

DRAFT

**(DRAFT) Minutes of the
Technological Crime Advisory Board**

December 16, 2011

The Technological Crime Advisory Board was called to order at 10:11 AM on Friday, December 16, 2011. Attorney General Catherine Cortez Masto, Chair, 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
Professor Hal Berghel, University of Nevada, Las Vegas
Nevada State Assemblywoman Bustamante Adams
Special Agent David Schrom (*meeting designee for Special Agent in Charge Kevin Favreau, Federal Bureau of Investigation (FBI)*)
Assistant Chief Kuzanek (*meeting designee for Sheriff Mike Haley, Washoe County Sheriff's Office*)
Christopher Ipsen (*Representative for David Gustafson, State Chief Information Officer, Enterprise IT Services*)
Special Agent in Charge Richard Shields, U.S. Secret Service (USSS)
William Uffelman, President & Chief Executive Officer, Nevada Bankers Association

ADVISORY BOARD MEMBERS ABSENT:

Daniel Bogdan, U.S. Attorney, Department of Justice (DOJ)
Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department (LVMPD)

STAFF MEMBERS PRESENT:

James D. Earl, Executive Director
A.J. Delap, LVMPD

OTHERS PRESENT:

Timothy Cary, Nevada DEM
Jack Homeyer, PSC Consulting
James R. Elste, INOV8V CyberCQRT
Suzanne Brunette, Nevada DEM/HS
Jeff Rauh, LCB Audit
Edie Cartwright, Nevada AGO
David Gustafson, Nevada EITS
Kimberly Munoz, Nevada DOT
Laura Fucci, CIO, Clark County

DRAFT

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

AG CORTEZ MASTO:

Good Morning. Let's call to order Nevada's Technological Crime Advisory Board this December 16, 2011. The first item on the agenda is the call to order and the verification of the quorum. Mr. Earl.

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

AG CORTEZ MASTO:

I would like to point out that we have new members on the Tech Crime Advisory Board. The first one is Assemblywoman Irene Bustamante Adams. Assemblywoman Adams, we would like to welcome you to the Board. We look forward to working with you in the future. You and I have had an opportunity to talk. We are excited to bring you into the realm of tech crime here in the State and help us address some of the issues we deal with. Welcome to the Board.

ASSEMBLYWOMAN BUSTAMANTE ADAMS:

Thank you.

AG CORTEZ MASTO:

The other new member joining us is Professor Hal Berghel from University of Nevada, Las Vegas (UNLV). He is an education appointee. He headed the now-cancelled Informatics program at UNLV. He remains a professor of computer science. Professor Berghel and Alan Paller, our major speaker today, have cooperated in the past in the areas they will be talking about. Professor, welcome. We look forward to having your expertise, information, support, and input on the Board. Thanks for joining us.

PROFESSOR BERGHEL:

Thank you so much.

Agenda Item 2 – Public Comments.

AG CORTEZ MASTO:

The next item on the agenda is Public Comment. Is there anyone in northern Nevada who would like to address the Board at this time? Seeing none, is there anyone in southern Nevada who would like to address the Board at this time?

SENATOR WIENER:

No one is coming forward, Madam Chair.

AG CORTEZ MASTO:

Thank you, Senator.

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

AG CORTEZ MASTO:

Moving on to Agenda Item 2, discussion and approval of the minutes from the last Board Meeting. Mr. Earl.

MR. EARL

All of the Board Members have received several drafts of the minutes of our last meeting. If there are no corrections, then perhaps an appropriate motion might be in order.

DRAFT

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. Ipsen.

The motion to approve the minutes was approved unanimously.

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

AG CORTEZ MASTO:

At this time, we ask for information from our Task Force and Board Members regarding agency activities. Is there any Board member who would like to speak now regarding agency activities?

SA SCHROM:

Madam Chair, this is Special Agent Schrom from the FBI. We have had a number of significant activities since the last Board meeting. I would like to update the Board.

On Wednesday of this week, thirteen individuals were arrested in Las Vegas for their participation in an Internet fraud scheme. A fourteenth individual was arrested at Dulles Airport as he was about to leave the United States. The conspirators situated outside the United States listed and offered items for sale in Internet sites and occasionally also placed advertisements in newspapers. The items offered for sale included automobiles, travel trailers, and watercraft. The conspirators typically offered the items at attractive prices and often stated that personal exigencies, such as unemployment, military deployment, or family emergencies required that they sell the offered items very quickly.

To gain the confidence of prospective buyers, conspirators posing as owners of the items instructed the buyers that the transactions were to be completed through eBay or similar on-line services, which would securely hold the buyers' funds until the purchased items were delivered. The conspirators sent emails to the buyers which appeared, or purported to be, from eBay or another such entity. These emails instructed buyers to remit payment to the designated agents of those entities, who were to hold the purchase money in escrow until the transactions were concluded.

In reality, the entire transaction was a sham. The conspirators did not deliver any of the items offered for sale. Neither eBay nor any similar entity participated in these transactions. The purported escrow agents designated to receive the buyers' purchase money were actually participants in the scheme who received the funds fraudulently, obtained from buyers on behalf of the conspiracy.

Relying on the schemers' fraudulent representations, scores of buyers agreed to purchase items that the schemers offered on line and in newspaper advertisements. The conspirators kept and converted the fraudulently obtained purchase money for their own purposes. The defendants and their associates allegedly obtained more than \$3 million through the fraud scheme, which they distributed among the conspirators both inside and outside the United States.

If convicted, the defendants face up to 60 years in prison and fines of up to \$1 million. These arrests resulted from a joint investigation by the FBI and the Las Vegas Metropolitan Police Department (LVMPD).

In other cyber task force matters, in November, a man was ordered to pay \$889,415 in restitution for an Internet fraud scheme involving event ticket sales. He had previously been sentenced to 30 months imprisonment.

DRAFT

Approximately 4 individuals were convicted pursuant to federal child exploitation laws since our last meeting.

That is all I have. Thank you.

AG CORTEZ MASTO:

Thank you, Agent Schrom. Is there anyone else from one of our sister agencies who would like to present to the Board.

ASSISTANT CHIEF KUZANEK:

Madam Chair, this is Tim Kuzanek of the Washoe County Sheriff's Office. Since last reporting, the task force in the north has served 8 search warrants and arrested 9 individuals for a number of different violations.

Of particular concern is a matter I want to bring to the Board's attention is we have seen significant increases in cyber bullying that is being reported through school police.

All of a sudden, we are seeing the numbers trend up, and trend up quickly. We are looking at whether the trend has to do with reporting or whether the trend is actually reflective of more problems occurring. Additionally, we are seeing considerable increases in reports of hacking into social networking accounts. Fraud schemes are being reported to us as a result of these social network hacks where citizen accounts are affected. That is what I have for you today.

AG CORTEZ MASTO:

Thank you. Are there any comments from Board Members?

Tim, I do have a comment on cyber bullying. I hope it is a combination of the legislation that was recently passed, the education awareness of cyber bullying that is occurring, and the new reporting requirements. We are just now getting a better understanding of the types of cyber bullying incidents that are occurring in our State as a result of that reporting.

ASSISTANT CHIEF KUZANEK:

Madam Chair, I agree with you. I think a lot of it may be access to reporting. A lot of the kids being bullied now feel freer to report that they are victims of what is going on. They are more comfortable with reporting now. There has been considerable media attention. The schools are certainly being supportive by helping these individuals who are victims. Hopefully, this is the case, and things are not getting worse on the other side.

AG CORTEZ MASTO:

It is interesting that you say that kids are more comfortable reporting. That was our biggest challenge, as you know. Anonymous reporting or just getting them to report incidents of things that they were seeing is important. I hope that is the case. I think we will have a better sense of this over the coming months as we analyze the data that is starting to come in pursuant to the new legislation. It should provide us with a sense of how things are going. We will be able to look at data over several months to see if reporting is leveling off, sustaining, or whether we see more incidents of cyber bullying. Thank you. I appreciate your comments today.

SENATOR WIENER:

As Board Members may know, I visit about 3,000 children in the school district each year. So far, I have visited 15 schools. Out of those 15, in fourteen, cyber bullying was the number one concern identified to me by students in my question and answer sessions. I was privileged to offer the cyber bullying legislation in the 2009 session because I had developed the sense that this was a genuine problem. The young people struck me as amazing because they were willing to talk about it in front of their peers. When you have a fourth or fifth grade class together, I knew that the bullied students were speaking out in front of the bullies. Students are now asking

DRAFT

questions that 2 or 3 years ago, this age group would cower to ask. They are being more forthright. They are a lot more courageous to have these conversations in public.

MR. EARL

Within the last 10 days or 2 weeks, the Superintendent of Washoe County Schools appeared briefly during the local news section of a National Public Radio show. He talked about cyber bullying. One of the things he laid out was his school district's increased attention to cyber bullying at an official level. I am not sure this is causally related to what the Assistant Sheriff mentioned, but it is certainly reflective of how the school districts themselves are attempting to heighten awareness and raise public consciousness of cyber bullying.

AG CORTEZ MASTO:

Thank you. Are there any other comments?

SENATOR WIENER:

I would like to echo that from the south, Madam Chair. Dwight Jones has taken a monumental step by establishing zero tolerance for bullying and cyber bullying in the Clark County School District. Anonymous reporting is now encouraged, and the infrastructure for reporting is evolving so as to be accessible to everyone. The mantra in every school is that we do not tolerate bullying and we encourage young people to come forward. They are urged not to watch, but to come forward through the anonymous reporting system. This is the culture down here. As I visit schools, and I have another 10 or 15 to visit this school year, I am pleased to see a culture shift. I know the administration and staff – everyone from the top down, including students and their families, are aware that there will be no acceptance of this misconduct at any level. We are experiencing a culture shift. I will keep you informed as to what I see.

I know that Assemblywoman Bustamante Adams is also visiting schools and is probably experiencing the same thing. Thank you.

AG CORTEZ MASTO:

Thank you, Senator. Are there any other comments? Are there other agencies that would like to present at this time?

SAC SHIELDS:

Madam Chair, this is Rick Shields with the Secret Service. The Secret Service now has 30 task forces. Our newest members are the Kansas City Field Office and the St. Louis Field Office. Internationally, we opened an electronic task force in our London and Rome offices.

I want to express some support to you, Attorney General Cortez Masto, for your support of the Las Vegas Electronic Crimes Task Force. We now have a full time investigator there, Tom Bishop from the Attorney General's Office. He came to us about a month ago. We will be sending him to our national crime forensic institute in Hoover, Alabama for some training.

AG CORTEZ MASTO:

Rick, thank you very much. We look forward the continued partnership. We have had investigators assigned with you in the past. There is definitely a benefit to the State from that. So, thank you for that partnership. The same is true for the FBI and our local law enforcement as well. These are areas and issues for us all. We are never going to have enough resources to address all the problems. The fact that we combine forces and work together to address cyber crime in our State and cyber crime that flows across other states and countries has a great benefit to the people of Nevada. So, thank you all for your partnership and collaboration.

Are there other agencies or persons who want to present at this time? Seeing none, thank you.

DRAFT

Agenda Item 5 – Report by Christopher Ipsen, Nevada State Chief Information Security Officer, Cyber Security Grant Projects Funded by the Department of Homeland Security (DHS) for 2012.

AG CORTEZ MASTO:

Moving on to our next agenda item, this is a report from one of our Board Members, Chris Ipsen, the Nevada CISO, on cyber security grant projects funded by the Department of Homeland Security (DHS) for the year 2012. Chris.

MR. IPSEN:

Thank you very much, Madam Chair.

First, I have a couple of comments based on what we just heard. Based on our efforts and the legislation put forth, it is apparent to me that awareness of cyber bullying is increasing. As a result, we are having a positive effect.

I have talked to Senator Wiener in the past. Often times she has said, "Gosh, I have a hard time coming to Board meetings because the news is so scary. It is challenging for us."

I am here to report something very positive. As a result of our efforts, including legislation in the last session, SB 82 that passed unanimously, supported by the Board and the Attorney General, signed enthusiastically by the Governor, I can tell you that reporting by State agencies is up. This is based on the requirement to report suspected security incidents. Monitoring has begun.

One of the parts of SB 82, allowed the Office of Information Security to conduct penetration testing through the State network, and also to perform continuous monitoring of State resources. This is the first time, nationally, that these functions have been codified in state legislation.

Monitoring has begun with increased results. Actionable items internal to the State and to other ancillary agencies that use the State has an ISP have increased. Some of those agencies are public safety oriented. Additionally, SB 82 contained a requirement to report incidents or suspected violations of security policy within 24 hours. I can tell you that our level of reporting is up. Primarily, I believe this is a result of the legislation. Overall attendance at our State Security Committee is up as well.

The efforts and the support by leadership within the State has had a net positive effect on security. Reporting is up as a result of individuals knowing exactly what they need to do. Minimal standards have been set as to what represents best practices going forward.

Additionally, there are positive activities that are occurring within the State Commission on Homeland Security. For the first time, in this grant cycle, cyber security was formally recognized. This flows from the efforts of the State-wide cyber security committee. This committee represents municipalities, counties, cities, and the State. We figured that if we were going to do this, we were going to do it as a group. We were going to get together to come up with common objectives. We were going to work together and submit grant applications based on the whole State rather than the needs of a few individuals.

As a result, three cyber security grants were awarded in this grant cycle. They represent approximately 10% of the overall State-wide Homeland Security grants.

One grant, our first priority, is somewhat similar to the legislation that was enacted. It involves a State-wide assessment and continuous monitoring project. We are looking to get those individuals who represent cyber responders together, to provide special consideration for those individuals, to develop plans and capabilities for response to incidents, and also to provide tools for them. Most importantly, we will begin to develop metrics that make sense. I think it really important to quantify what we are doing.

DRAFT

The second grant that was awarded to us represents inroads into identity management, specifically around authentication of global systems. This grant represents part of the national movement towards identity management. If we can identify who people are and how they respond, then we can verify they are the right people to access systems. This grant works toward that. Special attention is being made to map toward the national initiatives in this area.

Third, we have a UASI¹ - specific grant. The Clark County area is a designated UASI area within the homeland security process. Those grant funds will be used to enhance disaster recovery within the IT arena.

Those grants are moving forward. We are working collaboratively. They represent a positive step forward. I want to say that I am very happy to say at this holiday season that, as a state, we are beginning to make inroads to perform activities that represent a positive outcome. Thank you very much for your support over the years. I want to let you know that your efforts are not going without positive outcomes. We are moving forward.

I'll be glad to answer any questions.

AG CORTEZ MASTO:

Chris, thank you. Are there any comments, or questions for Mr. Ipsen?

ASSEMBLYWOMAN BUSTAMANTE ADAMS:

Chris, did you mention the total dollar amount of the grants?

MR. IPSEN:

Each grant represents, roughly, about \$500,000. The first grant I mentioned was for \$465,000; that was continuous monitoring. The second grant, involving identity management, I believe is around \$350,000. That includes a survey. We anticipate getting actionable product from that as well. The third one – and I believe Laura Fucci in the south may want to speak to this – I believe it was in the three to four hundred thousand dollar range.

I can get the specific numbers if you would like. I certainly can report on those grants as we report expenditures to the Commission on Homeland Security if you would like.

MS. FUCCI:

Hello. This is Laura Fucci. The third grant is \$180,000 for disaster recover.

MR. IPSEN:

I was way off.

ASSEMBLYWOMAN BUSTAMANTE ADAMS:

I have one more question. So, are there existing personnel who will be able to utilize this grant? Or, are you going to bring in additional individuals to carry out the work?

MR. IPSEN:

Our focus has been to address these challenges collaboratively as an entire State. One of the grants is an external assessment that will most likely go out to a vendor. This is the identity management grant. I can speak to the grant application with which I was most involved and for which I am primarily responsible. We may hire a project manager for that, or we may deal with it internally. I am trying to be as efficient as I can with the existing resources so we can maximize resources going to the counties and to the rurals. We are very mindful of using resources as judiciously as we can. Most of those resources will be spent with existing State, county, and, in some cases, private sector individuals, in training and software and other capabilities. For the most part, this will be internal to the State.

¹ Urban Areas Security Initiative.

DRAFT

AG CORTEZ MASTO:

So, Chris, as a follow up to that question, is the State the recipient for all three of these grants?

MR. IPSEN:

No. The State is the recipient of one of the grants.

AG CORTEZ MASTO:

Which one?

MR. IPSEN:

The first grant. We applied for that through the Department of Information Technology. That department doesn't exist anymore. It was combined into the Department of Administration. I talked to the Department of Emergency Management. They have agreed to manage that on the State's behalf. That is the first one.

The other two grants: one was allocated to the City of Las Vegas – the identity management grant. We will be working with them on that. The last grant was awarded to Clark County. Laura Fucci and Irene Navis and their staffs will be managing those grant resources.

AG CORTEZ MASTO:

So, is it safe to say that through the state-wide cyber security committee, which sounds like a diversity of stakeholders at the State and local level, will be helping to manage these grants to ensure the dollars are used in the most efficient manner?

MR. IPSEN:

Absolutely. I think in some cases, Clark County has been quite understanding that some of the needs of the State do not necessarily represent the needs of the county. In talking with Laura, and I hope this is not too much information, her priorities did not end up being the top priorities. But, from a State perspective, primarily from a rural county perspective and from the perspective of some of the smaller city and county governments, since they were not as mature in some areas as Clark County is, they are certainly a focus of this grant. It is truly a state-wide initiative that we are looking at.

AG CORTEZ MASTO:

Are there any other questions or comments? Chris, thank you very much for your presentation.

Agenda Item 6 – Report by Timothy F. Cary, Exercise Officer, Nevada Division of Emergency Management, What Nevada's Selection in the DHS-sponsored Community Cyber Security Maturity Model Program means for Nevada and Clark and Washoe Counties.

AG CORTEZ MASTO:

The next agenda item is Agenda Item 6. This is a report by Timothy Cary, the Exercise Officer with the Nevada Division of Emergency Management – What Nevada's selection in the DHS-sponsored community cyber security maturity model program means for Nevada and Clark and Washoe Counties. Welcome, Mr. Cary.

MR. CARY:

Thank you Madam Chair and distinguished Board Members.

I am Timothy Cary, the State Exercise Officer for the Division of Emergency Management within the Department of Public Safety.

DRAFT

I am here today to speak about Nevada's selection as one of the two states to receive the Department of Homeland Security's annual "Community Cyber Security Maturity Model" implementation for two communities within selected states, namely Clark County and Washoe County/Carson City.

The Division of Emergency Management became aware of this DHS program last year through a DHS solicitation to all states' Homeland Security Offices. As you may remember, the Nevada Office of Homeland Security was merged last year with the Division of Emergency Management under the Department of Public Safety. It was at that time during the merger of our two agencies that we became aware of a solicitation for 2011. However, the deadline for submission was less than two weeks away, too late for us to respond effectively last year.

This year, working with the DHS' National Cyber Security Division we received the solicitation early and, DEM working with the Department of Information Technology (now Enterprise IT Services Division within the Department of Administration) and through the Governor's Office, requested consideration for the State and its two major communities of Clark and Washoe Counties for this DHS funded program.

Prior to submitting Nevada's request, both DEM and IT Services reached out to our counterparts in both Clark and Washoe Counties, specifically the Chief Information Officers and Emergency Managers of each jurisdiction, and we received full support for the State's effort in requesting this cyber security assistance. Many other partners within the state and state government also strongly supported the State's efforts.

In DHS' solicitation letter regarding the Community Cyber Security Maturity Model it reads:

"This model serves as a tool for states and communities to measure their level of cyber preparedness and provides a roadmap for states and their communities to develop a viable and sustainable cyber security program."

Letters requesting selection were required to contain: (1) A statement of support with a specified point of contact from either congressional or state leadership, (2) The two proposed pilot communities for the state, and (3) A description from the state as to its previous cyber security efforts at both the state and community levels

In September, the Governor signed the letter requesting consideration for Nevada to be selected.

The letter of request spoke of some of the cyber security efforts within Nevada, in particular Senate Bill 82 (SB 82), supported by this Board, which not only strengthens cyber security efforts throughout the State by incorporating continuous monitoring and penetration testing into the mission of the Office of Information Security, but also enables the Enterprise Information Technology Services Division to provide goods and services, including combined procurement services, to all government agencies at State, county and municipal levels at lower cost.

Also referenced in the Governor's letter was Nevada's pending DHS grant application which contains, for the first time, an investment justification for three (3) cyber security projects. These projects emerged from Nevada's Commission on Homeland Security.

In November DEM and the Enterprise IT Services Division received notice that Nevada was one of the two States selected for this cyber security assistance. The other state selected was our neighbor to the south, Arizona.

In conversation between the DHS contractor and State representatives it was decided to include Carson City, the seat of state government as part of the northern community. And so our two major population centers of Clark County and Washoe County/Carson City will receive the full

DRAFT

support and assistance from the Center for Infrastructure Assurance and Security in implementing the Community Cyber Security Maturity Model.

I believe all Board Members were given the background documents that describe the Center for Infrastructure Assurance and Security as well as the roll out plan for the program.

The Center for Infrastructure Assurance and Security requested official points of contact representing the state and the two communities, and it was agreed upon that the Enterprise Information Technology Services Division and the Chief Information Officers for Clark and Washoe Counties would fill those roles. DEM and the Emergency Managers of Clark and Washoe Counties will be working closely with these Departments and Agencies to insure successful implementation of this program. As a team we are currently in the process of working with both the public and private sectors in these communities to begin this fourteen-month program as soon as late February 2012.

Nevada's selection for the Community Cyber Security Maturity Model in our two major population centers of Clark and Washoe/Carson counties along with the State government will give Nevada its first *comprehensive* and *systematic* assessment of our cyber security posture and preparedness in as communities, and not just as separate departments or agencies, and provide training solutions that will be tested in exercises **at no cost to the State**.

Each community will be assessed and trained separately, take part in community-specific discussion-based exercises, such as seminars, workshops, and tabletop exercises separately. However, near the end of the fourteen month program will take part in a unified, concurrent operation-based functional exercise in response to a simulated simultaneous cyber attack on both communities and the State government.

I stand by ready to answer any questions.

AG CORTEZ MASTO:

Mr. Cary, thank you very much. So, at the end of the day, what does this mean for Nevada.

MR. CARY:

As I see it, for the first time, the community as a whole will be taken into a more advanced stage of cyber preparedness – both the public and private sectors as well as individuals within the community – essentially, all who want to take part in this cyber program. Everyone and every organization, both public and private, within both the north and south designated communities is welcome to come into this program. The program involves self-assessment, the receipt of training, and participation in exercises designed to lift our cyber security preparedness.

AG CORTEZ MASTO:

Thank you. Are there any questions or comments?

SENATOR WIENER:

If I may... I heard early in your presentation that we were too late to apply. It sounds like this involves an annual application process, but the roll out is accomplished over a 14-month cycle. Is that correct?

MR. CARY:

Yes. We first learned about the program last year, in 2010. That solicitation was for implementation within 2011. We learned about the program with less than two weeks remaining before the submission deadline. We talked about it internally with DEM and DPS, and just felt we could not garner the kind of support needed and then go to the Governor's office for a letter supporting our application.

DRAFT

This year, working with DHS's national cyber security division, we obtained the solicitation information very promptly. We started acting on it immediately.

SENATOR WIENER:

Madam Chair, if I may continue. How money did we acquire for this 14-month program?

MR. CARY:

We acquired the services of the contractor. They are out of the University of Texas, San Antonio. They have worked with other states previously – some 6 or 7 states to date. Currently, they are working with North Carolina. I believe they have now completed Illinois. We receive their services. They will come out and plan with us as to how best to reach out to the community as a whole and who the participants should be. We select the venues. We help them with invitations and registration. They even provide lunch. Any training or exercise activity that goes over lunch time will be covered under the DHS contract support. So, we received a lot.

With this particular program, we will get out of it what our two major communities are willing to give and contribute to the process. Therefore, over the next several months, we want to have a very strong outreach effort. In late February, I believe it will be the last two days of the month, February 28th in the north and February 29th in the south, the contractor will meet with leadership (both public and private) to take part. Contract planners understand it is difficult to get everyone in just a single meeting, so they will spend all day in both communities, holding 3 or 4 meetings, to get leadership support. They will also explain to leadership what the program is and what it means for Nevada. They will be requesting assistance for the program to be as effective as possible for our two major communities.

SENATOR WIENER:

So, it sounds as though Nevada and Arizona are receiving in-kind support, that is, the expertise. Is the State somehow matching real dollars from a State budget to roll this out?

MR. CARY:

No. What we are receiving is their full support and work. This is being provided at no cost to us. We are going to try to identify venues that are no-cost within both communities, so that we have venues to accommodate the right numbers of people.

Within the Emergency Management agencies, we work with invitations and registrations all the time. The only concern my chief has is this. They do work with the communities separately. So, in theory, there should not be the need for travel – north to south or south to north. However, within State government, there may be individuals at times who want to go south. We want to work within the State to find out whether there are people at Enterprise IT Services, Emergency Management, or Homeland Security who may need to travel. So far, that is the only cost we can think of that may come into play. But, right now, I can not say whether even that will be necessary. DEM has personnel in Clark County we can utilize. So, within my own agency, I am not sure that any travel will be necessary.

SENATOR WIENER:

One final question, please. You mentioned that the program is being wrapped up in other states. Is this a grant that is given to only several states at a time? Do we have an opportunity later on to apply again so that we can continue to grow and improve our access and capabilities in the State?

MR. CARY:

I am glad you asked that question. The program has been running for 4 or 5 years. I believe they have done up to 7 states so far. As you may think, some of the larger states were first, Florida, New York, Illinois, California. Currently, they are completing the program in North Carolina. They believe they have two more months for completion. They will be working with Arizona and Nevada separately. Are there future possibilities? One of the states that received the program

DRAFT

initially a few years ago is Delaware. Delaware has gone to the next step. Within the Community Cyber Security Maturity Model there are different levels of preparedness. Delaware is at a point now where the state has justified a request for support from the same contractor to get the contractor to work with the state a second time to get it to the next higher level of preparedness.

Nevada is starting at the first level, like the other states, although, internally, some of our departments, agencies, and entities may be at a higher level. But, as a community, we have a goal to reach the next level over a 14-month period. Perhaps, in the future, we can request an additional program, 2 or 3 years from now, for consideration to the next level.

SA SCHROM:

Madam Chair, as you may know, the FBI is involved in the InfraGard chapters. We have two InfraGard chapters in Nevada, one for southern Nevada and one for Sierra Nevada. It sounds like we may have the people that you need. We have a lot of security people. We have a lot of people who do continuity of operations from the community – both public and private sector.

I would like to let you all know that we can probably assist in this effort. We can help get the InfraGard leadership together as well as the people who would actually participate.

AG CORTEZ MASTO:

Thank you, David. That's a great point. I would also like to offer the assistance of this Board. If we can help in any way, by, perhaps, identifying individuals who should be participating, please reach out to Mr. Earl. He can work with the Board Members to help identify how we might assist.

MR. CARY:

Thank you, Madam Chair.

AG CORTEZ MASTO:

Are there any other comments or questions?

ASSISTANT CHIEF KUZANEK:

Mr. Cary, I have a couple of questions. First, have the Fusion Centers, and more specifically, the Silver Shield program, been engaged by involving their contacts and leadership in the outreach effort you have made and intend to make?

MR. CARY:

Yes. Within DEM, as you know, the State's Fusion Center is collocated with us. Working through them, we have reached out to individuals such as Mr. Bob Dorsey early on in the process when we were working to get our letter of request. He saw the literature on the program. He supported the effort. He said, "We need this." I believe we have also reached out to our point of contact in the southern Fusion Center. They are interested in it.

The information supplied by the contractor lists the type of participants that have been involved in previous states that they really want involved. InfraGard is one. Fusion Center participation is very strongly supported. They are near the top of entities to engage within the program.

We do have information on the program. This morning, I have asked for even more as we reach out to both communities. I am willing to send that information beyond what has been presented to Board Members. It gets into particular details, like listing participants they would like to see. I am willing to send that out, and, as I get more information, continue to distribute it.

ASSISTANT CHIEF KUZANEK:

I appreciate that. It is very encouraging. The Silver Shield program, dealing with the interface between the public and private sectors, is very important since relationships have been built up over time. These could be very valuable in terms of getting the appropriate folks to the table.

DRAFT

Additionally, it sounds as though this program is fairly mature – some 4 or 5 years old. Do we have access to what was delivered to programs that have already been completed, in terms of what successes they saw, the gaps that were identified in various states, that type of thing? Is that available to us?

MR. CARY:

I don't have that currently. However, I have started reaching out towards North Carolina. I hope to find my counterpart there who is working on that project as I am to gather more of that information. We have a neighboring state where I have points of contact. While they are in the process of a physical move, I want to reach out to California to get more information. I have reached out to Arizona just to say congratulations.

I believe we can get more information about the successes in implementation of the program, what they identified as gaps, as well as lessons learned if they were to do the program over – how they would approach the implementation. We are definitely interested in those sorts of things.

ASSISTANT CHIEF KUZANEK:

Thank you. I appreciate that very much.

AG CORTEZ MASTO:

Mr. Earl.

MR. EARL:

Chris Ipsen and I participated in a call with Mr. Cary. This was essentially the initial discussion, at a very high level, involving the outline of the program. My personal observation is that the team at the University of Texas demonstrated tremendous flexibility and tremendous willingness to adapt to the situation as it exists in the State. Some of our discussions involved what Nevada has done at both State and community level through the present day, involving Fusion Centers and so on. The team from the University of Texas is taking all of this into consideration. They appear to be extremely flexible in terms of adapting their program to meet the actual needs of the State and communities in light of the progress we have made to date and in light of the different mechanisms that have been put in place that may vary from state to state. I just wanted to provide that personal observation.

AG CORTEZ MASTO:

Thank you. Are there any more questions or observations?

MR. IPSEN:

I have one quick comment. This is an expansion of something Tim mentioned. This was a competitive process. I want to complement both Tim and Jim Earl. They both worked actively on this process. Initially, DHS was going to make an award to a single this state this year.

I have learned from DHS that, based on the strength of our application, DHS agreed to do two states in this cycle, so that Nevada could be included.

I think that is important – when people go above and beyond by putting extra effort forward. We are winning because people are doing extra things. I want to complement both of those individuals for their contributions in that process. I also want to recognize the Governor's Office. It reached out as well. The Governor did sign the application. I think this is genuinely a team effort going forward.

AG CORTEZ MASTO:

Thank you. Is there anyone else? Thank you very much, Mr. Cary. I appreciate your being here and working with all of us. This is a big deal for the State.

DRAFT

Agenda Item 7 – Presentation by Alan Paller, Director of Research, SANS Institute, Four Forces Reshaping Cyber Security and The Imperatives and Opportunities They Create.

AG CORTEZ MASTO:

Moving on to our next presenter, Mr. Paller. We are really honored to have him here today.

I know the Board Members have received his background, but I would like to read a little bit for members of the public who may be watching the web cast.

Mr. Paller runs the largest cyber security education institution, with more than 140,000 alumnae in 70 countries. It is also the largest training provider of deep technical cyber security skills for the cyber, intelligence, and law enforcement agencies.

He helped establish the national cyber security talent search and talent development program, called the U.S. Cyber Challenge. In the year 2000, President Clinton recognized his leadership by naming him as one of the initial members of the President's National Infrastructure Assurance Council.

Alan has testified multiple times before the U.S. Senate and House of Representatives, and has helped Senate staffers with initial drafts of several pieces of legislation. His contribution to the Rockefeller – Snow draft legislation was specifically acknowledged in the text of the draft legislation.

Under President Bush, the U.S. Office of Management and Budget and the federal CIO Council named Alan as their 2005 Azimuth Award winner, a singular life-time achievement award recognizing outstanding government service of a non-government person. If that wasn't enough, in May of 2010, the Washington Post named seven people as "worth knowing or knowing about" in cyber security. The list included General Alexander, who heads the U.S. Cyber Command, Howard Schmidt, the White House Cyber Coordinator, other national leaders, and Mr. Paller.

So, we are honored to have you here today. His topic is "Four Forces Shaping Cyber Security and the Imperatives and Opportunities They Create." Welcome.

MR. PALLER:

Thank you. That introduction was way too nice.

I am going to try to be short because I like discussion. I am going to move a bit quickly. So, interrupt me when you hear something you don't agree with, rather than waiting until the end.

I don't know whether the slides will be viewable in southern Nevada. If not, I will describe them in greater detail. What are your thoughts?

AG CORTEZ MASTO:

Let me ask. Are those of you in Las Vegas able to see the PowerPoint presentation?

SENATOR WIENER:

Yes, we are.

MR. PALLER:

Great. We can move more quickly.

I am usually the guy who is asked to do briefings on how bad things are. Those are great. You can scare people to death.

DRAFT

The problem is that those briefings end with people being scared to death and not doing anything. So, I thought I would do something completely different this time. I want to show you the good things that are going on in cyber security, and where a couple of those initiatives can be harvested in Nevada because of some special characteristics you have here that other places do not have.

Now, don't call me a Pollyanna, but this is a reasonably positive briefing on cyber security.

I am going to start with the most interesting innovations identified at the Cyber Security Innovation Awards that Howard Schmidt and I did a couple of months ago.

The most interesting innovators recognized in the National Cybersecurity Innovation Awards

- *Who discovered the 4 key security controls that stop all low and medium sophistication targeted intrusions?*
- *Who discovered how to radically reduce the vulnerabilities on more than 200,000 computers – without command authority?*
- *Who discovered how to develop security experts using cyber simulators.*

2

This is your opening quiz. Who discovered the four key security controls that stop all low and medium sophisticated targeted intrusions? When I talk about “targeted intrusions”, this is what I mean. You have heard about all the intellectual property getting stolen. Everyone says it is the Chinese, but it is really a lot of people. This is how we have lost military secrets. This is how the attack on Google was undertaken. This set of four security controls seems to be stopping all the low and medium sophisticated attacks like this.

Then, who discovered how to radically reduce the vulnerabilities of more than 200,000 computers

without having command and control authority? This means that without having command authority over people, they still got the bugs out of the computers.

Next, who discovered how to develop security experts using simulators? It is hard to just teach people in a class. So, who figured out the hands on approach?

I am going to show you those stories.

The CEO security dilemma

- Security can be a black hole for spending and time
- Raises 3 questions:
 - What do I have to do to secure our systems?
 - How much is enough?
 - Whom can I trust to answer those questions?
- Today this devolves to: What are the most important things to do now to stop **targeted intrusions**?

3

This first one is the most important development. It is the first time I found CEOs of major companies feeling good about talking about security. They usually try to hide from it. The security guys come in, scare them to death, and then give them a huge bill to fix the problems. Then when they are asked if that will actually secure their system, the security guys say, “No.” “You will have to bury the computers to fix them.” That doesn't help.

This is the first time I have heard senior people say, “I can get my arms around this one.”

When you talk to CEOs of major corporations about security, and when they are being honest with you, they say, I have three questions: “What do I have to do? How much is enough? And, whom can I trust for the answers?” “Everybody is telling me that I have to do everything. But how much is really enough?”

We have never had answers to that question.

DRAFT

Today, in the places where data is being stolen, those questions devolve into a different question: "What do I have to do to stop these targeted intrusions – the ones that are stealing intellectual property, and, therefore, stealing our nation's future?"

The 4 controls in the Sweet Spot

- Australian DSD
- All civilian and military **targeted intrusions**
- 35 mitigations – too many?
- 4 mitigations – the "sweet spot"
- Ian Watt – Australian SecDef
- Two agencies finished first
- Results




The Australians are the ones who discovered the answers. This is a picture of Howard Schmidt in the White House giving the award to Vicky Brien. She is basically the Australian top intelligence person stationed in the United States.

The Australian Defense Signals Directorate (DSD) is a combination of the NSA and the DHS. Australia only has one department. The department head, who is the Secretary of Defense in our terms, manages security across all military and civilian federal agencies. He had the people at DSD figure out how all of the targeted intrusions had been done. He asked, "What was it that

allowed the bad guys to get in?"

They came back and essentially said that there were 35 things that needed to be done to stop these intrusions.

Note the division after number 4
Find them? Google: DSD 35 mitigations



I was amazed because our government has 240 things on 10,000 pages. These guys had 35 on one page. Ah hah! A major development! And, I talked about this a lot.

But it turns out even 35 are too many.

If you have 35 things to do, you can't do them all. You have to bring more order to things.

Last year, the Secretary asked again. This time, staff came back saying that four of these actions get rid of just about all the targeted intrusions. We can't stop the RSA-level attacks – the really

advanced ones, where a nation state will spend anything to attack successfully. But, we can stop a whole lot of attacks, and these four do that.

Then the Secretary ordered all federal government agencies in Australia to implement them in February. By June and July, two agencies had finished the implementation. The report back is that while other agencies are still getting hit, those two agencies are no longer getting hit.

So, this is one of those enlightening "It really works" moments.

Now, he lost his job on the 11th of August, but the security plan has nothing to do with that. He was made the top civilian official in all of Australia. So, he moved up from Secretary of Defense to Secretary of the Cabinet, which is the top job. This had nothing to do with the cyber implementation – but at least it didn't hurt his career.

This is the chart that was produced. The slide is not for reading. If you want to read it, anyone who is listening can Google "DSD 35 mitigations." You will find this chart.

DRAFT

The magic line on this chart falls right after the first four mitigations – the first four lines of advice². There is a line that says, “After you have done these four, then allocate resources to the remainder.”

No other government has ever done that in cyber security. Every other government has produced list after list after list of thousands of things you have to do. And, if you do the first 20, they say that was not enough.

The Australians are saying, “Do these four, do them now, because they work.” This is a very big shift in how to think about cyber security.

This is completely different from the top manager’s point of view, because the top manager can say, “I want to know if I got it done.”

Where as, before, no one had a discussion like that about government cyber security. No one ever asked, “Am I done?”

This is something that can actually be done across the agencies of government.

This takes us into the second award. What got this started was a push in the White House about 4 years ago. Melissa Hathaway, the cyber czar at the time, figured out that we were spending too much time listening to people who did not know how attacks were being done, who tried to tell us what to do.

All the cyber defenders in the world have no clue as to how the attacks are being done. None. But they are telling everyone else what to do.



She said, “I’m going to go to the guys who understand how to play offense.” There are two groups of these people. One is they guys who do this. We have people in the United States who do that for a living. The others are the people who go in and clean up the messes afterwards – the ones who go in and do the high-level forensics after the attacks, like the FBI guys, the Air Force OSI people, and the Secret Service people, and the NSA blue team, and others.

That led to a project where all of these groups came together – the NSA red and blue teams, the

DOD cyber crime center (DC3). DC3 is the group that does all the forensics after the really bad military attacks and the attacks on Lockheed and those types of companies. They really know what is happening.

Interestingly, the best of them all came from the Department of Energy national laboratories. The labs have a combination of really bad attacks. They are getting hit all the time because nuclear secrets are a pretty valuable treasure chest. And, they have really smart people. When you combine really bad attacks and really smart people, you find all sorts of interesting things about how the attackers work.

² The first four Critical Security Controls are: (1) Inventory of Authorized and Unauthorized Devices, (2) Inventory of Authorized and Unauthorized Software, (3) Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers, and (4) Continuous Vulnerability Assessment and Remediation.

DRAFT

The point is, all of these people work together. Everyone thinks that what they do is their own private intellectual property, so none of them would normally share it with anyone else – even across this group.

But there is a guy named John Gilligan. I bring his name up because it will come up again. He was the CIO of the Air Force, CIO of the Energy Department, and Obama's transition team lead on cyber security for the intelligence community and DOD. So, he is really one of the super guys. He brought these different groups together. It was his personal leadership that brought them together.

A lot of good things that happen in cyber security come from personal leadership, not just someone who comes up with a great idea. So, he got them together.

And his plan ends with something. We'll get to that in a moment. I'll show you the whole plan.

Who understands offense?

- NSA Red Teams
- NSA Blue Teams
- DoD Cyber Crime Center (DC3)
- US-CERT (plus 3 agencies that were hit hard)
- Top Commercial Pen Testers
- Top Commercial Forensics Teams
- JTF-GNO
- AFOSI
- Army Research Laboratory
- DoE National Laboratories
- State Dept.

Would they be willing to combine their knowledge of attacks and offense to define the most important defensive investments CIOs must make?

He said, "Start with the attacks. Offense has to inform us. You can not put anything on your list unless you can prove there has been an attack that has happened or an imminent one that will use this technique." Otherwise, you are just worried that the lights are going to fall down.

What is fascinating is that in less than 5 weeks, all those people came together about what controls were needed. There was no fight about the controls. The fight was always about what to do next if you don't have the primary controls in place. Because anything can happen, your defenses become infinite.

If you start with the attacks, you can focus on actual controls. Then – and this is the big thing – not to find out whether you are vulnerable, but to automate the monitoring of it.

The attacks happen way too fast for anything manual. So, if you are not automatically checking on this stuff, you might as well not be doing anything.

The idea of auditing once a year or once a quarter is silly. You might as well not audit. If you think it does some good, you're wrong. It does no good. You are giving false attention to the wrong problem.

Gilligan's plan for creating and moving the 20 critical controls to broad implementation

1. *Start with attacks (offense informs defense)*
2. *Agree on the controls that would stop or quickly recover from the known attacks.*
3. Agree how to automate and measure effectiveness
4. Public review period and revision
5. Pilot program in two agencies and tuning
6. Establish tests that reliably evaluate effectiveness
7. Find the tools that automate each control
8. Gain OMB, CIO and IG agreement to adopt the CAG.
9. *Buy it together to keep costs down.*

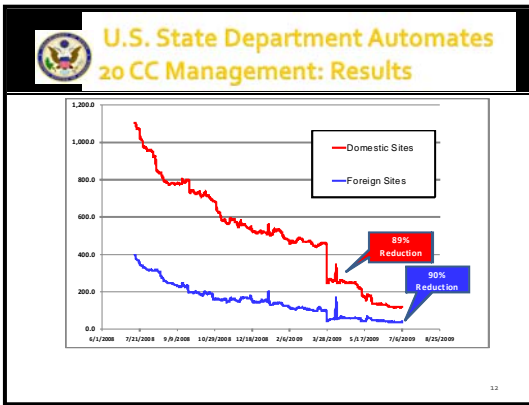
Then there was a public review period, a pilot program in two agencies to test to prove it was effective. And find tools to automate the process.

The reason John Gilligan invested his time in this is based on one simple thing. Look at number 9 on this slide. It turns out that if organizations buy things together, they can bring the cost way down. We have one great example of that. It turns out that DOD and the states got together a few years ago to buy encryption software for laptops after the VA had lost lots of data from a laptop that was stolen. The commercial price for that software at

Best Buy is roughly \$243. The GSA price was about \$97. When they got done with a group buy, Bob Lentz, who was then the CISO for DOD – just left last summer – told me just before he left the price was at \$5.50. So we went from \$243 to \$5.50. How can they sell it so cheaply?

DRAFT

Now, I want to prove that it really works. These are measured risks across 200,000+ systems over 12 months. The next 12 months, it went down another 45%. So, this is a continuing improvement.



There is another thing that happened. If you remember, almost two years ago, Google got hacked. That was a transformational moment in cyber security. That was when the CEOs of a lot of big companies said, "I don't think I can trust my security people." If Google got hit, and my guys are saying that I am safe – I don't think so.

This changed people's thinking about cyber security – when Google couldn't protect its own systems. That made people look a little more closely at their own operations and they found things they didn't like.

More Proof: Federal Aurora Response

- Google Hack
- IE Vulnerability – zero day
- IAVA and government notices
- What percent of systems were reported patched at DoD in four months?
- What percent were actually patched at State in the first 9 days?

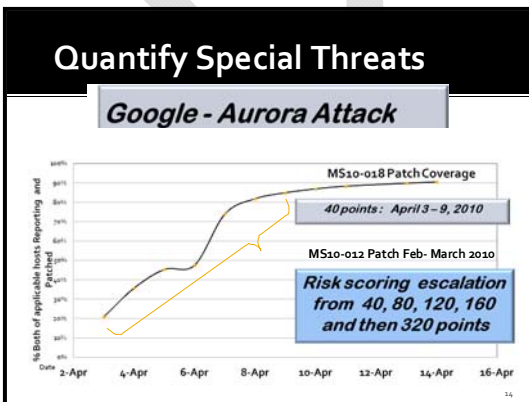
The hack that was used against Google, and the follow-up hack, was an Internet Explorer vulnerability that was present on just about every computer.

DOD has a program called IAVA: "Information Assurance Vulnerability Alert" or something to that effect. They send out a command and control message to every military organization that says, "You have two weeks to fix this. Get back to us within two weeks to tell us that it's fixed, or, if you haven't fixed it, identify the system that is not fixed up." This is the command and control authority that does this.

So, I was in the office of the woman who ran that program. Her boss was in the room too. This was two and a half months after the command went out. And I asked, "How many of your systems have been fixed?"

And she said, "About 65%." And her boss said, "And they're lying." Meaning this. In DOD,

command and control means, "We will tell them to fix it. They will report that they fixed it. But all they mean is that they put out a message that says, 'You have to fix this.'" But that doesn't mean it's fixed, it just means that the message has gone out. Later tests found out that only about 20% of the computers had actually been fixed.



The State Department is measuring every day, the status of every machine.

Here is the State Department data on exactly the same vulnerability.

On the 4th of April, the Department was at 20% patched. On the 14th of April, the Department was at 90% patched – actual, not someone reporting what they think their superiors want to know.

DRAFT

That is continuous monitoring and mitigation. But, how did they get that many thousands of people to fix that stuff that fast? Right? That's the question – no command and control authority at the State Department. The ambassadors in charge of embassies are all powerful over their operations. So, central has no control over anybody. How did they do this? It's fascinating.

Keys to State Department Success

- System administrators have only 30 minutes/day for security
- Targeting them on the most critical tasks allows them to use that time effectively
- Grading them and making the grades positive and visible is highly motivating
- Deliver charts only after 6 months of private improvement
- Raise the standards to continue success.

What they decided was this. Since the systems administrators have only a few minutes to work on security everyday because they have a lot of other things to do, we will tell them every morning what the most critical thing is that they need to fix that day. We know because we are monitoring every system.

And, we are going to give them "points" on everything they do. So, if there is a really critical fix, and you do it, it gets you a lot of points. If it's not that important, it doesn't get you as many points.

Graphics Guide Action

"Worst problems first"

So, you will fix the things that really matter. And we will graphically point it out to you – we will show you what specific system has those high risks – so you know what system to fix what on.

Then, we will grade you on your performance over time. So, every day, every office in the State Department gets a grade. And every manager gets a grade.

And the grades are posted daily. The winners get "A"s, and the losers get "F"s.

But they did another really fascinating thing. They didn't publish the data until 6 months after they started measuring it.

So, every office had 6 months to get better. By the time the first scores were published, over 85% of the offices were getting "A"s. And, they had come a long way to that "A" score.

They then changed the score that got you an "A". It became "11", when it started at "40". So, when reporting started, if you had 40 risk points, that was good enough to get an "A".

Grading Scale

Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

A few months later, you had to fall to 35 risk points in order to keep your "A". A few months later your risk had to decline to 30.

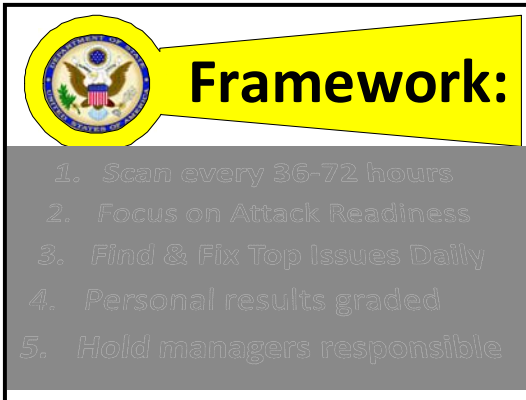
Once people have an "A", they really like to keep an "A".

If all you do is beat them up, they don't move. But if they got an "A", and they are getting reinforcement from their bosses to keep that "A", the results are just fascinating.

Originally, central would scan every 36 to 72 hours, the top issues would be found and fixed

DRAFT

daily, and the top managers would be held responsible. The reports go all the way to Hilary Clinton.



Framework:

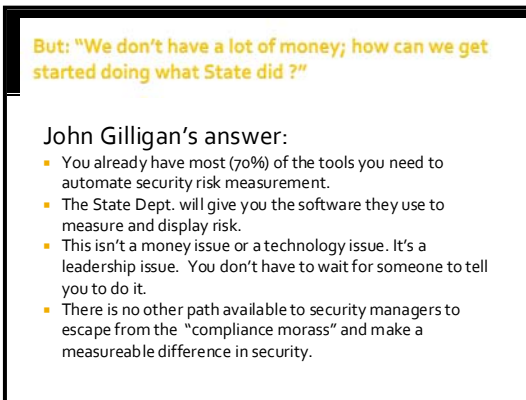
1. Scan every 36-72 hours
2. Focus on Attack Readiness
3. Find & Fix Top Issues Daily
4. Personal results graded
5. Hold managers responsible

It matters – security does. You know how the State Department is about security, particularly after Wikileaks. So, this really matters.

If you care about security, you do both monitoring and mitigation. If you don't, and you just monitor, then you know bad things are happening. And you can talk about them, but so what?

This is a really cool shift about how people are looking at security. The CSO at State, John Streufert, gives away the software. It was paid for by government contract, so he gives it away. He gives away the scoring system and the math

behind it. He provides help and assistance at no cost. More than 230 organizations are in some stage of implementation of this system across the world.



But: "We don't have a lot of money; how can we get started doing what State did?"

John Gilligan's answer:

- You already have most (70%) of the tools you need to automate security risk measurement.
- The State Dept. will give you the software they use to measure and display risk.
- This isn't a money issue or a technology issue. It's a leadership issue. You don't have to wait for someone to tell you to do it.
- There is no other path available to security managers to escape from the "compliance morass" and make a measureable difference in security.

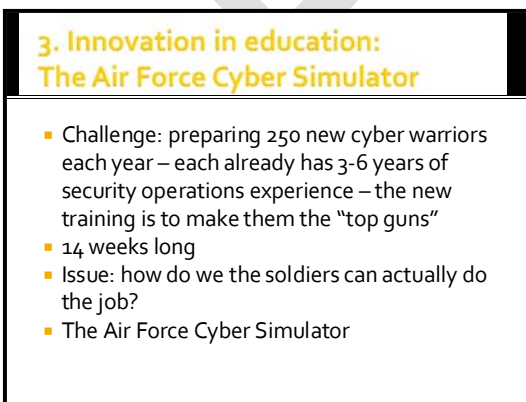
NSA was brought in to verify the measurements. So, they have come out with a 60-page report showing that the measurement systems being used are the right measurement systems to measure risk in these computer arrays.

I will give these hand outs to the Board Members in Carson City and will ask Jim to send them to folks in Las Vegas. These posters just came out a couple of days ago. You open it up, and it pulls all of what I have shown you together.

It shows the State Department slide, the NSA ratings, the Australian top Critical Security Controls. Last Friday, the United Kingdom announced it was going to adopt this as well for all their cyber security. Leadership told MI-5 guys, and the MI-6 people, and others that this was how they were going to measure security.

So, we have some momentum behind measurement.

Before I go to suggestions about what might work in Nevada, I want to talk a little about innovation in education. This is a manpower issue. Cyber security is a manpower issue, and I want to prove that in a moment.



**3. Innovation in education:
The Air Force Cyber Simulator**

- Challenge: preparing 250 new cyber warriors each year – each already has 3-6 years of security operations experience – the new training is to make them the "top guns"
- 14 weeks long
- Issue: how do we the soldiers can actually do the job?
- The Air Force Cyber Simulator

The Air Force is the other agency that got an award from Howard Schmidt. They found a way to train cyber warriors.

The problem with most cyber security education is that is book learning. When it is not book learning, it is exercise learning. But, you don't know whether someone, working under pressure, can do the job. So, it's a little like having a pilot learn to fly in the classroom with no simulators. You just wouldn't know if he knew what he needed to know.

So, the Air Force brought in cyber simulators.

DRAFT

Now, every student goes through these simulators to ensure they actually know what they need to know. The simulators measure them on such things as their operating system hardening vulnerabilities, their penetration testing, web application testing, intrusion detection testing, wireless forensics, packet analysis, malware... It monitors and scores them all the time. The Air Force has integrated this into the training – just the way it is done at Top Gun school. You do exercises to see how you are doing. You do more exercises to see how you are doing.

It's a shift in thinking about cyber security – from it being something you learn from a book, to it being something you actually have to know how to do. And, you have to do it under pressure when other people are fighting against you. It is just a whole different view of cyber security training. I am going to come back to this.

Evolution

- Initial use: for pre and post assessment
- Discovery: this was the "best part of the training" for participants; AF pilots recommended it be used as the foundation
- build the training around the assessment – every day raising the challenge level
- Creates a "top gun" training environment that challenges and accelerates learning of both mid level and the most advanced practitioners and provides diagnostic comparative assessments on all 9 score card elements.

The Air Force evolution was interesting. Originally, they were only going to use simulation as a "before and after" tool. "Before" to teach airmen that they didn't know as much as they thought, and "after" to see if they had learned anything.

But, it was the airmen who had gone through pilot training that said, "You've got a simulator. Let's use this as part of the instructional training." That's how the thinking evolved. It was a big breakthrough. Now, lots of other people have been searching for a way to measure whether people actually know how to do remediation and other

things. Everyone claims to know what is necessary, but when you sit them down in front of a terminal, you find out they don't have a clue what to do. So, how do you know? Simulators are a great way to find out.

Resulting growth opportunities and Nevada's unique assets

1. Rapid and substantial improvement in state/local cybersecurity in Nevada (making it the model for the nation) while building mid-level security skills and launching Nevada-based IT security service business
2. Nevada as home of one of the ten U.S. Cybersecurity teaching hospitals

I did review the recent Brookings report on economic development in Nevada. It is a bracing story. I think that is the right term. [Laughter] And, you are not alone. But is still a bracing story.

So, I was looking for things that would actually generate economic activity, not just things that would secure your systems and cost you a lot. It didn't seem that things that would do that would have legs. It might be a short term solution, but if it doesn't have an economic payback on a long-term basis, it probably won't get implemented well over the long term.

There are two ideas. One of them is really rapid improvement in State and local cyber security making Nevada a model. It is important that you do this first. I call this the Volvo idea.

Volvo was the first to have safe cars. People still think they are safe cars. I am not sure they are safe at all. But "no one has ever died in a Volvo crash in California." Who knows whether that is true? But the presumption is that they were first, they were safe. So, if you don't do this first, it probably won't play.

You do it first. Then you use the skills developed in implementing security across State agencies and local government – law enforcement and others. So you build a local industry that is then looked at by other States, asking, "Hey, can you help us?"

DRAFT

A lot of great things happen when someone finds a solution to a problem and demonstrates it works. Other people hear about it, ask how they can do it, and you make a business out of it. So, one idea is rapid improvement and making a business out of it.

The other idea is Nevada is home of one of the ten cyber teaching hospitals.

I'll give you some data about both of those ideas and then we can talk about them.

This is a top government-led, universal deployment, across State and local government, of the four controls the Australians found. This is doing in Nevada what Australia did across all of government.

You would do it across State and local government where they did it across their federal government.

You would do it with joint acquisition. So, if there are any tools you don't have that you need, you buy them together. So, the cost per city becomes hundreds instead of tens of thousands of dollars. The vendors will fall over themselves to be the one chosen. The economics of that kind of buy are really quite good.

Then, and it turns out it doesn't really take advanced talent for this stuff. This is middle talent. My sense is that you can build a community of people who know how to do this so you can provide a service to other people who want to do it – both commercial companies inside Nevada, but also other states and outside commercial companies. So, you can build a little industry around the implementation of these critical controls and then grow it to build more of them.

So, you take what the State Department did, you apply it to the four critical controls, and do it across all of Nevada – not with the purpose of just improving security here, but with the purpose of building up a talent team that would be offered to other states.

I don't think you would want to do it as the State of Nevada offering it to other states, but some entrepreneurial activity would generate revenues.

1. IT security business development while improving state/local security

- Opportunity: Top government-led universal deployment across state & local; joint acquisition; organic growth of talent (mid-level); IT security service business
 - Nevada's unique strengths
 - Small enough to do something state-wide (like Australia)
 - Top state leadership willing to act
 - Supporting legislation (TCAB)
 - Chris Ipsen and James Earl
 - Steady flow of "captive" business leads through the state

The reason I think you can pull this off is that you are small enough to do something state-wide. The United States could never pull off telling everybody to do anything. But Australia is small enough so that it can do something internally, together.

Number two is that you have senior leadership here who can spell "cyber security." You have people here who actually want to know about it.

You have supporting legislation that is really impressive. You have Chris and Jim who can make things happen.

The one thing that I think Nevada sometimes misses is that you have a steady flow of customers through here.

You do not have to exploit them. But, right now, you don't take the opportunity interact with them. I really didn't mean "exploit" them.

You have meetings in Las Vegas. We at SANS probably buy 12,000 room nights a year in Las Vegas – just SANS.

DRAFT

You have people flowing through Las Vegas who are interested in cyber security. They are interested in other things too, but they are very interested in cyber security.

If your leadership were to give a little welcome to us – “Welcome to Las Vegas. Welcome to Nevada. Let us tell you one cool thing we are doing...” You have customers just flowing through here, and they will ask, “How did you do this? How did you do that?” That is how you generate the interest and the revenue of the people you are building the business for.

It's like you have this pipeline of oil. And, you just tap it.

2. Nevada as home for one of the ten US “cyber teaching hospitals”

- The manpower challenge in cybersecurity
- The colleges and community colleges as pipeline
- The US CyberChallenge
- The teaching hospital concept
- A teaching hospital in Nevada

The other thought is more complicated. It's called a teaching hospital model. It is different from what most people think it is, so I am going to take a minute to put it in context.

I am going to show you the manpower challenge and show you why the colleges and community colleges are not working as a supply pipeline. They are completely failing the nation. Well, maybe not “completely” – maybe one half of one percent is not failing the nation.

Then I am going to show you the cyber challenge and why Nevada might be a good site for a teaching hospital.

What is their shared challenge?

Vice Admiral Bernard J. McCullough Maj. Gen. Richard Wolfson Major General Thomas A. Hammon Rear Admiral Robert S. Gray II

Lieutenant General Robert C. Schindler, Jr., Special Commander for U.S. Cyber Command General Keith B. Alexander, Commander, U.S. Cyber Command Janet Napolitano, Secretary of the Department of Homeland Security

These guys in the slide all have the same problem. The guy in the middle at the bottom is Keith Alexander who runs the cyber command. Janet Napolitano is in the lower right, the one-time governor of the southern wing of Nevada. [Laughter] She now runs homeland security.

The others run cyber security for the other military organizations. They all are saying that they need more people. And they mean it in thousands – “I need thousands of people.”

And when you translate this it does not just mean, “I need people who really know security.” They got people who “know” security coming out of their ears.

What they really mean is, “I need people who can do security. And do it at world class levels.” That we don't have anywhere. I am trying to differentiate between someone who has a degree in cyber security and can talk about it. And, maybe, can even tell you to buy a firewall. But, if you put them in front of an intrusion prevention detection monitor, they wouldn't have any idea what they were seeing. They can't spell “TCP” is the way we describe it.


We probably have 130,000 people who think of themselves as security people. Only a thousand or two are world-class technologists. We are actually in a huge mess.

General Alexander said this in June: “Our greatest challenge will be recruiting and training our cyber cadre to ensure we can sustain our ability to operate effectively...” So, this isn't just to secure a box. We have to be able to continue to operate even when the bad guys are inside the box. This is very challenging.

DRAFT

Gen. Alexander speaking at CSIS in June, 2010

- “One of our greatest challenges will be successfully recruiting, training and retaining our cyber cadre to ensure that we can sustain our ability to [redacted] cyberspace for the long term”



Here’s one of the ways to illustrate how important skills are. It comes from a congressional hearing. The chairman had the Commerce Department and the State Department both get up to testify about what happened when the Chinese broke into their agency IT systems.

You can understand why the State Department was a target. If you don’t understand why the Commerce Department was a target, it is because the Commerce Department manages the BIS Division⁴. This is the group that decides which technologies are too sensitive to export. They know every technology that we have that is too sensitive to export, who manufactures it, why it is too sensitive – every piece of data you would want if you were a spy. And they have it already collected in one place.

Setting the Stage

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
April 27, 2009
Chairman: Jim Langevin
“We don’t know who’s inside our networks. We don’t know what information has been stolen. We need to get serious about this threat to our national security.”

- State Dept witness: Don Reid, Senior Coordinator for Security Infrastructure
- Commerce Dept witness: Dave Jarrell, Manager, Critical Infrastructure Protection Program

That was what was taken. Although they swear it wasn’t. Well, they swear they have no evidence it was **actually** taken.

So, the Commerce Department got up and talked. And the State Department got up and talked.

Dave Jarrell from Commerce said, essentially, “We have no idea when they got in. We have no idea how they got in. We have no idea where the malware spread. It took us 8 days to put a filter in and it was an ineffective filter.” Actually, he didn’t testify it was an ineffective filter. He named the filter, and it is widely known to be ineffective. He went on: “We were unable to clean the systems. We were forced to replace them.”

A Tale of Two Departments

Commerce Department	State Department
<ol style="list-style-type: none">1. No idea when it got in, how it got in, or where it spread2. Took 8 days to filter (ineffective)3. Unable to clean the systems; forced to replace them4. Do not know whether they have found or gotten rid of the infections	<ol style="list-style-type: none">1. Detected it immediately2. Put effective filter in place within 24 hours; shared filter with other agencies3. Found two zero-days4. Helped Microsoft and AV companies create patches and signatures5. Cleaned infected systems, confident all had been found

Then one of the committee members asked, “Well, do you know whether you got rid of the malware?”

And Mr. Jarrell said, “No.” End of testimony.

The State Department guy, Don Reid, gets up, and he says, “We detected this one immediately.

We don’t get them all, but we got this one immediately. We put effective filters in place right away. We found two zero days.”

Now, a “zero day” is a vulnerability that has not been reported to the vendor, so there can be no patch to fix it. “Zero” means, how many days since the patch was issue – the answer is there is no patch, so there have been zero days since the patch was issued. So, even if you are good and you patch your systems as soon as they are issued, you would still be vulnerable to a “zero day” attack. The holy grail of an attacker is to be able to launch a “zero day” attack – something which exploits a vulnerability before anyone even knows the vulnerability exists.

⁴ Bureau of Industry and Security, the division within the Department of Commerce responsible for developing export control policies, issuing export licenses, and dealing with violations.

DRAFT

Two of the defenses the Australians put into their system are actually defenses against zero days – that work.

Then the State Department helped Microsoft and the anti-virus companies create patches, they cleaned their systems, and they are confident they got rid of all the malware.

A year and a half later, Jim Langevin, the Chairman of that committee asked Jim Lewis at the Center for Strategic and International Studies (CSIS), to find out what the difference was. What were the tools that the State Department had that the Commerce Department didn't have.

What enabled State to perform so much better than Commerce?

- Was it tools? No
 - Almost the same commercial tools – Commerce actually had more expensive and newer commercial IPS/IDS
- Was it skills? Yes
 - Commerce – staff's only experience was firewall operations not even firewall engineering. No training other than Security+ and CISSP. Managers were policy and compliance people - no hands-on security skills.
 - State – staff had experience and training in forensics, vulnerabilities and exploits, deep packet inspection, log analysis, script development, secure coding, wireless, Windows, Linux, and reverse software engineering. Plus counter intelligence. And managers with strong technical security skills. (Notice the MIX of skills – remind you of anything?)

CSIS sent in the best people we have in the country in this area, Karen Evans, who was the CIO of the entire government, Frank Reid, who wrote the computer security act and the computer privacy act. These are good people.

And they reported back. Not only were the tools the same, but that Commerce actually had better tools.

So, the difference turned not on the tools, but all the skills that were brought to bear.

This is the first time we really had hard data showing that the tools were not the distinguishing factor.

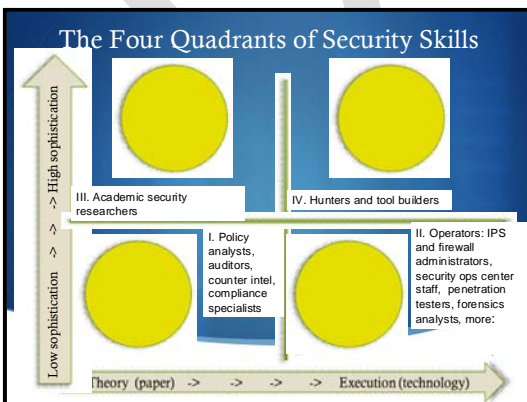
You think, "I'm going to buy something. And it is going to fix the problem." But it isn't going to. Because the bad guys buy the same thing you are buying and they program around it.

So, how good are you really, if you buy everything? Well, you're still dead.

What is important is the skills to do the analysis. And the types of skills are on this slide in the last bullet: deep forensics, vulnerabilities and exploits, deep packet inspection, log analysis, script development, secure coding, wireless, Windows, Linux, and reverse software engineering, plus counter intel, and managers who can do this stuff.

There is a mix of skills here. The military is thinking about this now as more of a Special Forces team – where you have some of each discipline and you deploy them as teams. The shooter isn't the explosives person, but the shooter can do explosives if he needs to. In short, you have

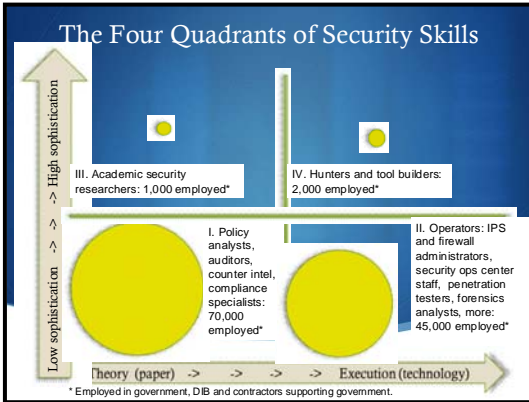
multiple talents that are cross trained. It is not, "Let's hire a security person." You have people who are specialized and then cross trained to work together.



This was the most sought after set of charts at the last NSA/DISA information assurance meeting because it explains the demand for skills. There are four categories on display here. We are going to leave out academics for a minute.

Look at the lower left. It deals with policy analysts, the auditors, the counter intel, and the compliance people. The lower right is all the people you think of as security people – intrusion prevention, firewalls, security ops folks, penetration testers, forensics – all the people that do this sort of thing.

DRAFT



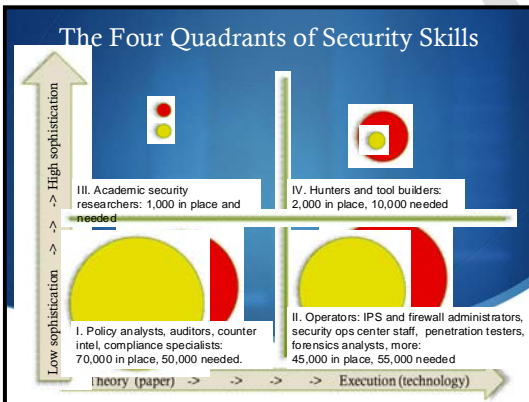
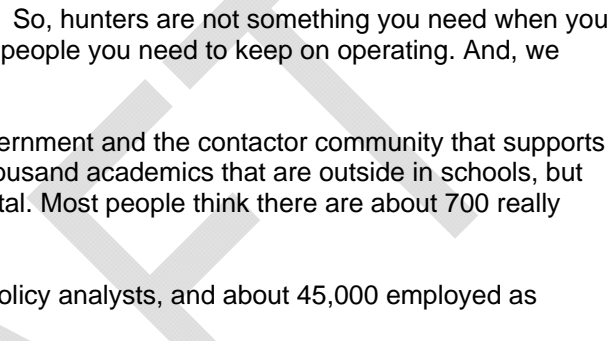
In the upper right are the hunters. The hunters are the people who go and find the stuff that is already inside.

Today we have no ability to keep the bad guys out. I can prove that if you want to ask me about that. But, if you have a truly important place, you can not prevent bad guys from getting into that important place. So, being able to find them fast after they get in, and get rid of them fast, becomes everything when it comes to keeping things operational. Does this make sense?

So, hunters are not something you need when you find out you have been attacked. Hunters are people you need to keep on operating. And, we have almost none of these people.

These are the numbers within the federal government and the contactor community that supports the federal government. There are about a thousand academics that are outside in schools, but there are only about two thousand hunters, total. Most people think there are about 700 really good ones.

We have about 70,000 people employed as policy analysts, and about 45,000 employed as security technical people.



What is fascinating – and this is the chart everybody wanted – is this next chart addressing “What do we need?” This need is across the federal government, across DOD, and across the country.

The answer is that we need a lot fewer of the folks in the lower left. We have way too many people who can write about security but can’t do it.

What we need is people who can actually do security. And, what we need even more are people who can do security at world class levels.

We need to move people from left to right across the bottom, and then from the upper right up into the upper right quadrant – all the way to the very top.

That is what survival means in the next war.

Not only that. It is economic survival for any nation that wants to keep its intellectual property over time.

If a country tries to protect itself with people who write about security instead of protecting itself with people who can actually defend at a world class level, then that country really does not have much chance of survival.


Do other nations notice this? Do they care?

DRAFT

This is a guy named Tan Wei Lin (Dailin). He was a graduate student at Sichuan University in 2005 when he got caught hacking into a Japanese computer. He called it “patriotic hacking”. The People’s Liberation Army (PLA) called it a capital offense. Hacking is a capital offense in China.

Why these skills matter

- ◆ Key weapons in the next war will be people with advanced, technical cyber security skill
- ◆ Wicked Rose →



So, when the PLA offered him an “opportunity” to enter a competition, instead of the alternative, he accepted – as did everyone else the PLA caught.

Every spring, in every PLA district in China, the PLA runs a competition. They bring in people who they think are good, or people who they caught being really good hackers, and they engage in competition.

This young man’s team won in the Cheng Du district. The PLA then put him in a 30-day, 16-hour a day computer network exploits class to teach him everything they knew. And he went and asked

why. The answer is that they were getting beat by the other PLA teams in southwest China, and they were tired of getting beaten.

So, they had this creative hacker and they were going to make him as good as they could. He actually won the entire southwest China competition.

And then, he dropped off the map. You couldn’t find him anymore. That was in September 2005.

In December 2005, the Secretary of Defense had his desk computer attacked. You remember the stories about that? Tan Wei Lin’s signature is all over that attack. We can not prove he was the individual, but the summer of 2006 was the summer of the zero day, and his team was responsible for 5 of the 31 zero day attacks. Remember the holy grail of attacks? That is what we mean by world class.

In China, we have a county that is searching for world class players all across its territory – every spring – in every PLA district. This is a whole nation doing the search. And China has been doing it for 8 or 10 years. Thousands and thousands and thousands are being screened through this annual competition.

And, what are we doing?

Well, we have colleges. We are teaching students how to write about security. But we are not teaching them how to attack and defend.

The U. S. CyberChallenge

- STEP 1
 - Forensics Challenge (DoD Cyber Crime Center)
 - CyberPatriot Defense Competition (Air Force Assoc.)
 - NetWars Challenge (SANS)
 - The Treasure Hunt
 - Security Foundations
- STEP 2
 - Cyber Camps
 - Courses and exercises
 - Tournaments
- STEP 3
 - Internships
 - Scholarships
- STEP 4
 - Moving into technical cybersecurity positions in important organizations

Melissa Hathaway started the U.S. Cyber Challenge when she was in the White House. I helped fund the first part of it. Karen Evans, the person who ran all computing for the federal government for the last six years actually runs it.

She was actually the first cyber victim. She was running the computers at the Department of Justice back when Janice Reno’s picture was changed to Adolf Hitler, and it was called the Department of Injustice. She had to drive in from her house in West Virginia to unplug all the machines. So, she was the first one to learn how bad it was to be hacked. This was in 1997 or

DRAFT

thereabouts.

She was really happy about 5 weeks later when the CIA got hit. The Washington Post had this wonderful article about the CIA attack, and the last paragraph said, "This was the second hacking incident. The first hacking was at the Justice Department."

So, when you are first, you never stop being first – whether for good or bad.

The US Cyber Challenge has wonderful competitions, some two thousand high school kids engaged, about a thousand college kids engaged. It is searching for the same thing as the Chinese.

But it hasn't caught fire yet. Those numbers should be 20,000 each – at both the high school and college level. Figure maybe within another year and a half.

The U.S. is a very competitive place. The kids who do well get invited to summer camps. They get to enter big tournaments. They get internships. They get scholarships. The Chief of Naval Operations gave me four full four-year scholarships for the kids who really do well – everything paid. The idea is to move them into technical jobs.

That is the U.S. response. It is not perfect, but I wanted to bring it up.

We know it is working on a small scale. I interviewed one of the kids identified in the cyber challenge at a conference.

I asked him, "You are a senior in high school, have you already taken computer courses?"

He said, "I took graphic design. I took web design, and computer network repair, but when I tried to take programming, there was no teacher."

So, if the U.S. were looking for "Johnny", how would it find him? It couldn't – not even when he raises his hand and volunteers. That's why the competition is a good idea. The competition doesn't rely on teachers to know anything. Teachers can't do good hacking anyway, so they don't know whether a problem kid is really just a bad kid or is the next cyber warrior⁵.

I asked him, "How do you demonstrate your skills if you don't have an opportunity to play?"

He said, "Well, most people just target random servers and hack illegally. So, it's great that I came across Net Wars.⁶" That's a federal felony, right?

My friend Sean Henry, who has now moved to a position as assistant director of the FBI for its cyber and criminal divisions, did a video for us. We call it "Ethics". Its effective argument is what life is like in federal prison. It is a really good ethical tale.

Then, the kid was asked, "Do you have a specific employer in mind?" He wants to work for the government. The competitors would like to be valuable.

The idea of searching for talent, finding it, nurturing it, and moving it into jobs is really a good idea.

You might ask, 'Why aren't the schools doing this?' The answer is in the Tulsa story.

⁵ See, *Ender's Game*, a science fiction novel by Orson Scott Card published in 1994.

⁶ The sanctioned competition.

DRAFT

Lots of colleges have security programs. There are 200 that are centers of academic excellence. One of those two hundred – remember earlier I spoke about half a percent of colleges not failing? – this is where I got that number. One of those two hundred has put more people into the NSA and the CIA in important jobs than all of the other 199 together.

Why? And the NSA and CIA guys fight over these people.

The reason is that at Tulsa, the kids work on real projects. They have a Secret Service lab on campus. They have a state police lab on campus. And, they get tasks from the NSA. The kids come out of college with security clearances.

Why Do We Need Cybersecurity Teaching Hospitals?

- ♦ Tulsa story
- ♦ Preparing physicians
- ♦ Teaching hospitals are NOT medical schools – they are hospitals with real patients and top medical talent

SANS

That is what a teaching hospital is. That is what I have been getting to.

A teaching hospital is not a school. It can be a school and a teaching hospital, but the teaching hospital part involves working on real projects under the direction of somebody who knows how to do them. When you come out, you have enough experience so the person who hires you is confident of your skills.

My youngest child is a doctor. I have lived with this. She gets out of medical school and has been

on one rotation for cardiology or maybe two, then one or two in oncology. That is a dangerous person to put out as a doctor. So, what do you do with a doctor? You put them in teaching hospitals where they actually work as interns and residents. She worked 90 hours a week. I mean literally 90 hours a week. It was 90 plus all the extra stuff they made her do. She did this for four years. That is something like 16,000 hours. Now she's pretty good at this stuff. But the difference between none and 16,000 is a big deal.

We have people coming out of college and university in security with no hands-on experience. We expect employers to do all of the training.

That's just crazy. The teaching idea involves identifying a place where you can take real cases – that's what Tulsa has, right? They have a real Secret Service lab, a real state police lab, real NSA projects. We need to build ten of these around the country. The people who go in are people who have already learned about security. They are not just going to classes, they are doing real projects under supervision.

Over time, the layering that we have in medicine, where we differentiate between interns and residents and fellows and attending physicians, may take hold. These locations are not just holding pastures, they become destinations, where, in this state, the gaming industry could come and get research done for new on-line gaming. The mining and critical infrastructure people could come for research in their areas, but they could also get services, because that is what a teaching hospital provides.

Don't think of a teaching hospital as a college or a collegiate program. It is actually a hospital where people learn. It is not a school where people learn. It is a hospital that does real work and real research where people also learn.

Now, why should a teaching hospital be located in Nevada?

You can get access to real cases better than other people.

DRAFT

The difficulty about cyber security cases is that there are a lot of privacy issues associated with getting the data. If you don't have cover from the top, you can't get access to the data, so people in the teaching hospital can't work on it.

You could actually contract with the teaching hospital to do your research and have all the clearances needed. You can do this in a small state.

Key Nevada strengths for creating teaching hospital

- State government and college-based "case" material available (Chris Ipsen)
- Hal Berghel – one of the very few people who have proven this idea works
- Nellis AFB
- Center of Academic Excellence at UNLV
- Continuing flow of "cameo" lecture opportunities and potential candidates
- Possible partnership with SANS and the US CyberChallenge

Second, you have a guy named Hal Berghel, who is the newest member of this Board, who is the only person, other than the folks in Tulsa, who has actually done this.

Hal actually built a program working with the gaming community and some of the folks in Washington. His students had real projects and came out great.

But something killed that program a couple of years ago, I think. The university killed it, because it didn't fit their university model. But you have one of those people in the State.

You also have Nellis Air Force Base. Nellis has the coolest attack guys in the Air Force. They don't raise their hands and say, "Hi. We're the coolest." But they are.

The balance of these two capabilities is really cool.

You already had a center of academic excellence at UNLV.

You have this flow of people coming to computer and computer security conferences. You could tap those people as lecturers. All these teaching hospitals have lectures from visiting specialists in the newest techniques in prostate cancer. You have all these computer folks coming through who could add value to the teaching hospital idea.

Discussion

- Australian Sweet Spot
- U.S. State Department Security Automation
- U.S. Air Force CyberFlight Simulator
- Opportunity 1: Building an IT cybersecurity business in Nevada around continuous monitoring
- Opportunity 2: Locating one of first cybersecurity teaching hospitals in Nevada.

And, you have a potential partnership with SANS. We are more willing to help if we can.

Here are the things I talked about on a summary slide: the Australian sweet spot, the State Department security automation program, the Air Force simulator, and two business opportunities I see for Nevada.

I will be happy to answer questions from anyone who might have them.

AG CORTEZ MASTO:

Mr. Paller, thank you very much. Let me open it up to the Board Members.

MR. UFFELMAN:

If I may? Steve Hill is going around trying to figure out how to move economic development. This is economic development in so many ways, but also at relatively low cost. Taking the time to give him this briefing might be helpful if he hasn't already seen it.

DRAFT

AG CORTEZ MASTO:

Thank you. That is a good point. Anyone else?

MR. IPSEN:

I certainly have a number of questions and comments.

First of all, I want to thank you, Alan, for coming out. I always want to take the opportunity to recognize those people who are uniquely important to our success story, the Nevada Experience.

When I think of Alan, I think of the quintessential person who represents the private sector civil servant. And, I use the term "civil servant" as the highest regard for people. Thank you for being here. I just wanted to say that in our venue, usually it is in your venue.

There are a couple of questions dealing with challenges that we have going forward. One of those is in conceptualizing the entire State. I'd love to say, "We are going to be the first state to do that." It requires leadership and it requires that we all work together.

Could you speak to two areas? First, is to leadership, which you already mentioned. And, second, how successful could we possibly be without working together collaboratively in a common enterprise approach?

MR. PALLER:

Well, you are not going to like my answer.

Chris, I don't think that leadership is top down. And I don't think leadership is pulling a lot of people together.

Leadership is going in some direction, looking behind you, and finding a whole lot of people following you.

My sense is that you already have enough money to do this on whatever scale you can do it on.

Go do it. Show people those charts. Have the people who run the other agencies ask, "Why don't we have that?" Show leadership.

The meetings will take you the rest of your life.

There is a great line from the former deputy assistant secretary saying, "I think I have attended this meeting before."

They just go on and on. So, I think leadership, now, is, well, you.

You're not going to ask me anymore after that, are you?

MR. IPSEN:

I feel properly challenged here. I will go forth and conquer.

MR. PALLER:

I will help.

AG CORTEZ MASTO:

Anyone else? Any other comments.

MR. EARL:

One of the things Mr. Paller mentioned early on – and I won't get this exactly right – he characterized the Department of Energy National Labs as being one of the best residual places to

DRAFT

find cyber defense and cyber forensic information. Board Members may recall we have seen an example of the work of one of the nearby national labs, Idaho National Labs. In Mr. Elste's presentation of last meeting on Stuxnet, you saw a very large generator essentially blow up as the result of a cyber attack. That took place at Idaho National Labs.

Within the last two months, staff at the Idaho National Labs have reached out to the CIOs and CISOs in western states, including here in Nevada, to foster the beginnings of an information sharing process that would draw on the expertise of the national laboratories. This is still in a very formative stage.

They have now circulated a draft MOU, which, surprisingly, looks an awful lot like the MOU signed by various agencies represented here to put together the State of Nevada Task Forces. I have no idea how that occurred. [Laughter] But I do want to let you know that Mr. Paller's suggestion that we at least be aware that national laboratories are important sources of information is, in fact, underway, in a consortium of western states that includes our own, although at a very early, formative stage.

AG CORTEZ MASTO:

Thank you. Any other questions or comments for Mr. Paller?

I think you have properly stunned us and challenged us. I echo what Chris just said. I am properly challenged. I think the information you have provided was not only very informative, but most important.

As you pointed out, we in Nevada are challenged economically, and there is an opportunity to blend the two components you talked about, expertise and skills in cyber safety with economic development. That has given me pause to think about where we go from here.

I thank you very much. It was important to have you here. I thank you for taking the time to fly here. I am hoping this is just the start of a relationship with you involving our State, our Board, and many of the folks here in Nevada. I can't thank you enough for being here.

MR. PALLER:

You are welcome.

AG CORTEZ MASTO:

Thank you very much, Mr. Paller.

Agenda Item 8 – Report by Ira Victor, a digital forensic and information security analyst, on the Mission of the Computer 4 Kids Program – educating low-income Nevada students on security, privacy, and good digital hygiene.

AG CORTEZ MASTO:

The next agenda item is a report from Ira Victor, a digital forensic and information security analyst on the mission of the Computer 4 Kids Program, which is educating low-income Nevada students on security, privacy, and good digital hygiene.

Welcome back, Mr. Victor. It is good to see you.

MR. VICTOR:

Thank you, Madam Chair.

I am an analyst with Data Clone Labs, here as a private citizen.

DRAFT

I am also a graduate of many SANS courses. I thoroughly enjoyed the previous presentation. Many of the things you will hear me talk about are traceable to the great training and the certifications I have received from SANS.

I am also president of the InfraGard chapter for northern Nevada. That was one of the inspirations for me to work on the program I am about to tell you about.

I am one of the founding members of one of the Lions Clubs here in Reno, Nevada. It is called the Reno Cigar Lions Club because there is a group of geeks in northern Nevada that enjoys fine cigars. I do not smoke, but I enjoy the company of the people who attend these events.

We put together the Computers 4 Kids Program. We discovered a few years ago that there was a tremendous number of old computers that were either being discarded or were being recycled by centers that were putting Windows XP on these old computers.

As information security and computer forensics people and people who cared about computer recipients, we were in shock and horror at the idea of giving people Windows XP computers fraught with all the security nightmares that Windows XP was famous for then, and is even worse now.

We decided to create a program where we would gather older PCs that would not run the newer Windows 7 operating system, or even Windows Vista, because they were not powerful enough, and install a desktop Linux operating system instead. We would then give the computers away for free to lower income children in Nevada, and teach the kids the basics of computer security and digital security hygiene. We thought that by combining the flexibility of Linux and its enhanced security with teaching the kids to use it effectively, we would empower a generation of young people who had far more computer skills than their wealthier peers, who had Microsoft Windows computers.

Now, I am not here to bash Windows-based computers. I use the application, that operating system and the applications. However, when you give or buy a young person either a Windows or Mac-based PC, there is an enormous amount of money that the student or family has to spend to buy applications in order to do things.

For example, a lot of young people like to do video gaming and create their own video games. The programs to do that on Windows or Mac machines cost thousands of dollars. Similarly, if they want to learn about security, there are a lot of security tools available that run on Windows, yet they cost hundreds to thousands of dollars to buy. Even wealthier parents have difficulty justifying that, let alone parents who are surviving paycheck to paycheck.

We give students free computers installed with a Linux operating system. It is free to us and free to them. There are tens of thousands of programs that are available to run on a Linux operating system. We even created our own customized version of Linux that we install on our computers. That is what I am using now. This would cost thousands of dollars to buy on a proprietary platform, but it is free on Linux. They can use this to create their own video games.

We show our students some of the video games and animations that were created with this program. Their jaws drop. We say to them, "In today's class, you will be learning about security. But we are also giving you something that is very fun to do. You can create animation and games with this computer, just like what we are showing you now." This clicks with young people. They see that we are giving them an incredible tool.

We have now done this for a number of years. We have impacted about 2,000 people in northern Nevada with these systems. We operate on a 100% volunteer basis. We receive no funding outside that we raise on our own. We created a special search engine we call Lionssearch.org.

DRAFT

We get a percentage of the resulting search dollars to buy parts and do fundraising events. It is completely volunteer.

The most amazing experience I had followed one of the training sessions. I helped a little girl, probably about 8 years old. She attended with her single mom and her two siblings, one a little older, and one quite a bit younger. This middle child was very attentive to all the things we were teaching. She asked a lot of questions, and I tried to make sure I answered all her questions. I showed her a lot about what we were doing.

She sent us a thank you note several weeks later. She thanked us for the computer we gave her. We install software that is similar to the Microsoft Office Suite on these computers. It is called Libre Office. It contains software that functions similar to Excel, Word, and PowerPoint.

This young lady taught herself how to use the spreadsheet application in Libre Office. Her mother works as a cleaning lady. The girl put all her mother's financial books into this Linux-based spreadsheet application, and was writing to thank us for giving her the computer so she could do this.

So, here's a young girl who now knows how to use Linux. Recall that one of Mr. Paller's slides identified Linux as a key operating system. She now knows how to use Linux-based spreadsheets.

Who do you think will be a more valuable asset to Nevada as an employee 10 or 15 years from now? That is what we want to affect with this program.

There are similar stories regarding students getting interested in security and forensics. Data Clone Labs has its first forensics intern, a high school student from Hug. She is interning with us. We are teaching her Linux forensics. She came to the program specifically to learn computer forensics.

Again, we are the Computers 4 Kids Program of the Reno Cigar Lions Club. We believe we have a very large market share in Nevada. We think we are the only ones doing this. But we don't have a lot of mind share. It is all through word of mouth that people know of our activities.

Part of my objective today is to let a wider audience know about what we are doing. I was very pleased to see Mr. Paller's presentation. We can assist in being that feeder organization to bring students into a teaching hospital environment or whatever program develops.

I would encourage anyone who would like to contact me regarding this program, to spread the word and spread the program to do so. I can be reached at security@iravictor.net. I will be glad to respond to any questions either now or by email.

AG CORTEZ MASTO:

Thank you, Ira. Are there any questions from Board Members?

MR. EARL:

Not everybody in the State knows this, perhaps not even a number of legislators. The Legislative Counsel Bureau has for probably the last 10 or 15 years run an internal recycling program whereby when new computers are purchased by LCB, they replace one generation of older computers, which are then moved down to other uses. The individual here at LCB who manages that program, at the end of the day, ends up with a lot of older computers. But he knows how much time is on them and so on and so forth. LCB has had a program for 10 or 15 years to place those used, but still very serviceable computers, into the community in a variety of different ways. This has evolved so it is very sophisticated in terms of the order of groups they try to place computers with.

DRAFT

I wondered if you could give us some idea of the type of computer you are looking for right now. What would be useful to you?

MR. VICTOR:

That is an excellent question, Mr. Earl.

The reason my computer took a little bit longer to boot up is that I am using a computer that has just about the minimum power we need to operate our computers. The beauty of Linux, and I won't get into the technical explanation, is that certain versions especially, are highly efficient. So, this computer is equivalent in power to a business PC of about 8 years ago. You could never run current operating systems on it – operating systems such as Microsoft Windows 7 to support Microsoft Office. You could never run current versions of those applications on old computers. But their counterparts will run just fine on most versions of Linux – especially the version we are using.

So, we can take computers as old as 10 years old, as long as they still run, and transform them to give to kids. This is what we do. Some of them come from businesses, both public and private sector. We can take these old computers, make them fully functional so that they can still do the same kind of work that their peers are doing on more modern, more expensive computers. They will not be hindered by using what would otherwise be considered an ancient, old, underpowered computer. We use our version of desktop Linux to restore their functionality.

SENATOR WIENER:

Madam Chair. Ira, have you reached out to similar Lions Clubs here in the south to see if we could move in this direction in the southern part of the State?

MR. VICTOR:

Thank you for the question, Senator Wiener. There is an awareness, around the world actually, about what we are doing.

This is sort of a two-edged sword. The excitement in the Lions Club International, which is over 100 years old, at the senior management level is, "Wow, this is a program that can lower the age demographics of the Lions organization." As many people are aware, Lions Clubs evoke the image of octogenarians. Let's put it on the table. The average age is much older than I am, and I am not a young kid. But I seem like a young kid when I go to a big Lions meeting.

So, there is excitement at the international level because we can attract young people to a Lions Club event.

The other edge of the sword is that when we go to make a presentation at a Lions International meeting and I pull out this computer and show this demo, the audience has no idea what I am talking about.

I think we need to expand outside of the Lions with this program, and then use the structure we have already involved in Lions. We need to attract people who are already interested in computers and information technology to help expand the program further because we do not find a lot of those people within Lions Clubs as they exist today.

Does that answer your question, Senator?

AG CORTEZ MASTO:

Thank you, Ira. Are there any more questions for Mr. Victor? Comments? Thank you very much for what you are doing. The fact that the Lions Club in northern Nevada is working with kids in this way to really have an impact in low income areas is really fantastic. If there is anything we can do to assist you, or get the word out about your program on how people can support what you are doing, please let us know.

DRAFT

MR. VICTOR:
Thank you, Madam Chair.

Agenda Item 9 – Public Comments.

AG CORTEZ MASTO:
This is the time for public comment. Is there anyone in northern Nevada who would like to address the Board at this time? Will you please come forward and state your name.

MR. HOMEYER:
My name is Jack Homeyer. I work with Ira Victor on the Computer 4 Kids and InfraGard programs and various other things.

I just wanted to say that this Saturday, we will be giving away 50 computers at the KNPB studios in Reno. I believe the Boys and Girls Clubs of Northern Nevada will be there.

If anyone would like to see what we do in the program, you are welcome to drop by, have a cup of coffee and see the excitement of the kids as they get their computers.

AG CORTEZ MASTO:
What time will you be there?

MR. HOMEYER:
From 9 to 3.

AG CORTEZ MASTO:
Okay. Thank you very much.

Are there any other members of the public who want to come forward here in northern Nevada?

Seeing none, are there any members of the public in southern Nevada who want to address the Board?

SENATOR WIENER:
Yes, Madam Chair.

AG CORTEZ MASTO:
If you would please come forward and state your name for the record? Thank you.

MS. FUCCI:
My name is Laura Fucci. I am the Chief Information Officer for Clark County, Nevada. I have served in that capacity for the last 5 years.

Prior to that, I was the Chief Technology Officer for MGM Mirage. I worked there for 11 years. I mention that just to highlight how long I have been in the IT community in the State of Nevada.

I wanted to take this opportunity to express my support for the programs that Mr. Paller recommended – specifically some sort of teaching hospital for cyber security.

I have had the privilege of working with Doctor Berghel on the School of Informatics over the last 10 years, since he first formulated the idea.

DRAFT

I think his school was the closest thing we have had to a teaching hospital for cyber security. It was wildly successful, in my opinion, until its recent cancellation by University of Nevada, Las Vegas.

That program is a combination of the business community with academia to formulate the curriculum that is needed by the business community.

It is also the only Nevada institution to become an NSA national center of academic excellence in information assurance education. It has been recognized by both NSA and the Department of Homeland Security.

Built within the program itself is a requirement for interns. So, students, as they went through the program, were required to work in all of our work environments – either in different casinos or in government agencies. We were able to get people who were hands-on, who had actually worked on projects, as Mr. Paller has recommended.

I hope we can take some of those components that were so successful in the School of Informatics and build a successful teaching hospital for cyber security.

I heard Chris Ipsen say he was going to be our leader, [Laughter] but I am right there with you, Chris.

I also want to express my enthusiasm for the program Mr. Cary spoke about – the program we were awarded as the State of Nevada. One of the things about that program is that it does not just speak to the choir. I am the choir when it comes to cyber security. Cyber security is something we all need to engage in and participate with. We need people who do not understand it to understand their part in making a safe and secure cyber space. That program will, hopefully, get us there, and we will educate people who are not aware. I am excited to participate in that.

I also want to express my appreciation to this committee for making all this stuff happen and bringing these people here so we can hear more about the subject. Thank you.

AG CORTEZ MASTO:

Ms. Fucci, thank you very much for your comments.

Is there anyone in southern Nevada who would like to address the Board? Seeing none, we will move on to item number 10.

Agenda Item 10 – Board Comments.

AG CORTEZ MASTO:

Now is the time for any member of the Board who would like to comment. If no one is doing so, I would like to mention something.

We have the opportunity, as Ms. Fucci said, to bring in some fantastic speakers, as we have heard today, to really support Nevada and help us identify where we need to go with cyber security in this state.

We have some fantastic partners – state, local, and federal partners. I can not thank you enough.

I want to highlight one speaker we had in the past. If you recall, Mark Weatherford spoke to the Board on behalf of NERC regarding cyber security in the electric grid.

DRAFT

You might be interested to know that he just accepted a position with the Department of Homeland Security. Thanksgiving week, he assumed the duties of the Deputy Undersecretary for Cyber Security. This is the top position dedicated to information security.

We expect that he will have some influence over the DHS grant process for cyber security in the future.

His presentation to our Board was his last policy presentation before joining DHS. That gives you an example of some of the folks we have had the opportunity to meet, engage with, and learn from.

I want to thank all of you for your support of what we do. We are not done yet. There is a lot to accomplish. We will continue to do so with not only the Board Members here but with people in the public who are so engaged and find this to be such an important topic. And, more importantly, cyber security is an area where we need to keep taking action.

Agenda Item 11 – Scheduling future meetings.

AG CORTEZ MASTO:

I believe our next agenda item is scheduling of future meetings. Mr. Earl

MR. EARL:

After New Year, when people have returned, I will be in contact with Board Members or their offices to schedule future meetings.

I would also like to issue a plea for assistance in advance planning. Those of us who have been involved in the legislative process here in Nevada will be aware that it is beginning all over again very shortly.

Executive Branch agencies will be beginning to look at Bill Draft Requests (BDRs) as early as the late spring and early summer.

I would like to hear from Board Members regarding any possible legislative needs that should be addressed, or that the Board can assist in, during the next Legislative cycle.

I know that the Chief Information Officer of the State has indicated there may be some additional modifications that need to be made to his statute. I would encourage other Board Members if there are similar concerns, either in law enforcement or any other area that deals with the vast subject matter breadth the Board is empowered handle, to please let me know. We can then line up appropriate back ground presenters to establish a solid base for any future legislation.

So, when I contact your offices in early January, if there is something you would like to pass on to me at that time, I would certainly appreciate it. Thank you.

AG CORTEZ MASTO:

Thank you, Mr. Earl.

DRAFT

Agenda Item 12 – Adjournment.

AG CORTEZ MASTO:

The next item is adjournment. I will entertain a motion for adjournment.

The Board voted unanimously to adjourn at 12:15 PM.

Respectfully submitted, (subject to approval at the next Board meeting)

James D. Earl
Executive Director

Approved by the Board at its subsequent meeting on [date]