of the other projects I am working on is a set of security guidelines. We are working with DOE and NIST on some voluntary guidelines that I see sitting on top of the standards. This would say, in effect, once you meet the base line security standards for critical infrastructure, there are guidelines above that. You can pick and choose from them using your risk management perspective. If you are in this kind of environment, your risk may be a little higher, so you may want to do something else. There is anxiety around this. There is a concern that the guidelines could become standards at some point, but that is not my plan. That is not my goal in identifying guidelines. I think that would take away the flexibility companies have to respond to the actual risks faced by them in their separate environments.

AG CORTEZ MASTO:

Mr. Earl?



MR. EARL:

Mark, I would like to follow up on that, particularly in relation to the guidelines sitting on top of standards, particularly NIST standards. Both you and Bob Cooper before you talked about the fact that many electric companies on the distribution end are essentially bounded by the NIST standards.

As you know, over the past several legislative sessions, the Nevada legislature has incorporated NIST standards by reference to meet exactly the sort of challenge you identify. That is, the threats change. The NIST standards change. So by incorporating NIST standards by reference we are able to stay more or less abreast.

My concern is that NIST standards are essentially the result of a consensus decision or series of decisions that NIST rides herd on. Is that true, and, if so, if there is a consensus driven standard, clearly in certain industries, you get agreement over something that is very low. I am presuming that is one of the drivers responsible for you looking at guidelines that would sit on top of standards. Is that roughly right?

MR. WEATHERFORD:

That's why you are a smart guy, Jim.

Yes. I don't know that I can address whether the NIST standards are consensus driven. I think you would have to define what "consensus driven" is. NIST is an organization that develops standards. That is one of the things that they do. They do take a lot of input from industry and from other subject matter experts in the standards development process. If that is what you mean by consensus driven, I would say they are consensus driven.

Much like the critical infrastructure protection standards that we utilize are industry driven. Let me rephrase that. They are industry developed. So, a lot of people think NERC develops these standards. We don't develop the standards, we follow the ANSI<sup>5</sup> model, and the ANSI model is a consensus model. We, or the federal government, say, "You need a standard on X." Industry puts together a team of subject matter experts. They go out and develop the standard.

There is some on-going discussion as to whether that is the right model to use. One criticism is that if industry is writing the standards to which it has to conform, well, how strong will those standards be?

I think there is some rationale to that concern. On the other hand, most of the people writing these standards are, in fact, experts that understand what is and what is not possible. I was in a discussion earlier this week. Somebody was suggesting that perhaps we should bring people in from outside the electricity sector to write standards for the electricity sector. This kind of boggled my mind. Why would you do that? This is a very complex industry. If you have people writing standards who do not understand the industry, then you break things. In our industry, if you break things, the lights go off. These are things you want to avoid.

Your point is exactly right. Standards establish a base line of security. They can be as detailed as you want them to be. My goal with the guidelines is for them to sit on top of the standards and offer companies the flexibility to pick and choose what is appropriate for their individual situation.

AG CORTEZ MASTO:

Thank you. Are there any other questions or comments? I have one comment. I am curious about your thoughts on this, particularly considering your previous work environments of Colorado and California, in state government.

---

<sup>5</sup> American National Standards Institute

As you know, particularly where local and state governments and agencies are trying to be more transparent and accountable, we put a lot of information, whether budget related or agency related, on our web sites. We try to push information out to the public. I fully support that.

Should we have a concern, on balance, so we are also protecting the government from cyber security intrusions? Will others use that information against us?

Are you aware of any guidelines or protocols that have been established to take into consideration cyber security components along with government transparency? Or, do you think that this is not an issue?

MR. WEATHERFORD:

I certainly think it is an issue. It involves an on-going debate. Every state is having that debate. The citizens and interest groups want to know how government is spending money. They want to know not only that money is being spent, but what kind of projects are being worked on. I think there is a sense of urgency in governments to make that information available.

I think there are two pieces related to security. Sharing too much information can be a problem. I come from the intelligence community and we always worry about aggregating information. A piece here, and a piece there, may not mean anything individually. But, if you put them together, you have a nugget that is worth something.

While citizen information may not rise to that level of aggregation concern, there are other things embedded in projects, funding and people that may rise to that level of concern. That is one piece of the issue.

The other piece of it is physically protecting the information so that it can not be exploited. I don't mean protecting it so that it can't be stolen – obviously, if you are making it public, then it's public. But you should be concerned about the integrity of the information. One of my biggest concern is someone getting into a system and altering financial information at its root. That could have a big impact on government. You could either be spending money you don't have or think you have too much. The physical aspect of protecting information – protecting the contents of the information – is important. That is where technology can solve that problem for the most part. There are technologies available to do that.

AG CORTEZ MASTO:

Thank you. I appreciate that. Are there other comments or questions? Mr. Weatherford, thank you for your presentation. You are welcome to come back to Nevada anytime.

MR. WEATHERFORD:

I asked Chris today if there were any jobs around. I love it here. (laughter)

**Agenda Item 7 – Presentation by James R. Elste, Principal, INOV8V CyberCQRT (former Director, Security Strategy & Programs, West Region, Symantec), STUXNET: The Era of Weaponized Malware and Implications for Critical Infrastructure.**

AG CORTEZ MASTO:

Moving on to Agenda Item 7. This is a presentation by James Elste, principal of Innovative Cybercort. He is the former Director of Security Strategy & Programs, West Region Symantec. He is going to talk about Stuxnet and the era of weaponized malware and its implications for critical infrastructure. Mr. Elste, welcome back to our committee.

MR. ELSTE:

Thank you for having me this morning. One slight correction – it is “Innovative Cyber Security.”

AG CORTEZ MASTO:  
I am sorry.

MR. ELSTE:

The spelling of that is unique. It is referred to as "leetspeak" in hacker communities. Today, an entirely separate language is being developed for use by the underground. I will share with you, those of you who are parents, one little bit of information. If you kids use "P911" or "P9" when they are texting, that means they are telling their friends that their parents are around.

I am very pleased to have the opportunity to come and talk to you about Stuxnet. As the former director of security strategy and programs for the west region at Symantec, I had the opportunity to provide briefings to over 100 companies. They ranged from some of the largest companies in the world to organizations that are much smaller. It was very interesting to sit down with organizations and have a discussion about this piece of malware.

Stuxnet Hyperbole

- "A military-grade guided cyber missile"
- "A hyper-sophisticated cyber weapon"

More accurately:

- "Weaponized Malware that was developed with intent, specifically targeted, launched, and successfully damaged it's intended target"

INOVBV CyberCQRT.

Stuxnet has categorically changed what we believe malware is capable of.

I am going to attempt to separate the facts about Stuxnet from the hyperbole, separate speculation from facts. I will offer some opinions where opinions are appropriate.

You have heard of Stuxnet I am sure. It is one of the latest exploits to be described in the press. We have heard it described as a military grade cyber weapon, or a hyper sophisticated cyber weapon. More precisely, it is a weaponized piece of malware

that was developed with a specific intent. It was targeted towards a specific target. It was launched at that target. It successfully infected that target, and damaged the systems as intended.

Agenda

- Framing a discussion on Stuxnet
- The Stuxnet "Weapon"
- Assessment & Attribution
- Cyber-Defense



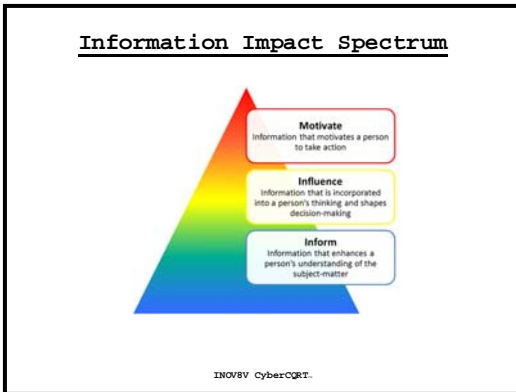
INOVBV CyberCQRT.

This is a watershed event in cyber security. This piece of malware, instead of doing something innocuous, actually caused physical damage in the real world.

First of all, we need to frame this discussion. It would be very easy to dive into the technical details and put everyone to sleep. I want to be able to discuss this with non-technical people. You need to understand Stuxnet as well as the technical guys because you are in a position to make decisions and to influence what we cyber security professionals do.

I would like to describe the Stuxnet weapon in terms we can all understand – intercontinental ballistic nuclear missiles. Every weapon since the advent of the flint-tipped spear has had three components. It has a delivery system. It has a targeting system. It has a payload. We are going to discuss Stuxnet in terms of those three major components. We are then going to discuss the impact of Stuxnet, some of the information circulating on attribution, and then discuss the implications for cyber defense.

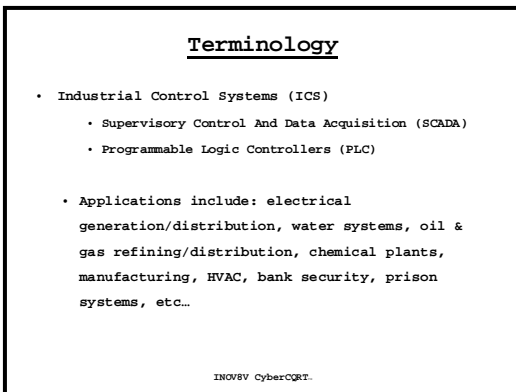
This is a bit pedantic, but the first thing I would like to do is to discuss the impact of information. When we share information, there are different degrees. We are inundated by information today that helps us become better informed. If we are lucky, some of that information is actually



relevant and shapes our opinions and decision making. In very rare cases, information motivates people to take action. I am hoping that some of the information I share will rise to the higher levels of this sharing spectrum.

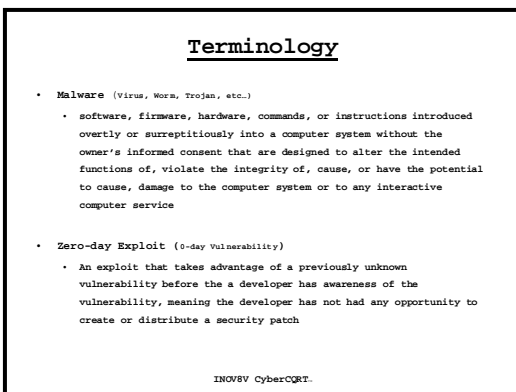
We do need to go over a little terminology so we are all working from the same perspective. The first thing is industrial control systems, SCADA<sup>6</sup>, and programmable logic controllers. We hear the term “SCADA” used quite frequently. Correctly applied, it is an industrial control system and SCADA is a subset of that industrial control system. Programmable logic controllers are an even smaller

component of this. They are the interface devices between the cyber world and the physical world. They control the systems that flip switches, turn valves, and report information about a process.



It is particularly important to understand that industrial control systems is that they are everywhere. They are fundamental to electrical generation and distribution systems. They are fundamental to our water treatment and distribution systems. They are part of the oil and gas industries and the processing of chemicals. They are part of manufacturing plants. They run HVAC in buildings. They run bank security systems and, most recently, at the Black Hat Conference this month, we learned of known SCADA vulnerabilities in prison systems. They impact the way the doors on prison cells are controlled.

It is this point of interface between the virtual world and our physical world that is of such concern. This is what we mean when we talk of industrial control or SCADA vulnerabilities.



The next term is “malware.” We hear terms such as viruses, worms, Trojans, and botnets. All of these fall under the umbrella term “malware.” The problem is this term is not well defined. It certainly does not exist in statute anywhere as I understand.

I have a definition here that I have worked on with Mr. Earl that proposes an encompassing definition of “malware.” It is software, firmware, hardware, commands, or instructions that are introduced overtly or surreptitiously into a computer system without the owner's informed consent, and that are designed to alter the intended functions of, violate

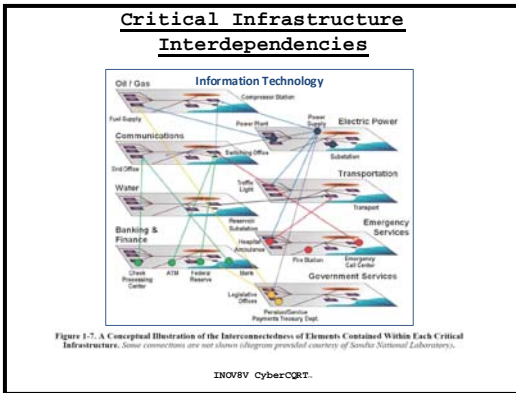
the integrity of, cause or have the potential to cause damage to that computer system or any interactive computer service.

It is important to define malware because individuals engaged in developing this type of attack material, well, it's hard to prosecute them when they are writing this stuff. Effectively, they claim a First Amendment-type right – “I am just writing something.” If you put a definition in statute that

<sup>6</sup> Supervisory Control And Data Acquisition.

describes malware and includes intent of the potential to cause damage, I think it extends the ability to quantify what malware is and pursue it with legal remedies.

You may have heard of “zero-day exploits” or a “zero-day vulnerability.” It is important to understand that a zero-day vulnerability exists in a system that has yet to be discovered or disclosed to the developers of the system. So, those developers have not had the opportunity to develop a patch or otherwise correct that vulnerability before the exploit is executed. Zero-day exploits are of grave concern. If the bad guy knows about the exploit and develops malware to make use of that vulnerability before the good guys know that the vulnerability exists, then the good guys are at an extreme disadvantage. That should get us through this discussion.



Next, it is necessary to understand the interdependencies of our critical infrastructures. One could write a dissertation on this, but I found a graphic that sums up the different critical infrastructures, and, more importantly, illustrates the interdependencies among these infrastructures. We tend to look at infrastructure in silos. We think about the power grid and the electric distribution system. We think about oil and gas. We think about finance. But we tend not to think about these systems collectively. These are interdependent systems.

As Mark pointed out, if you remove electricity, we no longer have a financial system to worry about. Currently, 60% of the electricity generated in the country is generated from coal. You don't see coal as a critical infrastructure system on this pictorial. What you do see are interrelationships that could lead to a domino effect among other critical industries.

When we look at industries collectively as interdependent, we begin to understand how to move towards defending against attacks more collectively and more effectively. Information technology affects all of these industries. Just as electric power is critical to all of these, so is information technology. These critical industries can not function without the information systems that support them. That is what makes cyber attacks against the information systems in critical infrastructure so worrisome.

Here are a couple of examples of failed industrial control systems.

The first occurred in Bellingham, Washington. A pipeline dumped a quarter of a million gallons of gasoline into a creek. The gasoline caught fire, killed three people, and injured eight others. A mile and a half section of the creek exploded and damaged public and property. The reason this occurred was that relief valves in the pipeline were set incorrectly. Inspections had been delayed, and the SCADA system was unable to report the discrepancies in those valve settings.

Another example involved the Pembroke refinery in the UK. In 1994, a lightning strike caused a half-second interruption in the electric power to the processing plant. This tripped a number of different pumps and coolers. They oscillated on and off. Flammable liquids were pumped into a processing vessel and that vessel was unable to open the outlet valve properly. This caused an explosion that destroyed the refinery. The impact of this failure cost the UK 10% of its refinery capacity for a four-and-a-half month period while recovery took place at the refinery. This also involved \$ 70 million dollars of lost business.

The last example involves the San Diego County Water Authority. Electromagnetic interference interacted with the wireless SCADA system. This prevented the Authority from controlling remote valves. They had to send technicians to remote locations to adjust the valves manually. They eventually wrote a letter to the FCC suggesting that they had narrowly averted a catastrophic

failure of the aqueduct system. That system pumps 825 million gallons of water a day. It could have spilled thousands of gallons through venting, damaged the aqueduct infrastructure causing a disruption of service, and/or caused severe flooding damage to public and private industry.

These examples illustrate three things. One, the inability of a SCADA system to report caused gasoline to be poured into a creek. Two, there is an example of the replacement of damaged systems. Third, there is an example of a potential catastrophic failure through a SCADA system, impacting a major water system.

Hypothetical Scenario

- "Las Vegas, NV"
  - Population (Clark County) > 2 Million
  - Annual Tourism > 40 Million (~ 750,000/week)
  - Economic Impact > \$35.2 Billion (8.8 billion Gaming)
  - Average Max Temperature (July) = 104.1F
- Southern Nevada Water Authority
  - 90% Colorado River, 10% Ground Water (5 Reservoirs)
  - 2 Main Water Treatment Facilities
  - 4 Major Water Distribution Systems
  - 7 Major Pumping Stations

INOVBV CyberCIRT.

Let's consider this hypothetical scenario. It will not be lost on anyone here that Las Vegas, meaning Clark County and the surrounding area, is a target for terrorists. The population is over 2 million people. Some 40 million visit as tourists every year. That is roughly 750,000 per week. Las Vegas obviously impacts the economy of the State significantly. Roughly \$38.5 million of revenue comes from gaming.

The average temperature in Las Vegas in July is 104 degrees. Anyone stepping outside Las Vegas in the middle of the day in July knows that the average may approach, I don't know, say 120

degrees. We have to have water to survive. The water provided to the Clark County area – 90% of it comes from the Colorado River. There are two water treatment facilities, four water distribution stations, and seven major pumping stations.

I am here to tell you today that a successful Stuxnet-class cyber attack against the Southern Nevada Water Authority's industrial control systems could disrupt the water supply to Las Vegas. If that were to happen in the middle of summer, when we have almost a million tourists in town, we would have a catastrophe of epic proportions on our hands.

This is the new reality we face in a time when malware like Stuxnet exists. Clearly, we hope this doesn't happen. We hope we are properly defending those systems. However, the explanation of Stuxnet today should be considered within the context of **all** industrial control systems and **all** of our critical infrastructure. None of these systems are removed from potential attack by Stuxnet-class malware.

Attack Comparison

<u>Kinetic Attack</u>	<u>Cyber-Attack</u>
• "Explosives"	• "Computers"
• Detonator	• Malware
• Physical Delivery	• Virtual Delivery
• Obvious	• Stealthy
• \$\$\$\$	• \$

INOVBV CyberCIRT.

I want to differentiate now between cyber attacks and kinetic attacks.

When we talk about kinetic or physical attacks, we are talking about someone getting explosives and blowing up a pipeline or blowing up a facility. Procuring explosives is not an easy thing to do. If you want to take the extreme example, we would be talking about a nuclear weapon. Getting plutonium does not involve running down to Home Depot and buying some off the shelf. If you manage to get the explosive material, you will have to build a detonator – something to trigger the explosion at the time of your own choosing. Detonators do not

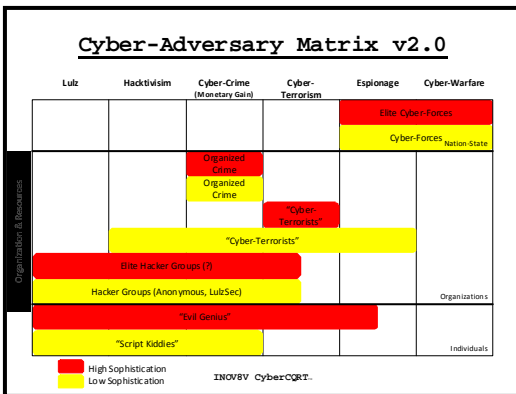
have to be particularly complex as we have seen in Iraq and Afghanistan where there are plenty of examples of IEDs [Improvised Explosive Device]. But you do need something. Then, you need to deliver the device to the location you are trying to attack. When you trigger the attack, it will be

obvious. It will explode. It will be noticeable. Ultimately, building an explosive device and delivering it to your target to effect a kinetic attack is an expensive proposition.

Let's compare that to a cyber attack. In a cyber attack, I need to assemble some computers. That oversimplifies the things I need to acquire – essentially a computer. I need to develop the malware I am going to use. Then I need to consider how to deliver that malware from virtually anywhere in the world – from the safety of another country or location. That location can be completely disassociated from the target I am attacking. The attack can be undertaken in an extremely stealthy manner. If you read the Shady RAT<sup>7</sup> report that was recently released, you learn that cyber attacks can take place over months and years. And, they can go undetected by the victims and targets of the attack for months and years.

Our systems are being infiltrated with such regularity, and we seem to have such a lack of ability to detect these stealth attacks that the attackers are able to explore our systems, identifying and exfiltrating information over months and years. In comparison to a kinetic attack, these cyber attacks are incredibly cheap. They are incredibly easy. This is what is so frightening about the potential for cyber attacks. There is a low barrier to entry. They are low cost. Resources, like computers, are relatively easy to acquire for individuals who want to launch an attack. Arguably, the only hard part is the construction of the malware code, but once constructed, it can be delivered with relative immunity as compared with a kinetic attack, which requires some type of physical presence.

Who are our adversaries? Mark made an astute comment to the effect that it doesn't pay today to draw the attention and ire of the bad guys. What we need to recognize is our cyber adversaries warrant a fair amount of our respect. They are very bright people. They are people with the ability to create cyber weapons. We are not dealing with dumb criminals here. We are dealing, in most cases, with very astute, very smart people. It is OK to respect your adversary while simultaneously wanting to defeat them.



This matrix is designed to illustrate who our adversaries are, what their motives are, and how they are organized and funded.

Across the top we have a spectrum. At one end is people doing things for laughs, essentially hacktivism. We then get into cyber crime, which is defined by a monetary objective, some financial gain through the activity. On the other end of the spectrum, we have cyber terrorism, espionage, and cyber warfare.

The other axis is arranged from the perspective of organizationally resourced perspective. In order to engage in cyber war, you need an extremely high level of organization and resources. On the other hand, the ability to go deface a web site entails much less organization, and certainly does not require the same sort of resources.

Finally, we want to differentiate between the sophistication of the adversaries. There are low sophistication attacks, and then there are attacks like Stuxnet that demonstrate extremely high sophistication.

<sup>7</sup> Operation Shady RAT is an ongoing series of cyber attacks starting in mid-2006 reported by Dmitri Alperovitch, of Internet security company McAfee in August 2011. The attacks hit at least 72 organizations, including defense contractors, businesses worldwide, the United Nations and the International Olympic Committee.

This tees us up to talk, first, about individuals. Script kiddies are defined as individuals who are taking pre-packaged, low sophistication attacks and recycling them. In contrast, there is the concept of the “evil genius.” That is someone with very good computer skills who is able to develop very sophisticated attacks independent of any organizational support.

When we consider motives, script kiddies are doing what they do essentially for laughs. They are motivated by hacktivism or notoriety or something similar. This potentially flows into cyber crime. Recently the FBI captured an individual who essentially destroyed the company’s information systems in an attack. This individual was a former employee who had an ax to grind because he had been laid off. He attacked the company using credentials he had from the time he was employed. It was done from a wireless access point in McDonalds in Georgia. The reason the individual was caught was five minutes before he attacked the company he spent \$5 at the McDonalds and charged it to a credit card. The FBI was able to tie the two together. So, script kiddies are not exactly our most sophisticated adversaries.

As groups increase in sophistication, we then come to the hacker groups like Anonymous and LulzSec. They use relatively unsophisticated attacks like denial of service attacks using well known methods like LOIC, which stands for Low Orbit Ion Cannon. This is readily available software used to carry out denial of service attacks. The concern is that they might increase in sophistication. There is chatter about malware this community has developed called RefRef that may be more sophisticated. These groups tend to be loosely organized, and they are not particularly well funded.

The next level up is cyber terrorists. Low sophistication cyber terrorists might have a broad set of motives, but they are not doing what they do for laughs – despite attacks that appear as hacktivism or cyber crime to fund their activities. They are looking for opportunities to effect a terrorist attack through cyber means. They may also be engaging in espionage for that purpose.

Here it is important to differentiate between levels of sophistication. The minute a cyber terrorist organization obtains a sophisticated piece of malware, or some attack capability, they are going to attack. This is because the shelf life of malware useful in a cyber attacks is rather short. On the other hand, what we see with Stuxnet, is that highly sophisticated users, utilized four previously unknown vulnerabilities. However, once Stuxnet was discovered, those vulnerabilities were patched. This makes the malware an obsolete mechanism for attacking a system.

While there is a lot of rhetoric around cyber terrorism, we haven’t seen a lot of evidence of cyber terrorist attacks, but, I do believe, that if these groups acquire the necessary capabilities, they will execute an attack in a rapid fashion.

The next organizational group is organized crime and cyber crime. These are folks we need to worry about. They are well organized and are well funded. They are motivated by financial gains. This motive is different from those of a cyber terrorist or a hacker group. When you compare hacktivism to organized cyber crime, it is easy to contrast the two. Cyber crime groups are very focused. They are looking for ways they can monetize the exploits they are engaged in.

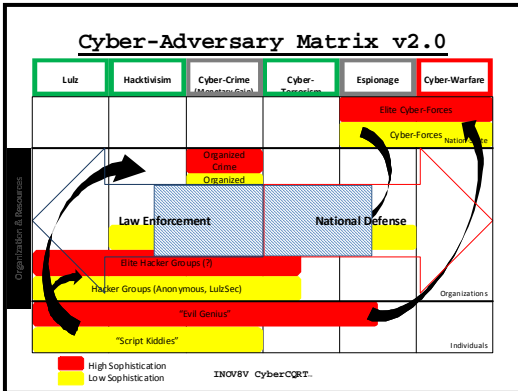
The highest level of organization involves nation states. It is fair to say that many countries are engaged in developing their cyber forces. There are two levels of sophistication here as well. There are normal cyber forces, and then, there are the elite cyber forces. This tells us that cyber warfare and the cyber attack space is going to be part of military doctrine going forward.

Albert Einstein had a wonderful quote. He said, “I don’t know what weapons world war three will be fought with, but world war four will be fought with sticks and stones.” He was referring to nuclear weapons, but I would argue that cyber weapons can have the same level of effect.

Where are these folks coming from and where are they moving towards? We see script kiddies and evil geniuses moving up to hacker groups. A script kiddy wants to use LOIC and participate



in an attack against PayPal or Bank of America, or whom ever is being attacked that day by Anonymous. They are also moving up the chain into organized crime. Individuals who have a certain level of skills are interested in monetizing their abilities. Albert Gonzalez, the individual who executed five of the largest identity theft intrusions in the last few years went from being an individual evil genius to working with a group to exploit these systems. When he was caught, he had a million dollars in cash in his back yard. He was monetizing his abilities very well by cashing in on stolen identities and credit card information.



There is also a movement from cyber forces in some countries. We see some of them sponsoring cyber terrorist organizations or organizations that engage in cyber activities that are not part of the activities of that nation state. We also see recruitment into the elite cyber forces of individuals who have skills, hopefully before they become too evil or go to far towards the dark side.

Cyber warfare is likely to be a very visible thing. The objectives will be to cause damage, to impact military operations, and so on. These things are pretty visible. Contrast this with cyber crime and espionage. They are the opposite. Their objectives

are invisible. They try to remain covert.

The remainder of these categories, cyber terrorism, hacktivism, and doing things for laughs produce very visible results. Hacktivists get information from a target, and then announce on the web site, "We just attacked the Arizona Department of Public Safety, and here is all their email traffic." High visibility means these attacks are a little easier to address.

The way we address attacks pretty much splits the spectrum. National defense is focused on cyber warfare, espionage, and cyber terrorism. Law enforcement focuses on cyber crime, hacktivism and Lulz. There is some meeting in the middle because all of this is effectively cyber crime and all of it has implications for national defense.

I spoke with two individuals from the Peoples Republic of China about the time of the Google attacks. I told them that, if in fact, the attacks were state sponsored, and China was behind them, then the problem is diplomatic and military. On the other hand, if the attacks were cyber crime attacks, then the US and China have a joint interest to work together to address these problems.

This spectrum analysis is helpful when we look at Stuxnet. Ultimately, one of the questions about Stuxnet that has not been definitively resolved is who is behind it.

**Stuxnet: Key Observations**

- Stuxnet is a computer worm designed to infect Siemens WinCC and SIMATIC S7 PLC products
- Stuxnet takes advantage of multiple vulnerabilities in the Windows operating systems and Siemens products
- Once Stuxnet detects a targeted system, it modifies control logic in specific models of Siemens PLCs
- The objective of Stuxnet was to sabotage a specific industrial process: Iranian Uranium Enrichment

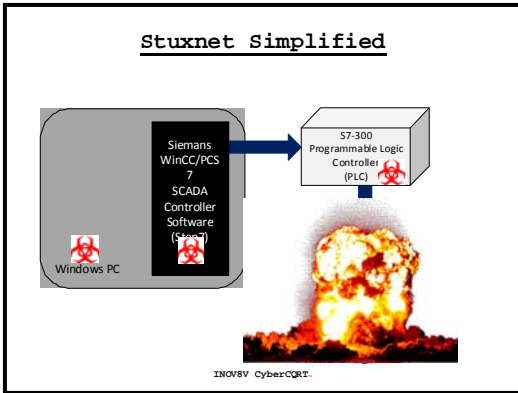
INOVBV CyberCQRT.

I am going to be quite explicit about certain aspects of Stuxnet that others have only danced around in the press.

Stuxnet is a computer worm that was designed to infect Siemens, WinCC, and SIMATIC S7 PLC products. There is no doubt about that. If you look at the technology of Stuxnet and the way it was constructed, it was directed to infect these systems. Stuxnet takes advantage of numerous vulnerabilities in the Windows operating system and in Siemens products.

Once Stuxnet detects a targeted system, it then modifies the programmable logic controllers. This is one of the most notable aspects of Stuxnet. This is the first time we have seen a PLC root kit that could actually affect the component of a SCADA system that controls the physical devices.

The objective of Stuxnet was to sabotage a specific industrial process. That process was the Iranian uranium enrichment facilities in Natanz. I will support that conclusion in a moment.



Here is the simplified version. We have a Windows PC. That Windows PC runs the Siemens data logic software. It communicates with a programmable logic controller device. That programmable logic controller device is attached to an Iranian IR1 nuclear enrichment centrifuge. What is involved is a process for creating enriched uranium.

Stuxnet infects the Windows system. It infects the Siemens software. It infects the programmable logic controller, and then initiates a sabotage routine that destroys the centrifuge. It doesn't cause the explosion on the slide, but, suffice it to

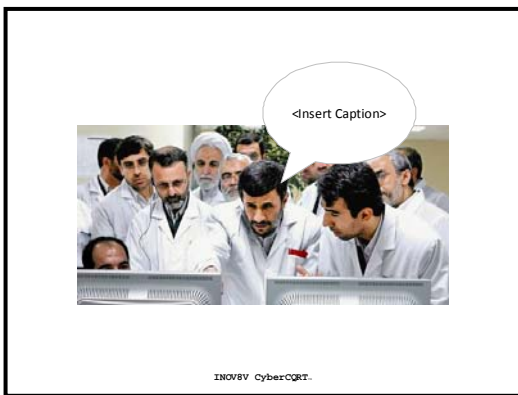
say, it is effective in destroying the physical device. That is the scheme, in a nutshell. Everything I talk about is filling in the details, so, hang in with me.

This is a Siemens SIMATIC S7-300 PLC. For reference, it is about the size of a small radio or stereo. It doesn't have a lot of interface devices. It is remotely controlled through the Windows computer.



This is a picture of the Iranian uranium enrichment facility in Natanz. This is President Mahmoud Ahamadinejad. The cylinders beside him are the IR-1 centrifuges. Essentially, in uranium enrichment, uranium hexafluoride is spun at very rapid speeds in order to separate highly enriched uranium, which is then used for nuclear weapons.

This is a publicity shot that is not related to Stuxnet, but I could not help include it. When you see 15 or more Iranians looking at a computer screen with Ahamadinejad pointing it, it invites you to insert your own caption. It is not hard to imagine them looking at the effects of Stuxnet wondering why these centrifuges are being destroyed in their own environment.



These are the vulnerabilities. Without addressing the gross details of those vulnerabilities, I can tell you that to come up with four previously unknown zero day vulnerabilities is an extremely significant accomplishment. It is almost unheard of.

It is a rare thing for an individual to come up with one previously unknown zero day vulnerability. To come up with four of them, to be able to construct

them into a cyber weapon that uses them in a distribution process to affect these systems, is phenomenally sophisticated.

When I talked to Eric Chien at Symantec, one of the primary Stuxnet researchers, a guy who spends every day examining malware, I saw his eyes light up. He talked about how incredibly sophisticated this was. This is not a normal piece of malware. This is a singular event.

Stuxnet took advantage of one previously known vulnerability. This should reinforce the message that patching is important. That vulnerability was patched in 2008. It had been used for the Conficker attack. Conficker was the computer worm with the largest impact we had seen since 2003. It affected about 7 million systems – government, business, and home computers in 200 different countries. State of Nevada systems were infected by Conficker.

**Vulnerabilities Exploited by Stuxnet**

- **Four (4) 0-day vulnerabilities**
  - CVE-2010-2568 (MS10-046) LNK Exploit (USB Propagation)
  - CVE-2010-2729 (MS10-061) Spool Server Exploit (Print Spooler Propagation)
  - CVE-2010-2743 (MS10-073) Win32K.sys Exploit (Privilege Escalation)
  - CVE-2010-3338 (MS10-092) Task Scheduler Exploit (Privilege Escalation)
- **One (1) Previously known MS vulnerability**
  - CVE-2008-4250 (MS08-067) RPC Exploit "Conficker" (RPC Propagation)
- **Two (2) Siemens WinCC/Step 7 Vulnerabilities**
  - CVE-2010-2772 Hard-coded password in WinCC Database
  - MS Security Advisory #2269637: Insecure Library Loading Remote Code Execution (Step 7 Project files DLL auto-execute vulnerability)

INOVSV CyberCIRT.

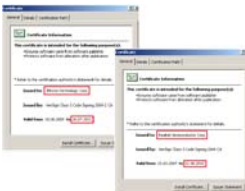
To provide a comparison, Stuxnet only affected about 100,000 systems in total. However, combining Conficker, based on a previously known vulnerability, and still get mileage out of it, comes as a surprise.

Additionally, Stuxnet exploited two vulnerabilities in the Siemens system. Anyone who has worked in cyber security for any length of time, the notion of hard coded passwords is anathema. You just want to hit your head. Frankly, passwords of this sort enabled Stuxnet to propagate through one mechanism because the password was available

on the Internet. If you search for the Siemens WinCC/Step 7 passwords, you will find the two passwords on the Internet.

**Stolen Digital Certificates**

- Stuxnet device drivers were digitally signed with the private keys of two certificates that were stolen from two separate companies (Jmicron and Realtek)
- Both companies are located within about 1 mile of each other in Taiwan at the Hsinchu Science Park



INOVSV CyberCIRT.

Stuxnet did something else that indicates high sophistication. It used stolen digital certificates. You may recall a discussion at a previous Board meeting about digital certificates. Stuxnet was able to sign the device drivers it used with two stolen digital certificates. They were taken from two separate companies. What is interesting about this is the two companies are located about a mile apart from each other in a business park in Taiwan. The speculation is that a physical attack against these companies led to the acquisition of the necessary digital certificates.

We are currently seeing news reports about attacks against digital authorities, the DigiNotar and Commodo attacks, for example. There is a news article today that could be even more significant. Digital certificate authorities are one of the fundamental underpinnings of trust on the Internet. They are how we determine that software or transactions are trustworthy. The DigiNotar attack seems to be coming from an individual attacker who has some association with Iran. It had a significant impact on Dutch e-government because the DigiNotar certificates were used by the Dutch e-government services. When the certificate was compromised, those services were no longer available. The consequences of stolen digital certificates are significant.

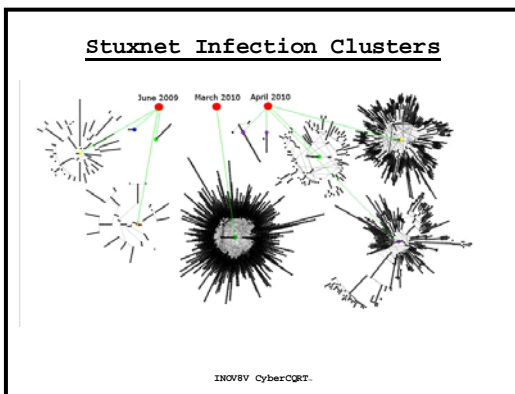
The fact that Stuxnet used stolen digital certificates to fake the authenticity of these DLLs is equally significant.

Here is the Stuxnet timeline. The earliest version of Stuxnet, based on analysis, was 2009. In January, it used the stolen digital certificate to sign the payload. March and April is when we saw the widest proliferation. Stuxnet was discovered in June of 2010 by a company called VirusBlokAda. Shortly after that, the certificate authority realized its certificates had been

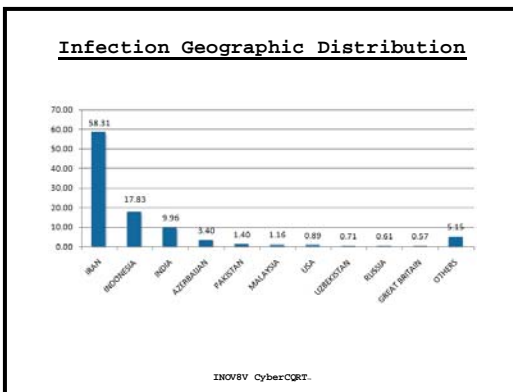
compromised and started to revoke them. They revoked the RealTek certificate in July. Then they discovered the JMicron certificate was being used. Siemens then reported vulnerabilities in their systems. In September, Symantec released a fairly detailed report on what had happened with Stuxnet.

Let's move on to the delivery system. Stuxnet spread primarily through USB flash drives and removable media. This is important because most SCADA systems are "air gapped" from other systems. This means they are physically separated from the Internet. However, SCADA systems are serviced by contractors who come in with USB sticks that are plugged into the SCADA system to do maintenance.

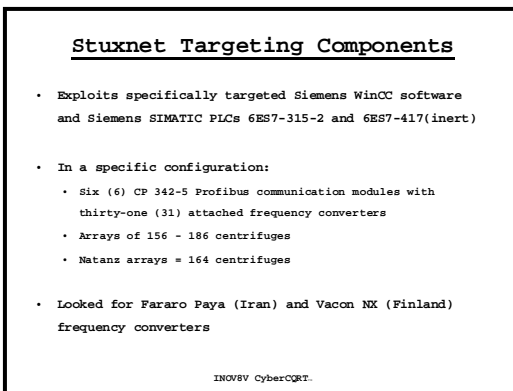
Stuxnet also could propagate through the local network and printer services. As I mentioned, making use of the hard coded password, Stuxnet was able to propagate using SQL stored procedures. It also had the ability to infect project files for the Step 7 systems so that operators of this system ended up sending email that would also propagate Stuxnet code.



This picture is worth 1,000 words. Based on an analysis of the command and control traffic, it illustrates the different infection clusters of Stuxnet and the timing of the releases triggering the clusters. Stuxnet affected many systems. The largest cluster infection was in March. By September, about 100,000 systems were infected. If you analyze the infection pattern in detail, we find that Stuxnet was targeted at five different organizations. Each of those organizations had a presence in Iran. Stuxnet propagation patterns were not accidental. It was not simply released into an Internet environment, with the hope that it would end up in Iran. Stuxnet specifically targeted Iran and was specifically distributed into organizations that have a presence in Iran.



All other infected systems represent collateral damage. They were not intended targets. As you look at the geographic distribution, 58% of 40,000 odd infections were in Iran. This represents an anomaly when compared to normal malware distribution patterns. Normally, the United States and other first world countries with lots of computer infrastructure would be impacted the most.



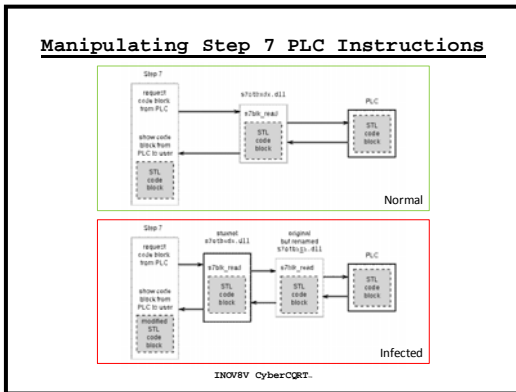
Of the infected systems, 67% had Siemens software running on them. That leads us to the targeting mechanisms. It was specifically targeted in a unique way. It looked for two specific types of PCLs, the 315 and the 417. The 315 was active, the 417 was inert.

It looked for a specific configuration in the SCADA environment. It looked for 6 communications modules with 31 attached frequency converters. That means an array of 156 to 186 centrifuges. The centrifuge arrays in Natanz had 164 centrifuges. A bit of quick math, had there been only 5 controllers,

the spectrum would not have been wide enough to accommodate the Natanz arrays. The specific numbers were 6 and 31. This provides the right range. Someone knew there were arrays of 164 centrifuges in Iran.

Additionally, Stuxnet looked specifically for Fararo Paya and Vacon NX frequency converters, the devices that adjust the speed of the centrifuges. Iran is embargoed. It can not simply buy uranium enrichment equipment off the shelf. The ability to look for specific frequency converters supports the conclusion that Stuxnet targeted one site and one site only, world-wide, the Natanz enrichment facility.

Turning to the payload, the ability to inject malware into a specific system is pretty impressive by itself. Once on a specific system, what Stuxnet did was equally impressive.



This shows the normal operating sequence for communicating with a PLC. There is the controller system on the Windows box. There is a piece of code that communicates with the PLC, and everything that an operator of the system sees or understands about the current operation of the system, comes through that interface in the Windows box. That is in normal operation.

When Stuxnet code was injected, it intercepted every single communication from the PLC. If the operator tried to adjust the controller, Stuxnet was able to see what code was adjusted and prevent

the operators from seeing the Stuxnet code. If an operator said, in effect, "Show me what the system is doing," what Stuxnet reported was the parameters that the operator was expecting to see. Stuxnet hid any sort of alarm conditions or any other signal that would indicate there was a problem monitored by the Windows box. Stuxnet did an extremely good job of this. There was no way for an infected system to effectively report that it had been infected or that the operations of the environment were being altered by Stuxnet.

Stuxnet created what is called a "man in the middle" condition, where every communication was intercepted and altered so that an alarm, or Stuxnet itself, could not be identified or removed. The effect on the PLC was interesting. It monitored the environment. In doing so, when it saw certain conditions existed, it then initiated its sabotage routines. It also prevented the system from reporting any alarm conditions, or, doing what it was supposed to do – initiating a graceful shutdown in response to a catastrophic event.

- ### PLC Rootkit
- Stuxnet creates a "man-in-the-middle" condition and intercepts requests and modifies requests so that infected PLC code is not discovered or damaged
  - Infects Organization Blocks (OB1, OB35) affecting communication with PLC connected devices
  - Monitor PLC communications
  - Initiate sabotage routines
  - Prevents OB35 code from initiating a graceful shutdown during catastrophic events
- INOVS CyberCIRT.

- ### Sabotage Routines
- Monitor events for 13 days
  - Ensure system has been operating between 807 Hz and 1210 Hz (normal operating conditions)
  - Set frequency to 1410Hz for 15 minutes
  - Return to normal operation
  - Wait 27 days
  - Set frequency to 2 Hz then 1064 Hz (nominal frequency)
  - Wait 27 days, repeat
- INOVS CyberCIRT.

The sabotage routines were novel. The system monitored the environment for 13 days. Stuxnet ensured the system was operating at a frequency between 807 Hz and 1210 Hz. This is very high speed, but normal, operation of the centrifuges. It then set the frequency to 1410 Hz for 15 minutes. This raised the frequency to a level where an harmonic imbalance in the system was created. This caused damage to the centrifuge. If that did

not inflict terminal damage, it returned to normal mode. It waited for 27 days. It then reduced the frequency down to 2 Hz, another harmonic value, then returned the frequency to normal operation. It waited 27 days and repeated again.

If the centrifuge survived the first pass, by raising the frequency, and the second pass, by lowering the frequency, then, 27 days later, the attack routine was run again. This was specifically designed to destroy those centrifuges. There were no unintended consequences involved. These procedures were baked into the code. These effects were specifically designed.

```

Command & Control

• Establishes communication with C&C servers if Internet
connectivity is available
  • www.windowsupdate.com
  • www.msn.com

• C&C Servers located in Malaysia and Denmark
  • www.mypremierfutbol.com
  • www.todaysfutbol.com

• Sends information regarding infected system
  (OS version, IP address, Computer name, Domain name, WinCC and Step 7 Versions)

• Also has the ability to update infected systems via P2P
network
                                INOVSV CyberCQR.T.
```

The command and control of Stuxnet was pretty much “hands off.” There was no operator on the other end providing instruction on how to attack these systems. Stuxnet was pretty much “fire and forget.” However, it did report its presence and information to two domains that would not normally be blocked by normal people – MyPremierFootball and MyFootball.com. This is the round football, not the oblong handball we use in the United States.

Stuxnet has the ability to send information about the systems that were infected, and it can be updated through peer-to-peer connectivity. This gives Stuxnet the ability to be updated.

Jim is giving me the high sign to move faster, so I am going to move quickly to the impact assessment.

President Ahmadinejad admitted that a software attack affected Iran’s centrifuges: “They succeeded in creating problems for a limited number of our centrifuges with software they had installed in electronic parts.”

The head of civil defense said their programs “suffered potentially major damage.”

I don’t know how reliable comments out of Iran are, but the Washington Institute for Science and International Security suggested that Stuxnet destroyed about 1,000 centrifuges, 6 cascades of 164 centrifuges, roughly 11% of the Iranian capacity. The estimates vary. I have heard numbers as high as 30% of capacity destroyed. I have heard estimates suggesting the nuclear program was set back by 3 years.

```

Attribution

• No non-classified attribution has been made at this time

• MYRTUS reference in Stuxnet Code
  • “Esther was originally named Hadassah. Hadassah means ‘myrtle’ in Hebrew.” Esther learned of a plot to assassinate the king and “told the king of Heman’s plan to massacre all Jews in the Persian Empire...The Jews went on to kill their would-be executioners.”

• 19790509 - This is thought to be a “do not infect” marker.
  • May 09, 1979 - Prominent Iranian Jewish businessman Habib Elghanian was executed by a firing squad in Tehran. Prompted the mass exodus of the once 100,000 member strong Jewish community of Iran.

                                INOVSV CyberCQR.T.
```

The ISIS report also suggested that Stuxnet was a reasonable explanation for delays in the program, but there are still questions that remain about drawing this conclusion.

We have no non-classified attribution at this time. Jim Lewis of the Center for Strategic and International Studies recently said in a C-SPAN interview that the US government has very sophisticated attribution techniques that are classified.

There are interesting factors that indicate attribution, and I will try to cover these quickly.

The first is this interesting reference to MYRTUS that was embedded in the Stuxnet code. This is a biblical reference to an attempt by the Persian Empire to massacre all the Jews. The Jews were forewarned and attacked their would-be executioners.

There is also a compelling reference that involves "19790509". This is a marker thought to signify "do not infect." Coincidence? Yes, but a strong and compelling coincidence that May 9, 1975 is the date a prominent Iranian Jewish businessman was executed by firing squad in Tehran. This prompted an exodus of the Jewish community in Iran. The US Senate condemned the execution. This marker, within the code, would have prevented Stuxnet from infecting the relevant system.

**Attribution**

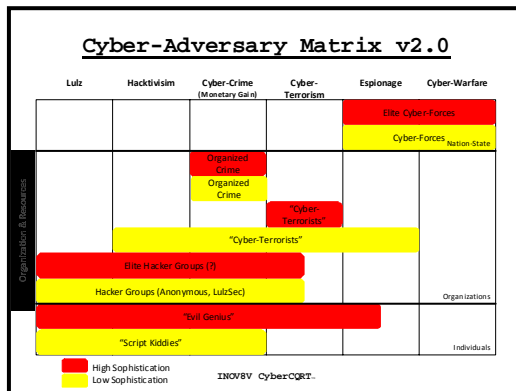
- **Meïr Dagan** (former head of the Mossad, retired 2010)
  - His legacy was the battle against Iran's nuclear weapons program
  - Invited reporters to a secret facility (suspected Stuxnet test site)
  - In favor of anything that could set back the Iranian nuclear program without starting a conventional war
  
- Current speculation is that Stuxnet was a joint effort of Mossad and the US
  - Research done at the INL in 2008 regarding ICS vulnerabilities, specifically Siemens WinCC and Step 7
  - "My opinion is that the Mossad is involved," Ralph Langner
  
- True or not, Stuxnet is driving other countries to develop similar capabilities

INOV8V CyberCQRT.

The next indicator involves Meïr Dagan, the former head of Mossad who retired last year. His greatest legacy was his fight against the Iranian nuclear weapons program. He invited a number of reporters to a secret facility, now not so secret, a known secret facility, in Israel. It is suspected that Stuxnet was tested there against a duplicate environment. He did not say explicitly that Israel had launched Stuxnet, but he was very proud of anything that would set back anything that would set back the Iranian nuclear program without using military force. He did not put a lot of stock in the ability of military force to be effective.

The current speculation is that Stuxnet was a joint effort between Mossad and the US. Specifically, Stuxnet would leverage some of the research done at the Idaho National Labs back in 2008 regarding ICS vulnerabilities, specifically the Siemens systems. Ralph Langner, who does a significant amount of SCADA security research in Germany, said, "It is my opinion that Mossad is involved."

Either way, we have to realize that Stuxnet is driving countries to develop similar capabilities.



These are the people who could do it. It will not be the unsophisticated. It will not be organized crime since there is no economic motive. It is not going to be the hacker groups, there is no motive. It's not going to be cyber terrorists as we know them because they will not be motivated to attack the Iranian program. It might be an evil genius, but to develop four previously unknown zero day vulnerabilities, to have the necessary depth of understanding of the nuclear enrichment process in Iran, and to be able to construct Stuxnet in the way it attacked its specific target, that's just not possible.

This leaves but one conclusion. The elite cyber forces of some nation state were behind Stuxnet. This conclusion is supported by The Guardian, BBC and New York Times. They said, based on the complexity of the code, it could only be a nation state.

I would like to say categorically, I hope it is us. I hope that if there is a nation state out there that has this sophisticated a cyber force and this sophisticated a capability that it is the United States of America. It would not be a good thing if we are not leading in this arena.

AG CORTEZ MASTO:

Mr. Elste, I am going to ask you to wrap it up, we are close to lunch time and we do have one more speaker.

MR. ELSTE :

Stuxnet has a kill date of June 24, 2012. There could be another shoe left to drop. I will be glad to offer an explanation of the remainder of my slides. They go into a broader examination of the attacks and possible defenses.

In case anyone doubted the notion of a cyber attack against critical infrastructure, this is an attack against a 27-ton, one megawatt generator. [video plays]<sup>8</sup> This was a staged attack by DHS. They constructed a similar control environment and completely destroyed this generator with a cyber attack.

We now know it can be done in a staged attack. We know it can be done in real life with a specific target. We need to up our game in terms of cyber defense.

MR. EARL:

If I could add one additional observation. In the demonstration, all systems were being reported as nominal during the attack. So, much like Stuxnet, the demonstration attack that took place in the US involved no report from the generator under attack that anything was outside its normal operating parameters.

MR. ELSTE:

That is correct.

AG CORTEZ MASTO:

Thank you very much for a very informative presentation. Are there any comments or questions from Board members? Thank you again. We have one final presentation, and then we are going to wrap this up. This should be a quick presentation on SB 82, a bill passed during our last legislative session.

**Agenda Item 8 – Presentation by David Gustafson, State Chief Information Officer and Christopher Ipsen, State Chief Information Security Officer, Implications for Government Information Systems of the Passage of SB 82 (2011 Legislative Session).**

AG CORTEZ MASTO:

We have David Gustafson, our State Chief Information Officer and Chris Ipsen, our State Chief Information Security Officer.

MR. IPSEN:

Thank you Madam Chair. Members of the Board, I would like to introduce David Gustafson. He is the CIO of the State. He has not been in these meetings, but it is a pleasure to have him and all the previous presenters. It's a privilege to have Mark and Jim in the State.

Last legislative session, at the prompting of the Tech Crime Advisory Board, and through the Attorney General's Office, SB 82 was presented successfully. It involved some important changes. I am going to turn it over to David and finish up at the end.

MR. GUSTAFSON:

Before I begin, I would like to make comment here. Chris doesn't know I'm going to say this. I would like to echo Mark Weatherford's comments. Over the past several years I have been with

---

<sup>8</sup> See <http://www.youtube.com/watch?v=fJyWngDco3g>



the State, Chris has not only been a trusted advisor of mine, but has become a personal friend. The State is fortunate to have an individual like this working for us. So, Chris, thank you for your service to the State.

I would like to lay out some of the key facts about the Department of Information Technology. There are two reasons for this. First, doing so is a shameless marketing plug. Second, I want to provide a perspective on what Chris and his team are responsible for securing within the State IT system.

The Department has roughly 130 employees. Chris and his team make up 7 of those. We have a \$39 million annual operating budget. We provide the wide area network known as Silver Net. This State network transports 22 Terabytes of data each day. Silver Net reaches all corners of the State. We have the only mainframe computer in State service. We have an email system that is comprised of 11,000 email accounts. We provide over 21,000 programming hours annually. That includes the education and training of State staff by the Office of Information Security. We support 160 Executive Branch web sites, approximately 8,000 telephone lines, and a microwave system that has over 600 circuits carried over 1.5 million miles of circuit paths and supporting 114 digital microwave sites.

If you thought Chris's job was difficult before, consider all this as providing an additional perspective regarding what is expected of the small group of security professionals we have and the small budget they are allocated. We really ask them to do a lot. Chris and his team have done a phenomenal job and I want to thank them for that effort.

I am excited to be able to talk to you about technology. As Chris and I have stated many times on the record, security is our number one priority. There can be no compromise. When we require our citizens to provide their information to the State, we have an obligation to protect that data.

We do not have the luxury, as a lot of private enterprises do, of buying insurance. So, for example, it's OK if the UPS guy loses our back-up tapes, we'll just write off any liabilities or cover the loss with insurance. The State doesn't have that luxury. The State obligates citizens to provide information, and we have an obligation to protect it.

More specifically, as this relates to SB 82, I would to identify several things. The new law changes the Information Technology Advisory Board (ITAB) – something we are trying to reconstitute. It promotes collaboration among the State, cities, and counties. It provides the authority to investigate and mitigate security related incidents and allows for security scanning and other proactive activities to secure systems and infrastructure.

I will talk about the first two items, and Chris will talk about the last.

The ITAB is important because it provides another forum to educate and inform users in cyber security matters. The new Board, comprised of 11 members, appointed for 4 years, are to advise the Department on issues related to information technology, including but not limited to, and I will paraphrase this, standards, policies, budget review and technology plans for the Executive Branch.

I will go through the 11 members now: One member appointed by the Majority Floor Leader, one member appointed by the Speaker of the Assembly, two representatives of using agencies from among the top 5 users of DoIT services, the Director of the Department of Administration, the Attorney General or designee (We removed the Superintendent of the Education System and replaced that slot with the Attorney General.); and five persons appointed by the Governor as follows (and this is where we made the most significant changes): three persons appointed who represent a city or county in the State, at least one of whom is engaged in information technology or information security (I have made recommendations to the Governor's Office for three CIOs, two counties and one city), two persons who represent information technology but are not

employed by the State. This portion goes on about how they can not benefit under State contracts. I recommended one person to the Governor's Office. This was a bit difficult because we do business with a lot of people.

The Board is important for many reasons. It will allow us to propagate the security message. It helps us inform others. The Board can make recommendations to the Department on how we are going to advance our security posture. Thank you, Madam Chair, for that.

Additionally, NRS 242, the DoIT governing legislation had language that was eliminated by SB 82. The removed language limited the State's ability to collaborate. We could collaborate with counties and cities only when "sufficient resources were available." This condition could not exist under OBM 87 reporting rules.

The new language added, thanks to Mr. Earl's help, "The Department may provide services, including, without limitation, purchasing services to a local governmental agency upon request if such a service will result in reduced costs to the State for equipment and services." That condition exists much more often than the previous limitation. Two examples of that are volume purchasing, bulk buying if you will, and enterprise agreements. We can now collaborate with cities and counties now. (Jim, I know there was also additional language that was removed at the last minute.) This will allow us to begin to remove the barriers that inhibited collaboration among State, city and county governments. I think that is what the citizens of the State would want us to do.

In consideration of time, let me turn this over to Mr. Ipsen.

MR. IPSEN:

I have several reflections on the bill and what its impact will be. It is significant in the area of collaboration. It removes barriers to collaboration. That will save money for the State, counties, and cities. That will allow resources to be used for other purposes or for security, if necessary.

As for specific implications for cyber security, it has had a significant impact already on our office. Security is not a responsibility we take lightly. The bill gives my office the ability to perform security testing proactively. This includes penetration testing and assessments on State systems.

Most people would assume we could already do this. Shouldn't the Office of Information Security have the ability to go out and test the computer systems of the State of Nevada? The problem was, the way the statute was written, if we broke into systems during the normal course of a test, we could be charged with a crime.

In some instances, where local State administrators have authority over local State systems, those administrators demonstrated reluctance when we wanted to demonstrate what hackers could freely find – we couldn't even look for those vulnerabilities. So, this is a very significant change brought about by this new legislation. We now have a process whereby we can look at State systems, evaluate those State systems, and make recommendations to fix the State systems they control. This is a profound positive impact on my office.

Second, the new law requires agencies to report suspected security incidents within 24 hours. This is 24 hours faster than the proposed federal requirements, which has some people up in arms. This language removes the subjectivity of a breach from agency judgment calls. It says, if you have a *suspected* incident, then we need to address it. It takes away the arbitrary and capricious nature of local reporting, where it is easier not to address problems. It is much easier not to address problems. It is less embarrassing not to address problems. But, as David said, we have a responsibility. In terms of the responsibility to report, mitigate and control, I think the legislation is important.

If I had to say one thing about SB 82 from our perspective, it is not a responsibility we take lightly. There is a process being created around this so we do not see the data that is sensitive, so we do not make changes in systems without assessing the business impact, but, where we do find security vulnerabilities, we do point them out and create a mitigation plan. In all these cases, the legislation was very successful. It was unanimously approved by the Legislature, proposed by the Attorney General, and signed by the Governor.

The State is sending a clear message on cyber security. I will leave it there.

AG CORTEZ MASTO:

David, Chris, thank you very much. Thank you for the work you do on behalf of the State of Nevada. Are there any comments or questions for either David or Chris? Thank you.

Let's move on to agenda item 9.

### **Agenda Item 9 – Public Comments**

AG CORTEZ MASTO:

This is an opportunity for the public to address Board members. Are there comments in northern Nevada? Any member of the public who would like to come forward? Seeing none, is there anyone in southern Nevada who would like to come forward?

SENATOR WIENER:

Madam Chair, if I could take just a moment. Today is a day of praise, and I would like to thank Chris, Jim Earl, Keith Munro, and Brett Kandt. They were all significant team players. I also want to thank you in your capacity as Attorney General for working so diligently on a measure I sponsored that provided for secured data protection. This was an extension of work we had done in the 2009 session. It was an ideal, team model that ensured that information collected by data collectors in the State is protected in incidents where people don't even know they are at risk.

I want to thank you for working on the measures I have had the privilege of sponsoring to ensure the citizens of Nevada are protected. I thank all of you. Madam Chair, in particular, I know that you dedicated several days where you relinquished other commitments on your schedule to ensure that bill was appropriately processed through the legislature. I want to thank you publicly for that.

AG CORTEZ MASTO:

Senator, thank you. Of course, all this would not be possible without your continued support on these issues. Thank you for being so willing to introduce needed legislation and fighting to get the bills passed. We really appreciate it.

One other important thing to highlight about Senator Wiener's legislation is the flexibility we talked about in our standards. We were able to ensure that flexibility moves forward with the help of Mr. Ipsen and the new role he is going to be taking. That was instrumental, and we would not have been able to do that without the Senator's assistance. So thank you very much.

Are there any comments from the public in the south? I did not see or hear of others. Hearing none, let's close that section and move on.

### **Agenda Item 10 – Scheduling future meetings**

AG CORTEZ MASTO:

Mr. Earl?

MR. EARL:

For the first time I am able to announce a specific meeting date. I spent considerable time with a lot of administrative assistants. We are scheduled to meet next on December 16. That is a Friday, and so, unfortunately, there is at least one Board member who will probably designate a representative. Part of the reason for the advance scheduling is we are set up to hear from Mr. Alan Paller. Mr. Paller is the founder and director of the SANS Institute, an exceptionally high-end educational institute for computer security and information security. Moreover, he has undertaken a special project over the past 3 or 4 years to institute training programs at the university and high school level, and, based on some conversations Chris and I had with him several weeks ago, potentially at the middle school level.

One of the things he will talk about, in addition to some overall background is the possibility of beginning some specialized training and education programs in Nevada at the high school and university level. He is available on December 16 and that is one of the reasons I wanted to set the schedule well in advance.

AG CORTEZ MASTO:

Thank you. Unless there are any questions from the Board members, we will adjourn the meeting.

But before we do so, let me say one more time, thank you to the presenters today. Everybody did an incredible job. It was so informative and very helpful for the Board members. We appreciate your taking the time to be with us today.

**Agenda Item 11 – Adjournment**

AG CORTEZ MASTO:

I now declare this meeting adjourned. Thank you to everyone who attended. [Time: 12:20 PM]

Respectfully submitted,

James D. Earl  
Executive Director

Approved by the Board at its subsequent meeting on December 16, 2011]