

**\*\*\* NOTICE OF PUBLIC MEETING \*\*\***

**INFORMATION TECHNOLOGY ADVISORY BOARD**

---

**LOCATIONS:**

Legislative Counsel Bureau	Grant Sawyer Building
401 S. Carson Street	555 E. Washington Avenue
Room 2134	Room 4412
Carson City, Nevada 89701	Las Vegas, Nevada 89101

If you cannot attend the meeting, you can listen to it live over the internet. The address for the legislative websites is <http://www.leg.state.nv.us>. Click on the link "Live Meetings"- Listen or View.

**DATE AND TIME: May 19, 2014, 1:00 p.m.**

---

Below is an agenda of all items to be considered. Items on the agenda may be taken out of the order presented, items may be combined for consideration by the public body; and items may be pulled or removed from the agenda at any time at the discretion of the Chairperson.

---

**AGENDA**

**1. CALL TO ORDER (For possible action)**

**Joe Marcella:** 2014, Information Technology Advisory Board, ITAB, meeting to order.

**2. ROLL CALL (For possible action)**

**Joe Marcella:** Lynda, can I have a roll call?

**Lynda Bashor:** Assemblyman Anderson?

No response heard.

**Lynda Bashor:** Mr. Capiral?

No response heard.

**Lynda Bashor:** Senator Denis?

**Senator Mo Denis:** Here.

**Lynda Bashor:** Mr. Farrell?

**Kevin Farrell:** Here.

**Lynda Bashor:** Ms. Fucci?

No response heard.

**Lynda Bashor:** Mr. Malfabon?

**Rudy Malfabon:** Here.

**Lynda Bashor:** Did I say it correct? Mr. Marcella?

**Joe Marcella:** Here.

**Lynda Bashor:** Ms. Schmidt?

No response heard.

**Lynda Bashor:** Ms. Teska?

No response heard.

**Lynda Bashor:** Mr. Willden?

**Mike Willden:** Present.

**Lynda Bashor:** Mr. Chairman, we do not have a quorum.

**Joe Marcella:** Okay. Thank you. We'll continue with the meeting without a quorum. As soon as we have -- we're just missing one individual? Okay. So as soon as we do have a quorum, we'll -- I might even step back and get some of the voting out of the way.

### **3. PUBLIC COMMENTS**

**Joe Marcella:** So let me -- this is a public meeting and it's open for public comment. Anyone from the public have a comment? Hearing, seeing none. Anyone down south, in Las Vegas?

**Senator Mo Denis:** No, we have one person here, but he doesn't wish to comment at this time.

**Joe Marcella:** Thank you, Senator.

**Senator Mo Denis:** Maybe he'll hear something later on and feel like he really needs to.

**Joe Marcella:** Thank you, Senator Denis. We'll give him an opportunity at the end of the meeting. Thank you. Hearing none and seeing none.

### **4. APPROVAL OF MINUTES: January 27, 2014 (For possible action)**

**Joe Marcella:** Then I'd like to move on to the approval of the minutes. We'll skip the approval because we do not have a quorum, we cannot vote. But even though we cannot vote, is there any discussion on the minutes from the January 27<sup>th</sup> meeting? All right, let's move on.

### **5. DELOITTE CYBER RISK ASSESSMENT PRESENTATION (For possible action) presented by Deloitte Consulting**

**Joe Marcella:** We have the Deloitte folks with us today and they're here to provide -- making sure they're ready -- provide us with a risk assessment overview from a state and government perspective. Do I have that correct?

**Srini Subramanian:** Yes, you do.

**Joe Marcella:** Now, please proceed. Introduce yourself, let me know who's here, and then frame your conversation, please.

**Srini Subramanian:** Very good. Thank you very much. My Name is Srini Subramanian. I'm a principal from Deloitte's Cyber Risk Services. I also lead the state government practice for Deloitte's security and privacy, which we call a cyber risk services practice. So in my -- for the past 14 years or so, I've been working with various states governments and developing point of views on the impact of cyber security on state governments. And so today I wanted to share some of the thoughts as to what the evolving cyber threats that every one of us read in the news about and what is the impact of that to the -- with the state governments. And, specifically, that gives you some thought-provoking ideas in terms of what you can do in the State of Nevada to really protect yourself against cyber threats.

So maybe I'll just give a quick introduction in terms of the topic itself. We call it the imperative to become secure, vigilant, and resilient. So I'm going to talk in today's presentation about how for the many number of years we've always been professing and talking about let's protect our infrastructure, let's protect our data, and things of that kind. And now we are at a point -- the cyber threats have evolved to the point where it is not enough -- it's not adequate just to be secure. So we've got to have other measures to be vigilant, to be looking for ways and means of being able to detect and prevent the threats, as well as attacks, and to be resilient, to be able to respond and recover when the events do happen. Because one of the things that I'm going to talk today about is perfect security is impossible, so we've got to be able to respond and recover.

So why do state governments have to worry about cyber threats? One of the questions that is often asked is, well, state governments do not have money like the banks have. And so why would cyber criminals target state governments? Now, if you look at it, states collect enormous amounts of large volumes of comprehensive citizen information. Every state agency collects information right from the birth all the way to the death. And in terms of your financial information, tax information, driving records, student identifiers and student information, and increasingly more related to health records as well. Now, they are -- most of these records are distributed amongst multiple agencies. But still, compared to a private-sector organization, a bank or a financial institution may only have information about your finances. And whereas another agency may have only -- or another private corporation may have only information about your health records. Whereas state governments have the most comprehensive information and this is a good target for not only cyber criminals, but also hacktivists.

Now, what do we mean by them? There are really two types of threat actors. Ones who are perpetuating this crimes for money, for monetary purposes. So their purpose is to attack and gain information about credit card or PII, we call it, personally identifiable information, to get

monetary gains out of it. And there is other types of criminals who are called hacktivists. They are really trying to make a political statement. They are not really interested in money, but they are using very similar tools to make a political statement on a cause that they are after. And who to make a better statement than government organizations and government agencies? So both cyber criminals and hacktivists target state governments. Cyber criminals because they're able to get millions of records when a breach happens, and hacktivists because they're able to make political statements.

And in the last few years, this issue has gotten elevated to be one that is at the Governors' level. Two or three large state-based data breaches resulted in the governors needing to take action. And consequently, the National Governors Association has formulated a Cyber Security Policy Council to advise the states on what to do about cyber security.

Now, one of the things -- the State of Nevada is lucky to have some really advanced thinking leaders in this space. Governor Sandoval was in the NGA meeting in 2013 as the Vice Chairman of the Homeland Security Committee, actually kicking off the Cyber Security Policy Council for the state. And your CIO and the chief information security officer, CIO David Gustafson used to be the NASCIO co-chair for the Security and Privacy Subcommittee last year. And Chris Ipsen is known in the national circuit as someone that has been in the Chief Information Security Office role for a number of years. And we follow some of the initiatives; like there is a continuous monitoring initiative that the state is putting forward, advanced thinking in terms of not looking at just the state's infrastructure, but also looking at the county and city government infrastructure. So these are commendable and unique accomplishments and initiatives that the State of Nevada is looking at.

But with the trend of increasing threats, now what are some of the other things to consider? So, for example, the government uses technology and innovation to really improve citizen services. And comes along with that is a risk related to cyber, because the threat factors exploit the weaknesses of the technology and how they are implemented. Now, cyber threats are also asymmetrical threats or risks because a small and highly motivated group can cause quite a bit of damage. Now why do I say that? Because if you look at some of the most visible threats that happened or most visible attacks that resulted in a large amount of data loss, these were perpetuated by a very few people. And they are across the globe; you don't know where they are and how they attack. And they leverage a number of different weaknesses and all that it takes is one vulnerable point. And oftentimes it happens to be a user that clicks on an email link or provides their credentials to someone unknown.

And because of this, we are changing or we are coming up with the point of view that the perfect security is impossible, because the velocity with which the threats are evolving, every organization, private or public, is almost certainly going to suffer a breach at some point in time or other. So it doesn't mean that we cannot take the measures not to be secure. Absolutely, you have to do the due diligence, take a very risk-based approach, understand what the prime jewels are in the organization, which is the data that people may be after, and protect them. Those measures -- there is no deficiency. We cannot really do anything about them.

But in addition to being secure, being vigilant; implementing those continuous-monitor type processes, so that we are alerted when a threat has actually succeeded. And our experience shows, looking at some of the recent breaches, that most of the times the hackers have been in the environment for multiple days, if not weeks. So they were able to get into the environment and they are there looking at what is the data that might be of interest to them. And they are able to really look and get the data that they need, that is most advantageous to them. So having those alerts through the continuous-monitoring processes, that can really help surface and alert the organization of an ongoing threat that has succeeded, can still help mitigate the risk of large data loss.

And the last point is about being resilient. Now, considering that every organization is going to be breached at some point of time or other, there is always going to be an incident; how about having a strategy to respond and recover? And respond and recover in a way that it may not be business as usual, but you will at least have the strategies and processes to be able to do that.

And my last point is this is the IT Advisory Board, but this is as much as a business issue as it is an IT issue. It is a technology issue from the perspective that the preventive and securing measures are being implemented as technology measures, but it is really a business issue. Why do I say that? So whenever you look at a large breach, if it is a state government, right from the Governor's level or an agency director level, those are the ones at the forefront of leading a response, to be talking to the citizens about, and how do you go about and assure trust on the measures that the state government is taking? Next slide, please.

So how do you go about preparing yourself or preparing a state government agency? First thing is to really start analyzing who might attack. I talked about the cyber criminals and hacktivists, and looking at what is it they would be after. Like, for example, in addition to the cyber criminals and hacktivists, there are nation-state sponsored cyber terrorism. Some of you may have heard the news today about the Department of Justice going after -- with a cyber-espionage case against five people in China. Now, the nation-state sponsored type of activities, while a state government may not have intellectual property that some of these cyber nation-state criminals are after, states do have a good bit of critical infrastructure that could come under attack, like your transportation systems or your utility systems and so forth.

So really having an understanding as to who might be interested in what is a first step in really looking at an assessment of where your risks are, and once you know that, looking at the key risks that need to be mitigated and what tactics some of the cyber criminals might use. Are they using software and hardware, typically called information technology? Are they using the information technology type of medium to attack? Or are they using the stolen credentials, in which the people, our users of the computer systems, become victims unknowingly? Because you and I would be able -- sometimes will be in a position to click on a link that came from a very genuine source, and people that we receive emails every day. And sometimes we may be clicking on those links. But having those cyber-awareness courses and training to the users to really be able to differentiate which ones that they need to be careful about is an important measure.

And once we know the tactics, really looking at all the three pillars: the secure aspects, being vigilant aspect, and the resilient aspect, becomes part of your information security program for the state.

This is just an illustration in terms of looking at the different type of threats. Now, we have organized it in, for example, on the first column, there is a financial threat, theft, and fraud. This is something that the cyber criminals have been interested in. The hacktivists are really looking at reputation damage. They're trying to inflict pain in terms of either as simple an attack as defacing a website to embarrass a government agency or an executive, and all the way to executing a data breach that could result in a huge financial hit, as well an impact to citizen trust. And looking at some of the other aspects, which have got very high impact for state governments, insiders and partners. Insiders, meaning insider threat, is a growing challenge. It could be fraud or it could be inadvertent issues caused by users who simply do not know what is an attack versus a genuine email or information technology resource they are accessing.

We have some insights from the 2012 Deloitte NASCIO Cyber Security Study. We did the study in 2010, and the 2012 was the next. And we are in the process of doing a study today, 2014 report. The 2014 report will come out in September. So the study really involved assessing and doing a survey of all of the states. And in every one of the studies, 2010 and 2012, 49 states and in 2012, 48 states participated in the study. And in the 2012 study we also had business stakeholders participate in a very brief survey about cyber security.

The findings: consistently the states are hampered by budget. That seems to be the top issue in terms of being able to tackle cyber-security problems. And the two other issues are, increasing sophistication of threats and inadequate availability of resources to address the cyber-security problems. It's almost like a perfect storm of not enough funds to address cyber-security issues and the threats are increasing in sophistication and you don't have enough professionals to tackle them.

So what are some of the strategies and tactics that the states can take under such circumstances? Now, some of the presentations like this really help in spreading the awareness of the business stakeholders to help support cyber-security initiatives and provide adequate funding and really increase the level of stability for some of these programs. Next slide, please.

And in terms of the business-official response, if you look at it, the executive sponsorship has to come from the top. In the case of the state government, from the Governor, from the legislature, and from the body that help the technology and agency heads in putting the necessary controls and vigilance measures, and being able to respond and recover from attacks. Now, this is very consistent with what we are seeing in private sector. In private sector, for a number of years, cyber security had become a board-level issue. It is not a technology issue any more the boards are tackling with it. And it is not just a financial-impact issue, because in addition to financial impact, the reputation and the business itself could suffer. Next slide, please.

And in terms of the actions for the state leadership, I have two callouts here. One is from the 2012 Deloitte NASCIO Cyber Security Study. The first step is really assessing your risks and

sharing the results with the business stakeholders. This was really meant for the state CIOs and really understanding the results, not at just the state-enterprise level, but also at the individual agency level. Which agencies have high-risk data that some of the cyber threat actors would be interested in and what is their current posture in terms of security measures? And really doing that assessment gives you the runway to make your security program more effective. And some of the other steps are like coming up with a strategy to address the risks and threats, investing in cyber-security measures, and educating on cyber security to your users and people, and finally, really measuring and reporting and sharing the story.

Now, in terms of measurements and reporting, one of the questions that we're often asked is, well, how much is adequate? This is really a program. It's an evolution. It takes multiple years to invest and understand and measure and really see the progress. Next slide, please.

So in terms of the call for action and some of the checklists, really assessing and communicating the security risks, better articulating the risks and all the findings with the business stakeholders. And one of the things that we found in the survey was a very interesting observation from the business stakeholders. Most of the business stakeholders that responded to the survey said -- 92 percent of them, in fact, said cyber security is very important or extremely important.

They also thought that the states are in a much better state of being able to protect against cyber threats than what the CIOs and Chief Information Officers thought. So we were able to compare and say, well, the business stakeholders believe that the cyber security is very important. But they also believe that the states are in a much better state than what the CSOs and CIOs think that they are in. So the aspect of reporting and communicating the risks becomes that much more critical. Because when the business understands the risks, then they are able to better support, either through the resources or funding or other measures, to be able to support these cyber programs.

And the focus on audit and continuous monitoring -- I mentioned about Chris Ipsen, Christopher Ipsen, and David Gustafson having a continuous monitoring program in collaboration with the city and county governments. I mean, that's commendable, starting those initiatives and having the necessary support for those. And we talked a little bit about the raising the stakeholder awareness.

And the last item is really making better security an enabler for emerging technologies. What do I mean by this? More emerging technologies, like the use of mobile technology, big data, and cloud technologies is something that's being increasingly embraced by the state governments. And in all of these technologies, the biggest barrier for implementing these technologies is the security concern. And so using these technology implementations as a lever for doing better security is another way to get the necessary support and funding. Next slide, please.

We just have a couple of brief synopses from the 2010 and 2012 surveys. This talks about the trend, in terms of in the state governments, where the threats are emerging from. I mean, in this particular case, cyber crime and state-sponsored threats will require a strong response from the states, because it looks like they are the ones that are on the rise. Next slide.

And I talked a little bit about this in terms of the business stakeholders reaction, 92 percent of them said it's extremely important. But in terms of the Chief Security Officers feeling, 74 percent of them get commitment, but inadequate funding. Next slide.

And these are the top five barriers: lack of sufficient funding; 86 percent of the states respondents indicated that as a challenge. And increasing sophistication of threats and inadequate availability of resources.

Now one of the other observations -- next slide, please -- one of the other observations was that the 2010 and 2012 surveys, not a whole lot of improvements. We saw that the states had not made tremendous strides or progress between in those two years. And we are looking to see how the 2014 survey results are going to be like. And so the point of sharing some of the results of the survey was to reiterate the point that the CIOs and the Chief Security Officers of the states really need the support of the legislature and the Governor's Office in order to implement an effective cyber program.

Now, again, thank you very much for giving me the opportunity. I'll be willing to take questions.

**Joe Marcella:** All right. I want to thank you for your report and I want to open the floor up for questions. There are a couple of observations and to start the ball rolling for at least a couple of questions. I noticed in your slide that you started to articulate the biggest offenses in causing the vulnerabilities within state government, and it was funding and so forth. But the biggest that I saw, but it wasn't ranked as the highest, was inconsistency across the board. That meant that structure and collaboration among multiple agencies, so that there was standards across the board, didn't seem to rank as high as I would've thought, and I'm not talking about consolidation. But when it comes to sustainability and when it comes to security, some sort of homogenizing the overall organization, normalizing that, seems to be almost rudimentary. It has to be done. And would you find that to be -- that folks are -- states today are approaching that rapidly or that it's just languishing?

**Srini Subramanian:** The states are talking to -- to take note of that because one of the things -- coincidentally, we actually called the study heading as State Governments at Risk: A Call for Collaboration and Compliance. The collaboration is a huge aspect, particularly after the 2012 report when all the states came back and said budget is a challenge. One way to really overcome the budget challenge is look to see how can you leverage the potential funding sources from the agencies and trying to do consistent implementation of security like you mentioned.

One of the best practices that we are starting to see is really the centers of excellence. If an agency is really doing some aspect of security really well and really developing that and promoting that to be an enterprise solution or shared services for security is another way to promote that level of consistency. It certainly is a challenge. It continues to be a challenge. And looking at the way of implementing cyber security more consistently at the agencies is going to be part of the strategy.

**Joe Marcella:** When it comes to mobile, eDiscovery, transparency, open data, and the like, is that even -- are we able to even accomplish that in any safe fashion without addressing cyber security first?

**Srini Subramanian:** I think for implementing any type of mobile or large initiative, cyber security should be a forefront activity. It should be part of the implementation. Doing cyber security as part of the implementation, thinking about it right from the business requirements is the way to go. Now, one trend that we do see is most of the states are quite competent at doing the eDiscovery and those kind of technology measures. The challenge comes in when large implementations need to be done and need to be done consistently and making sure that the agencies follow those standards and policies.

**Joe Marcella:** One more question. Joe Marcella, for the record. Is a single administration a best policy for cyber security within an organization?

**Srini Subramanian:** Single administration meaning a single point of administration?

**Joe Marcella:** A point of administration, governance, someone that's ultimately in charge.

**Srini Subramanian:** Certainly. I think someone being empowered to have a cyber security program is certainly something that needs to be done. And state governments have made strides, and about 82 percent of the states have a chief information security officer. I think the challenges, in terms of being -- for them having the disability of individual agencies -- what's going on with security in individual agencies and also being able to really straddle the certain aspects of cyber security has to be then enterprise wide.

But certain things have to be done at the agency level. Like, for example, communicating to the agency stakeholders on what their business risk and what they need to mitigate, is something that needs to happen very close to the agency business. So the states are still working on coming up with the perfect solution for how this can be managed.

But in the process, there are certain aspects of it that can be done through single administration or single point of contact. And one thing that we do see is consolidating some of the technology infrastructure plays a big role, because you have -- multiple points of infrastructure creates that many more points of failure, as well as being able to monitor that many different points of infrastructure. So consolidating definitely is helpful.

**Joe Marcella:** Thank you. Can I call for some questions from the Board? Kevin?

**Kevin Farrell:** As far as the underfunding, do you have a sense for how underfunded? Is it by half? Is it by more than that?

**Srini Subramanian:** So we were able to do some comparisons with the private sector, so with the financial services industry, for example, because we do similar surveys in those industries. And one of the things that we found was the underfunding is in two aspects. One is budget and the other is the number of people looking at cyber security. In terms of the number of people,

about 50 percent of the states said that they have one to five FTEs, full-time equivalents, looking at cyber security. A comparable multi-billion-dollar financial services institution has got 100-plus. And that's growing by leaps and bounds. So there is a huge gap in terms of how many FTEs are there really looking at cyber-security measures in a state government.

The second aspect is that it's a budget. Less than 50 percent of the states spend 1 to 2 percent of their technology budget on cyber security. And there is no real magic number as to what is right, but some of the research analysts, like Gartner and Forrester, they look at a number of 5 to 8 percent. And so in terms of the spend as a percentage of the technology spend, there is still a lot of catch up that the states have to do.

**Joe Marcella:** And do you find, on the FTE side, that states are having difficulty finding qualified people to fill the FTE positions they do have allocated?

**Srini Subramanian:** Absolutely. And then they're also losing cyber-security professionals, because this is one of the careers much in demand outside. I mean, we have difficulty filling positions in private sector. And some of the states are really looking at the pay scale for the cyber-security professionals and trying to see if that would enable them to attract more professionals. This is definitely a huge challenge across the states.

**Joe Marcella:** Okay. Thank you.

**Mike Willden:** Thank you, Mr. Chair. Mike Willden, for the record. These questions may be as much for Mr. Gustafson as you all. But I assume you're pretty familiar with what we're doing in Nevada, because you've mentioned Mr. Ipsen's name three or four times and Mr. Gustafson's, so -- but my questions are this, so I'm familiar somewhat with Chris' work, and then we also have people working on it out in the divisions. But I'm not sure if I really know that we've ever quantified the amount of resource that Nevada is applying. So that's maybe a question I would ask, is what level of effort is Nevada, and how do we stack up?

And then the other thing is I know they have coordinating meetings. Is there enough coordination going on, you know, because there's what each does, and then there are some efforts out in our agencies, because I mean, I know I get the emails frequently, both from Mr. Ipsen and our own staff. And I guess I would -- are there some recommendations to the Board that we ought to be looking at to either help support, you know, budgetarily or different coordination? And I know we, you know, we've done a lot of, oh, I'd call them surveys, of the agencies and what we're doing on various things, but I don't recall really a security survey, and so maybe I missed that. So just a couple of points of thought there, Mr. Chair.

**Srini Subramanian:** I will invite David Gustafson to talk about the specific to Nevada efforts. I'm familiar with what David and Chris have done from a national coordination aspect, because there are monthly coordination meetings at a national level, and so they do participate and share some of those aspects. But, David, do you want to talk about your specific efforts?

**Mike Willden:** Sorry, David, I threw you under the bus.

**David Gustafson:** Dave Gustafson, for the record. I think you might be right. There are monthly meetings and Chris Ipsen is going to be here later on to talk about some security stuff. We can pin him down on some more details. But there are monthly meetings. The problem is that as most of the security is decentralized, then we just, at best, try and keep everybody cobbled together with the same information. What Chris is going to tell you guys later on is about -- because of the directive from the Governor to start consolidating and centralizing security services, we have a really good story to tell. And we've been able to find some really interesting things that are happening on our network. And those would not be possible under the old directive of where we were going. And so there are coordination efforts going on, but when you look at securing all data in all places, that's a monumental task.

Especially when they're spread across 30 different data centers and 30 different networks and 30 different IT teams and scores of people -- hundreds of people who have access to that data, the information security task becomes insurmountable at that point. And so I think we do the best we can, you know, at the state, given the situation we're in. But I think, as Srinu is sort of saying, is that it's not really an ideal state, and generally speaking, we're underfunded. We are understaffed. And the way that we have implemented information technology in a decentralized way, it makes it exponentially more difficult to secure the data. And I think we're doing the best we can, but I just think that's the reality of our world.

**Joe Marcella:** Joe Marcella, for the record. Is there a best place to start?

**Srinu Subramanian:** I think the best place is to have a security program and to really do an assessment of your current state, of where you are, and really establish a target state. And look to achieve that state over a period of four to five years. And one suggestion I would put forth for this Board is looking for the visibility. I mean, ask for periodic reporting in terms of the progress being made against those goals and what are some other challenges that is preventing the teams locally to achieve those goals. Because once the level of awareness increases at the executive level and at the Board level in terms of, well, these are the risks that we are tackling and these are the resources that we are challenged with, I think some creative solutions through collaboration and some agency measures would come in play.

**Joe Marcella:** And what's the biggest barrier to success? Is it process, policy, people or funding?

**Srinu Subramanian:** This is a people-process technology. And this is my belief; I believe the funding challenge will go away once the real threats are known and the risks are understood. If you take a risk-based approach, most of the business leaders would find ways to fund such efforts.

**Joe Marcella:** Are there ancillary benefits to the business delivery by being secure? In other words, by going through the security process, are there other things that get dragged along or get considered to make that computing environment better, from a business-delivery or services perspective?

**Srini Subramanian:** Absolutely. Oftentimes, the security is thought of either as an insurance or as something that only comes into play when a data breach occurs. So security done right, right from the beginning and as part of a -- it can be a business enabler. And doing the security right, could really help elevate the citizen trust, as an example. You are working with the citizens, providing citizen services, and setting the example that here is a way to conduct business in a very easy, seamless way, and yet we provide assurance that it is secure. It means a lot. In the states that suffered breaches, the biggest impact that they had was more than the financial impact, was the citizen trust impact.

**Joe Marcella:** And in your opinion, what state has done a really good job of uniformly creating a security environment?

**Srini Subramanian:** I think most of the states. We don't rank the states. And I don't think the states rank themselves as well. Most of the states have done a very good job in certain aspects of their security programs. But in general, when we compared the state government sector with the private industries, the biggest advantage that the states have is their natural inclination to share. Because private sectors, they are in a competitive business and they don't want to share all the best practices and all their threats that much more readily, even though the last few years of the cyber threats evolution is forcing everybody to share information about these threats. But the state governments have done this very, very well in terms of being able to share specifically what's working and what's not working. And I think that's a huge advantage that the states have.

**Joe Marcella:** Any additional questions from the Board?

**Kevin Farrell:** Kevin Farrell, for the record. Is there any common way of classifying a breach, such that you can layout the breaches that have occurred and perhaps show an increasing frequency and intensity or severity that could foreshadow the need for that funding that you mentioned, as far as the legislature recognizing that it's coming and it's getting more intense?

**Srini Subramanian:** Oh, absolutely. I think, particularly in the state government sector, all of the breaches that need to be notified, they're all recorded. And some of the large breaches, there are information about how the breach occurred and how many days that the hackers were in that environment and how they actually -- when they took that millions of records -- how they actually secured it and took it back, took it away. All of the information is public. So that information is available. And the states, in terms of the state environment, the breaches from about five years ago used to be in advertent loss of laptops to really organized criminals making targeted attacks, using sophisticated mechanisms. So that information is available. And most of the states and CIOs and chief security officers have that information readily available as well.

**Joe Marcella:** Senator Denis, you had a question?

**Senator Mo Denis:** Yes. Thank you. I'm just trying to think about how other states are dealing with the cyber -- and I couldn't see the presentation. So I got most of it. But the question I have has to do with, you know, if we're going to (inaudible)...

**Joe Marcella:** The print is very small, Senator. The print was very small. I couldn't read it.

**Senator Mo Denis:** Okay. That's fine. I guess my question is, currently, I guess, with ours, what we're doing, and compared to other states, it seems like our cyber-security stuff is based on reactive versus proactive. You know, as you mentioned, a lot of times you have to wait for something to happen, some kind of a breach, before everybody understands how important it is. Do you see that changing throughout the country or is it still basically, you got to wait for something big to happen? Because, you know, when you start talking about budget things, you know, it's hard to get people to understand technology as it is. And they don't really understand the cyber stuff. I mean, they see the stuff that happens, like at Target and other things, and they're concerned about it. But generally you have to wait for something like that to happen before we can do something. Are you seeing that -- I mean, what's happening across the country in respect to that?

**Srini Subramanian:** Senator, you're right about the general tendency is more reactive than proactive. But in the last about 18 months or so, the level of awareness has increased tremendously. With the National Governors Association, National Association of State CIOs, and everyone actually taking this and sharing the information about what a large breach can do to a state government environment, that has been very effective in conveying the message that, don't wait for a breach to occur, because it's too late and it is too disruptive. When a breach occurs, it can have a pretty disruptive effect in terms of what happens to the people that have been putting a security program in play, versus the response efforts continuing for a number of weeks, months, if not years. So to answer your question, Senator, it is not going to be acceptable for state agencies or state government in general to wait for a breach to occur, because the impact of that could be too disruptive.

**Senator Mo Dennis:** Thank you. And my hope is that we'll be able to get that message across. We only have one chance every two years, as a legislature, to have this discussion. And if we don't -- if it's something we need to do, which obviously we do, we're going to have to make sure that at least all my colleagues understand the importance of this, including the Governor's Office, as we move forward, and how important this is for the state. So that's just a comment. But thank you for answering the question.

**Srini Subramanian:** Yes, Senator. Thank you for your question. And I think that, again, with the NGA, there are also some modern legislations that are being talked about that the states could do. And that just provides more visibility to the legislature in terms of what are the cyber threats and where the state agencies are with respect to addressing those. And this could be an ongoing challenge, program, and improvements that would happen over a period of time, several years.

**Joe Marcella:** Again, thank you for your presentation. Are there any additional questions? Rudy?

**Rudy Malfabon:** Recently, there was that Heartbleed, I think it was called, that...

**Srini Subramanian:** Mm-hmm.

**Rudy Malfabon:** ...it seems that the hackers are getting more and more sophisticated. And what I read was that people might not even know that their computer or whatever device is infected. These things kind of hide themselves, so it's not as evident. Could you have any comment about that? How sophisticated some of these things are getting and how we have -- we're always seeming to try to catch up, just as the comment made about being reactive. It seems like that's always going to be there.

**Srini Subramanian:** To some extent, it's always going to be there, the catch-up aspect of it. Because the cyber threats are becoming more sophisticated. And in the case of Heartbleed, it was a vulnerability that existed for a number of years, and I think someone had looked at it and exploited it. What we are seeing is a major difference is how the cyber criminals and cyber actors are able to exploit it much more systematically, like in terms of their communication mechanism and how the threats are exploited and monetized in a very short amount of time. And that seems to have really dramatically increased in the last few years, or intensified in the last few years.

Even today, there was a news about another similar type of a program being available for -- it costs as little as \$40. You could spend \$40 and get that kind of a malware, or think of it as a small tool that you can use to take ownership of somebody else's computer. And when these type of tools are available so freely and so inexpensively, then there are -- and when the threat is global, it just is a different world. I mean, which is the reason why we started talking about, well, there is really no perfect security. So it is a program that you are constantly playing catch-up to some extent. But you are doing the due diligence, being secure. But you are also monitoring what's going on in your environment to be able to respond and recover. And in the case of Heartbleed, most of the states responded really well and quickly.

**Joe Marcella:** Thank you. Any additional questions? Lynda, could I ask you to -- I understand we now have a quorum. Would you explain that?

**Lynda Bashor:** Mr. Chairman, with your permission, we'd like to request that Assemblyman Bobzien be acting as proxy for Assemblyman Anderson.

**Joe Marcella:** You have my permission.

**Lynda Bashor:** Thank you. We now have quorum.

**Joe Marcella:** Thank you. Understanding that we didn't have a quorum, I'd like to just back up one agenda item and have a motion to approve January 27<sup>th</sup> minutes. Can I have a motion?

**Senator Mo Denis:** So moved.

**Joe Marcella:** And second?

**Rudy Malfabon:** Second.

**Joe Marcella:** Discussion? All those in favor?

**Group:** Aye.

**Joe Marcella:** Okay. Let's move on to the next agenda item. Thank you. Before we move on to the next...

**Srini Subramanian:** Chairman, may I be excused?

**Joe Marcella:** Yes, you may. I'm sorry. Thank you. But, then again, there will only be one seat for David, and that would shorten the presentation. Much of what this meeting is going to be about is what we're going to do in the future, not necessarily what we've done in the past. And I'd like to make just a couple of quick comments before we move into that. I know David's going to give a presentation on legislative issues, your current state, what the rest of the world is doing. I also want to repeat what we already know -- it's actually repeating the obvious. We've spent a great deal of time in this Board deciding what was broken and what needed immediate attention. We just heard some of that discussion about security.

I think we've done a good job of identifying, from consolidation right on through to cyber security and cloud technologies and upgrading some of the infrastructure, as well as what would happen if we did put certain groups together. And we're doing that with a pilot with DTS currently. The next meeting of ITAB is going to talk specifically and focus on where the state needs to go from a business perspective and services that need to be delivered. Once we know that, we can then start to back into what kind of infrastructure, cooperation, consolidation, if it's necessary, shared services are going to be necessary to accomplish that.

To date, we've been able to help each organization survive, reorganize, pilot some things and then start to move forward. Also, create some documents that have helped in budgeting and getting the legislators attention, as well as the community's attention, so that there's more of a focus on the ability for technology to assist in the delivery of services -- almost advancing the delivery of services. So, again, we'll finish up this meeting through talking about where we were. At our next meeting, we'll focus on where we're going to go. So, David.

## **6. CIO UPDATE (For Possible Action) Presented by David Gustafson, State CIO**

### **A. MAY 2014 NASCIO CONFERENCE**

### **B. ISF/BILLING STATUS**

**David Gustafson:** Thank you, Mr. Chairman. David Gustafson, for the record. I always feel like I'm sitting on the ground every time I sit in one of these chairs. I don't know why.

**Joe Marcello:** There's a little lever to make you taller.

**David Gustafson:** Yeah. Apparently, I'm not tall enough. I wanted to say that the last session, probably in this exact very room, I arranged to have the streaming of the firewall logs up on the screen when I was giving my budget presentation. And at the time, I had said that there were about six million attempts every day to access state data that -- unauthorized access. And I said, you know, that the task of our information security group is to sort through the scrolling log, which is unreadable by human eyes, and pick out the good traffic from the bad traffic. And that's just a taste of how we have to use technology and we have to have the right strategy in place to be able to address cyber security. It's very important to me, has been and it will continue to be, because I don't see there's no easy way to solve that problem. It's going to be through brute force and technology are the only ways we're going to be able to get a handle on that.

So, Mr. Chairman, I have some prepared remarks I want to go through with my CIO update here. And feel free to chime in at any time if there's any questions. Today, I'm breaking rank and tradition. I brought with me two members of my senior management team; both Jim and Amy, whom you'll hear from later today, are very experienced and well respected in their fields. Jim, a former JAG and State Department attorney, and Amy a certified professional in Human Resources, and a tenacious customer service and business representative. Together we bring unique perspectives and ideas to the very challenging problems of today: a simple IT guy, an HR and business virtuoso, and an accomplished lawyer. A potent, yet intriguing combination of ideas and creativity. I've come to rely on their counsel, and I believe once you've had a chance to know them, you will too.

Mr. Chairman, I begin my presentation with a NASCIO update. As many of you know, last year I was elected by the NASCIO governing body to represent the association as the secretary and treasurer. In my capacity as secretary and treasurer, I bring critical positive energy and attention to Nevada. Jim, Amy, and myself all attended the mid-year conference in Baltimore, Maryland, this year. We traveled on May 5<sup>th</sup> and the trip began in earnest on the following day, Tuesday. Tuesday was marked for state business only and no vendors were allowed to participate in any of the presentations or discussions. I presented the NASCIO budget and work plan for the coming fiscal year. And it was a nice opportunity to catch up with some of the state CIOs and see how some old friends were doing.

I spoke with the CIO of Connecticut about their Deloitte Insurance Exchange, the Utah team about their Enterprise Network Services, and Texas about their email migration to the cloud, to name a few. As a point there, something I was not ready for with Texas, Karen, the state CIO, told me that they had moved 110,000 seats. And that they were moving a total of 300 and -- I can't remember, 330,000 seats to the Microsoft cloud email. And I just started thinking about the magnitude of Texas. You know, we already know Texas is a very big state, but those are some really, really big numbers. The day concluded on that Tuesday with a nice dinner with the Wisconsin team, the CIO and the CISO, and Gartner leadership.

On Wednesday, May 7<sup>th</sup>, we went to D.C. for meetings and briefings with federal agencies. The briefings began with FCC Commissioner Jessica Rosenworcel on E-Rate 2.0 and the FCC priorities. Commissioner Rosenworcel outlined the changes that she's encouraging the

Commission to adopt with E-Rate and the states provided some critical feedback on the program as a whole. I don't know if you guys know about E-Rate, but the purpose of the whole E-Rate initiative is to get subsidies set out for underserved schools. This is for a school program. So if you're a school that doesn't have a lot of funding, then the federal government makes available funding to buy data circuits and connectivity so that everybody has an opportunity. This is really important to a lot of states because, as we move to online assessment testing, which is mandated, I think in 2014, I think, then all of the online assessments and everything have to be taken online. So the E-Rate is a mechanism by which they sort of help bring bandwidth considerations as a whole.

Next, we heard a very nice presentation from J. Patrick McCreary, he's the associate deputy director of the Bureau of Justice Assistance, Department of Justice, on the importance of partnerships, the value of data, and most importantly the impact of data-driven justice on policy, operations and discussions. Following Mr. McCreary, we moved into a presentation from Ms. Roberta "Bobbie" Stempfley, she's a deputy assistant secretary for Cyber Security Strategy and Emergency Communications; and Mr. Matthew Scholl, acting director chief and deputy division chief of Computer Security Division of NIST, the National Institute for Standards in Technology on the cyber-security framework and intergovernmental cyber-security relationships. Well, that's a mouthful. But NIST just came out with a whole cyber-security framework, which they've released to the public, to sort of help people to bring security programs together. It was a really nice, interesting conversation.

After lunch we had a briefing from Ms. Teri Takai. You may know her. She was the Michigan State CIO. She was California State CIO. She was Department of Defense CIO. And she had -- let's see, we had met on Wednesday and the previous Friday she had tendered her resignation as the CIO of DoD. But she is a member of the FirstNet Board. And so, if anybody knows anything about that, that's the public communications broadband initiative, whereas the federal law requires FirstNet to establish public safety communications essentially coast-to-coast and islands. That is easily done in some of the other states and not so easily done in mountain states. So high-speed broadband connectivity, even in rural Nevada today, does not exist. So their task is quite large.

We also heard from on that particular one, T.J. Kennedy, he's the deputy general manager of FirstNet, about their implementation. There's a lot of state feedback on their business case. We have yet to hear a defined business case from these folks as to how they're going to actually roll this system out. Most of us are afraid that once the cost estimates come back, that the cost-per-radio-per-month, if you will, is probably going to be an outrageous amount of money. And so we're waiting to hear about that.

This is where things, I think, in my opinion, got little more interesting. After FirstNet, Jim and Amy and I all attended a smaller breakout session on cyber security with Mr. Keith Castaldo and Dr. Steven Lev from Senator Kirsten Gillibrand's office. They are attempting to put together separate and direct grant funding opportunities for state and local governments. We pledged our support and offered assistance to review their bill draft language as it became available. They

recognize that most states are getting funding from Homeland Security for their state cyber security programs. And that puts the cyber security folks in competition with, you know, fire trucks and robotic dogs and all the fun stuff that those guys like, and bullets and shotguns and everything. So they recognize that that probably, in a push-came-to-shove situation, the guys with the guns usually win. And so what they're aiming to do is really put together a program where cyber security will have its own direct funding from the federal government; most likely through DHS, but it would be direct and separate, just for cyber security. So we were interested in that.

On Thursday, May 8<sup>th</sup>, I moderated two disaster-recovery roundtable sessions and there were some great presentations from NSTIC, that's the National Cyber Trusted Identities in Cyberspace, I think is what it is, cloud procurement, and a session on state IT workforce development. The evening concluded to a trip to the Baltimore Aquarium, which was quite fascinating, and I had an opportunity to catch up with Xerox, First Aid at Oracle, and the Symantec teams. And I'll put a shameless plug in here for the Baltimore Aquarium. I was actually very impressed. I travel around the country, going to all these various places for conferences, and I can tell you, the Baltimore Aquarium was definitely one of the most interesting places I've been in a while. And if you're in the area, it's certainly definitely something I would consider.

On Friday, we began with a mobile lap showcase breakfast, followed by a Cyber Security Panel discussion, health insurance lessons learned, and a keynote on institutional culture change, leadership innovation, and inclusive excellence by Dr. Freeman Hrabowski, president of the University of Maryland, Baltimore County. I'm trying to think of how to even describe that. It was really interesting. He was throwing out all kinds of statistics about college graduation rates from, you know, the Fifties, and he went in to breaking it out by ethnicity. And it was really an interesting conversation about where the world is going and why the United States has had excellence. And my takeaway was that because of immigration, the brightest people in the world come to the United States. But as we sort of wane in our prestige, if you will, at other countries, we tend to emerge from that, then what we may find is that the brightest people from India or pick your, you know, favorite country, then they may end up going to China or to Japan or wherever else may be the next best thing. And so it was really an interesting conversation by NASCIO.

And then, lastly, Mr. Chairman, I'll talk about the internal service fund billing status. And as of lately, my energies have been focused on the budget-building process, which is not a trivial matter for us. Heartbleed, Windows XP computers, and the Insurance Exchange. So I haven't had a whole lot of time to dedicate to this. I had submitted to former Director Mohlenkamp, a proposal for a procurement and implementation of a department-wide enterprise billing software solution. I have not had that opportunity to discuss that initiative with our new director, Julia Teska, though. So I had put that in the queue, in the hopper, if you will, but I have not had a chance to catch up with her on that topic.

Mr. Chairman, any questions you might have?

**Joe Marcella:** Joe Marcella, for the record. Just had a couple of comments. And I think, Kevin, you may want to chime in on the ISF and the billing status, at least from a recommendation perspective. But to talk about NASCIO and what came out of that -- was it four days you spent?

**David Gustafson:** That's correct, yes.

**Joe Marcella:** Correct? And I think this is important, because it runs a correlation, as well as a validation, of everything that we've heard today. Security -- for 2014, the state CIO top priorities, beginning with security. Second would be consolidation, optimization, centralization, consolidating services operations, resources, infrastructure, data centers, communication, and marketing. Now, keep in mind, they didn't say consolidation of business, not like there were for DMVs and consolidating all of them to the same DMV. We don't have four DMVs. The other -- the next one in line -- the next item, number three, was cloud services. And the state should be proud of themselves for pursuing alternative service delivery and alternative service providers.

This is what's most important and we're here where the focus is, right in the middle; project and portfolio management, and second to that priority is strategic IT planning. None of the -- the beginning part of the first priorities are to set a foundation. The middle priorities is to get to some level of business direction. All of the remaining priorities are in support of the first five. So, again, where this Board needs to go and where the state needs to go is a clear definition of what we can build from the foundation that's already built, and that would be service delivery.

And I'll go through them very quickly. The next one in line is the magic budget, mobile services, shared services -- which again has already been piloted by EITS -- interoperability nationwide, and we heard a little bit about that both at what you've viewed, as well as what we heard from security, and then health care, and we know we're all dealing with that. Kevin?

**Kevin Ferrell:** Well, related to the Internal Service Billing, I wasn't at the January meeting. I had a conflict in my schedule. But my recollection from the prior meeting to that was the report that was presented by the internal team that had gone through some management program. And my recollection is that they were making some recommendations about the need for process alignment and some requirements definition around that. And so I'm curious as to kind of where that stands in regard to the proposal that you were discussing.

**David Gustafson:** David Gustafson, for the record. We have known about some of our billing challenges. That assessment from the internal team is what spurred me into action to get with the Director to make an official proposal. Our new Director is probably no less than 30 days on the job now, and so I haven't had a chance to get with her on that. But that is something that she also needs to be aware of.

And really what -- let me rewind the clock a little bit and sort of explain how we got here. When we were a department, we had our own policies, our own procedures, our own everything, and our own staff to do that. And when we merged with the Department of Administration, they just tried to take what we had and just plop it over into the Department of Administration and it didn't

really work out very well. And so we've struggled with trying to find the right magic again, the right secret sauce here. And I think what we're really missing is really an enterprise piece of software to do that.

And we are not the only billing division in the Department of Administration. There are others that should also be a part of this discussion as well, which is why I think the conversation really needs to be had at the Director level as to, from a department perspective, they need to have -- the department needs to have an enterprise billing piece of software for various services that are provided from the Department of Administration, not just IT but including IT. And so in all fairness, you know, Julia has only been on the job for a month or so and I haven't had a chance to get with her on that. But it is on the top of my list.

**Kevin Farrell:** And is the platform you're looking at something of an IT service catalog or something that could be turned into a business-service catalog as well?

**David Gustafson:** David Gustafson. That's exactly what I would have in mind. Absolutely.

**Joe Marcella:** Mike?

**Mike Willden:** Mr. Chairman, Mike Willden, for the record. David, I wanted to follow up. If I was following your discussion on the grants for cyber security from DHS -- not DHHS, but DHS -- and so if I heard you say that they would be separating out potentially the guns and robotic dogs pool to a cyber-software pool. So my two questions is -- well, actually three questions. When would we expect that that grant opportunity would come available? In my department, you know, they come out and you've got 45 days to turn something around. So that means you'd better have a plan or you better be -- we, I don't mean you, but all of us -- we better have a plan or you're going to miss the window. And so I don't know if you have any feedback there. And then does it require a match? Do we need to be rallying the troops to be ready to demonstrate match?

**David Gustafson:** Dave Gustafson. All very good questions. And at this point, the Senator's office is trying to build the right legislative model. They know that funding is going to be really challenging. And I think the federal government already has their funding already set for the next fiscal year, I think, for the federal government. So this would be something that probably would come after that.

**Mike Willden:** So very long term then?

**David Gustafson:** Well, sure. Right. It's -- but what we had proposed was that we'd be available to, you know, to...

**Mike Willden:** Help draft language or (inaudible)...

**David Gustafson:** Yeah, absolutely. And review language. And also to speak with our leadership about, you know, our federal representatives as well. How we might encourage such action to do so. They're still in the preliminary stages. They know that funding is going to be a

problem, and so they're trying to find the right vehicle to do that. I think their heart's in the right place and I think that just starting that conversation is really encouraging to me. I think it'll be a longer term.

You see, as they sort of explain it to us, they don't want the states to have to fight with pretty, you know, fire trucks and all those kind of stuff, or aging infrastructure or programs that are already billed through the Homeland Security system. And they realize though that if they do nothing in cyber security, then what will happen is states don't have the funds to do that. So they'll do less.

It sort of gets back to what Srini was saying. We're already way behind the power curve here. And so if we don't find funding in other places, then we'll just continue to do less and less. And we're a huge liability because, when states get breached, it's a one-way tunnel straight to the federal government. And so, if we get breached -- we, the State of Nevada -- and our communication line goes straight to the federal government, then, you know, then it puts them in direct risk. So they're trying to also hedge some of their bets, give us an opportunity to sort of increase our cyber security programs, and advance the ball a little bit against the actors of today. And so, Chris, did you want to add something?

**Chris Ipsen:** Do you want me to talk about what's happening with that grant right now? I just...

**David Gustafson:** No further comment. Mr. Chair, any more questions?

**Joe Marcella:** Any more questions from the Board? Rudy.

**Rudy Malfabon:** Dave, I've been hearing about Net neutrality in the news. And how does that affect (inaudible). It's more for public internet?

**David Gustafson:** Yeah, they're trying -- Dave Gustafson -- they're trying to figure out how to regulate the Internet. And it's -- I have to be honest with you, there are some heavy hitters on both sides of that fence. And I'd just as soon let them scrap it out a little bit and see what happens. I personally don't see anything happening any time soon because, you know, there are some really big, heavy-hitting players on both sides and they have a lot of money. So I figure they'll fight it out for a decade or so before they finally get to some conclusion. But I don't worry too much about it at this point.

**Joe Marcella:** Any other questions for the State CIO? Can I have a motion to accept David Gustafson's report?

**Senator Mo Denis:** Move to accept.

**Joe Marcella:** Second?

**Mike Willden:** Second. Mike Willden.

**Joe Marcella:** Any discussion? All those in favor?

**Group:** Aye.

**Joe Marcella:** Okay. I'd like to move on to the next agenda item. Before we do that, is a five-minute break appropriate at this time? Would folks like to take a five-minute break? Well, let's go ahead. Thank you.

**7. EITS STRATEGIC PROPOSALS FOR NEXT BUDGET SESSION –  
David Gustafson, State CIO & Jim Earl, Cyber Counselor (For possible  
action)**

**A. LESSONS LEARNED FROM MERGERS/CONSOLIDATIONS**

**B. STRATEGIC SOURCING DISCUSSION**

**C. BILL DRAFT REQUEST - NRS 242**

**Joe Marcella:** All right. I'd like to call back to order and continue. Thank you. Mr. Earl.

**David Gustafson:** Mr. Chairman, Dave Gustafson. I'll begin with the introductory statement here and then we'll move into -- Mr. Earl will present the actual bill draft request that we're proposing.

I'd like to begin by outlining our present strategic direction. This is not written in stone. Quite the contrary, I seek the Board's advice as our statute contemplates. Does the Board believe we're headed in the right direction? And if the general direction is appropriate, how might we modify our approach to be more successful? This is exactly in line, Mr. Chairman, with your direction of where you'd like to take the Board as well. To sum up in a single sentence, we want to position state agencies, including Enterprise IT, to efficiently and effectively take maximum advantage of evolving technology services, whether they are provisioned internally or externally.

My number one priority as State CIO is to move the government forward, leveraging all the benefits of information technology. That objective is easily stated, but is problematic to obtain in light of the turbulent environment we find ourselves in. On one hand, as you heard during the last meeting, directors of major executive branch agencies remain opposed to full IT consolidation. And by full IT consolidation, I mean the current model where EITS and DPS IT personnel and operations were merged. On the other hand, key legislators have reiterated their position since the close of last session that they expect full consolidation efforts to be part of the next Governor's budget. We at Enterprise IT have produced a BDR that seeks to align IT service provision with existing and future executive and legislative branch policies, regardless of how the mix of consolidation activities may play out over the next several legislative sessions.

Jim will get to the BDR in a minute. But first, I want to summarize the BDR objectives, and second, explain how we incorporate the lessons we have learned from our work with the Department of Public Safety IT. We believe our governing statute, NRS 242 and other related statutes should be amended in such a way as to accomplish the following:

1. Provide the Governor the statutory ability to determine what Enterprise Services executive branch agencies will be required to receive from the IT Services Division.
2. Expand and strengthen the ITAB, the Information Technology Advisory Board, Mr. Chairman, giving it a review of approximately 75 percent or more of the state total IT spend up from currently about 15 percent. And Jim will talk about the specifics of that in a moment.
3. Institute strategic sourcing to align management and budget decision makers with the business outcomes of the programs.
4. Complete the integration of the former Department of Information Technology into the Department of Administration.

I'd like to go through a few lessons learned here before I hand the microphone over here to Mr. Earl. We've identified these goals and the statutory language to obtain them, in light of our recent experiences. Here are some of the most important lessons so far from our consolidation of DPS IT.

1. The DPS network was not in as good a shape as we had expected. By the DPS network, I mean both the NCGIS (sp?) network and the currently commingled administrative networks.
2. The DPS IT staff, along with Enterprise IT staff, had suffered from the consequence of long-term personnel budget deficiencies and lack of training funds and opportunities.
3. Staff experience and training from both organizations was a mixed bag. Meaning, there were areas of excellence within both organizations, but when the consolidation and the teams were reformed, some weaker areas remained within the organization, irrespective of their increase in size.
4. We have a severe deficiency of project managers and in light of DPS's recent experience, see the likelihood of recruiting personnel with the necessary qualifications into state service at existing funding levels and current FTE compensation levels to be difficult.
5. EITS effective responses to DPS service outages were possible only by ignoring our current limitations on management authority and accounting rules. And I've spoken about that before, where we have certain cost pools and certain resources, and they're not to be commingled.

As you are aware, DPS consolidation was not the only major undertaking we found ourselves tasked with during the past year. We have been simultaneously engaged in a number of things. Here I'll go through five of them just quickly.

1. Deploying the Symantec Security Suite across executive branch agencies, using independent IT staffs in agencies outside of the Department of Administration and Public Safety, an Enterprise initiative.

2. Working with the Procurement Division and the AG's office to move as quickly as existing procedures and personnel allow to procure and deploy replacement equipment to support the state's core telephone system infrastructure.
3. Replacing over 2,000 Windows XP operating systems with currently supported operating systems, often installed on new hardware, with the attendant task of reinstalling and reconfiguring software applications currently in use.
4. Research, writing, and initially releasing a major RFP design to replace both the state email system and current methods of document production with a cloud-based solution.
5. And lastly, Mr. Chairman, researching, writing, and drafting another major RFP designed to provide for a centralized, self-funded state resident portal.

While each of these undertakings has produced its own lessons learned, let me summarize only two lessons that are common to them. First, all these undertakings utilized only existing staff, with one half-time contract project manager. This had the effect of lowering our overall efficiency, because existing IT managers were already fully burdened; had to take on the task of the project management skills relating to tasks, training, and expertise, in addition to their daily workload. Second -- and this is quite important in light of what we propose in our bill draft request -- we have learned that enterprise-wide implementations, such as our centralized security solution we call Altiris, which is the product name, can be a relatively efficient way to deploy new technologies across IT decentralized executive branch agencies, as long as clear directives, leadership, and funding are made available.

At this point, I'd like to introduce you all to Jim Earl, our cyber counselor, who will be briefing you on the proposed bill draft request details.

**Jim Earl:** So, to put it bluntly, our bill draft request is an attempt to thread a needle in the middle of a hurricane. There are people who feel very strongly in Nevada State government about the issue of IT consolidation, when IT consolidation is taken to mean full consolidation, as we've experienced with the Department of Public Safety in the last year or so.

Now, you have two documents in front of you that deal with our BDR. The first more lengthy color-coded document, let me ask you to put aside for a bit, because we're going to get to that later, if at all. This is the line-in/line-out version that presently sits in the NVS (sp?) system. And after putting together these changes, some of which are proposals that deal with taking language entirely out of the Nevada State statutes. Some of which would put new language in to NRS 242. Some of which would move statutory provisions from NRS 242 into other areas of the Nevada State statute series. And there's a sunset provision in here as well. Those are all color-coded in the long version, with explanatory notes in text boxes to the left. But it would be a monumental job to try and go through those and explain in a simple, coherent fashion, what we're trying to do.

So I'd ask you instead to take the much shorter document, which on the first page has only black and white. As the parenthetical after the chapter heading indicates, this is how a new NRS 242 would read, after legislative action, which would pass our bill to position agencies for evolving information services. So if you...

**Joe Marcella:** Mr. Earl, I'm going to interrupt just a second. I don't have the documents, so -- please continue.

**Jim Earl:** If you flip to about Page 3 and look down at the bottom, you will see a provision which is new provision NRS 242.064, and that's the definition of common services. This is a new concept which we want to introduce into the statutory scheme. And, essentially, common services means those information services that the state generally provides to state employees, and they're listed there. Now, of course, not every state employee gets a computer. Our groundskeepers don't. Our motor pool folks don't all. But generally speaking, a common service would be the type of communications and information technology capabilities that are provided to an average employee.

Specialized services are defined later. And those, in essence, are the services which EITS presently provides to agencies. And some of examples of those are wide-area network capabilities, and server and mainframe functions.

The concept of enterprise services in draft 242.065 draws on an idea that was discussed in the last legislative session and was brought up for further discussion in one of our ITAB meetings by the former Chief of the Budget Office Jeff Mohlenkamp. And that is the concept that rather than consolidating people and programs in large chunks, taking all of the DPS IT staff programs and equipment, for example, and moving them into EITS. One of the things to consider was a service-by-service consolidation. And so this definition of enterprise services is the first step in providing both legislators and the Governor with options that may not exist in quite the same form in the present legislative structure.

If you move on to the purposes of the Division of Information Services, you'll see the first use of the common and specialized services. We would describe our mission going forward to provide common and specialized services to the two agencies that are consolidated, Department of Administration and Department of Public Safety. And then if you look down to three -- and I'll get back to two in just minute -- the third purpose of the Division is to furnish such enterprise services to executive branch agencies as the Governor may direct. Now, two, which appears in bold -- oh, excuse me, in maroon typeface here, would sunset. And essentially we would provide, should this bill be passed, the specialized services that we provide to state agencies, only for the next interim period. And we'll talk a little bit more about that in just a moment.

So, looking at one, where the common and specialized services are listed to -- our mission is described in providing those to consolidated agencies. That list, of course, could be expanded by normal legislative proposals and actions, either on the Governor's initiative or on the legislature's initiative. Division would provide enterprise services to those executive branch agencies as the Governor may direct -- that flows out of paragraph three. Now, the Division's provision of

specialized agents' services to state agencies, other than those that are fully consolidated, would sunset after the close of the 2017 legislative session. This gives agencies in the executive branch a full two years to examine their strategic sourcing options. It also provides the Governor the same two years to determine which, if any, services he will direct to be enterprise services.

Now, let's come to that same type of issue from another route. If you continue on in the shortened version and flip a couple more pages as you come to NRS provision 242.131. And you'll see that that text is produced in maroon type as well. That entire section would sunset after the close of the 2017 legislative session. Between the enactment of our proposed bill and the time of sunset, agencies would have two years to determine whether it was in their best interests to fully consolidate their IT operations. In which case, the Division EITS would provide their common and specialized services both. Or alternatively, agencies could determine they wanted to self-provision both common and specialized services. Self-provision would require agencies to fully cost that option and present their proposals as part of their 2017 budget preparation process. And quite frankly, we envision that during the period of that two years, agencies who had questions as to whether they should become fully consolidated or not, would take the time and spend the effort to do a fully cost-allocated study of what was best for them in terms of self-provisioning or become fully-consolidated agencies.

Now, it's very important to recognize that the agencies would not be making those self-provisioning decisions in a vacuum. And bear with me just a minute. If you flip through the new NRS 242, that portion that's quite a bit shorter than the present version, you'll see that virtually all of the provisions relating to ITAB, this Board, will have disappeared from the new NRS provision 242. Well, are we suggesting that ITAB be established, simply vanishing into the ether? No. ITAB, in fact, will have its composition and mission expanded. Right now ITAB is set up to advise David -- a Division, not a Department -- a Division administrator, who presently controls less than one-sixth, as near as anybody can tell, of the total IT spend of the executive branch.

Our proposed bill -- the text which accompanies the BDR, which you have in the longer, line-in/line-out, multi-color format -- would change ITAB so that after the bill's enactment, in the next legislative session, ITAB would advise not David, but the chief of the Budget Division, who controls, on behalf of the Governor, 100 percent, or nearly that, of the IT spend of the executive branch. Additionally, our bill would expand ITAB in the following ways. First, the directors of the departments with the largest IT operations would become Board Members of ITAB. Secondly, additional legislators representing the government operations committees of the Senate and Assembly would join ITAB in light of the increasing reliance placed on IT operations in the provision of state services to Nevada citizens. And lastly, we want to open a discussion around whether the heads of the Legislative Counsel Bureau and the Administrative Office of the Courts would become ITAB members. The new statutory provisions relating to ITAB would allow them to request, should they deem it appropriate, information enabling them to take advantage of economies of scale in service procurement and in security monitoring, if doing so would advantage their respective branches of government.

So let's go back and look at what strategic sourcing would mean in practice. After passage of our proposed bill in the 2015 legislative session, ITAB would be expanded and would advise the chief of the Budget Division on strategic issues across the executive branch and indeed, potentially, across the entire State of Nevada. Two, executive branch agencies would have to determine whether they felt it in their best interest to self-provision both common and specialized services. The self-provisioning decision of those agencies would not necessarily take place in a vacuum. It would be open to the new ITAB, with directors of the largest departments to recommend appropriate actions directly to the chief of the Budget Division during the two-year legislative interim. And lastly, the strategic-sourcing decisions of executive branch agencies would need to be enshrined in the Governor's budget recommendations to the 2017 legislative session.

Now, to be sure, the proposed bill -- the extensive line-in/line-out multi-color version -- tidies up a lot of additional issues to align future statutory provisions with past and existing executive and legislative branch policies. But rather than go on to these issues, which might be put off to another ITAB session, let's wind up.

The following agency item deals with EITS personnel. So if you look at 242.080 -- that's in the shortened form -- you will see that the vision consists of the administrator and such personnel as he deems necessary and appropriate to carry out the provisions of the statute. That cuts down the existing statutory language by quite a bit. But that same formulation is used in other statutory provisions in the Nevada Code to establish agencies. So we're not out of the box on this. We're simply adopting a relatively standard description of the powers of the head of an agency.

The administrator is directed, in one of the next provisions, NRS 242.101, "to employ and manage classified and unclassified position." This is because we envision a shift towards the unclassified service. And in the next agenda item, my colleague, Amy Davey will talk a little bit more about some of the underpinnings of that. We have, over the last year or so, with the consolidation of DPS IT personnel, attempted to employ them despite the budgetary restrictions that have been imposed on us, in their highest and best use, while simultaneously becoming sufficiently adaptable to accommodate both more consolidation and service changes. Essentially, that's what we want to do. We know that it's difficult when you take people into an organization, to employ them to their highest and best use. And one of the ways that we want to -- one of the manifestations of changes in this language is we want to allow sufficient personnel flexibility to enable those types of deployments to an individual's highest and best use, should the Governor determine that there are certain classes of services that he defines as enterprise services or should the legislature and Governor, acting together, enact statutes that add to the list of fully-consolidated agencies.

Let me conclude by saying that the line-in/line-out version of the current NRS 242 is pretty lengthy. But the provisions that are transferred, added, deleted or sunsetted have been identified, along with the explanatory text boxes. And you have received that version electronically, as indeed have all of the current Nevada State legislators, each of whom was invited not only to this ITAB meeting, but to all of the ITAB meetings that have existed for the last year or so.

We're available to answer any questions either now or at the next ITAB meeting, after you've had the opportunity to consider how our proposals relate to one another and how they interact in the larger line-in/line-out more colorful version.

**Joe Marcella:** Joe Marcella, for the record. And I've got a comment and a series of questions. First comment would be -- and it's more of a question -- when you talk about consolidation that always brings up a different vision and different definition to certain folks, and not necessarily uniform across the board. Could you be a little bit more specific when you talk about consolidating technology?

**Jim Earl:** Okay. And, Joe, we look to you. And we take the ITAB records and transcripts very seriously. We refer to them in answering a number of questions which the legislative staff has posed to us, both in the interim and the last legislative session. We're looking for a way to describe the type of service-by-service coming together, because I'm not using consolidation on purpose, that was discussed during the last legislative session and since. And realizing what you just said, that consolidation is a loaded word across multiple audiences, we found a term which, at least in our experience, you were the first one to use several ITAB meetings ago. And that was strategic sourcing. Now, whether you realize that or not, we have used that and seek to use that in explaining how we would like to empower both department heads and the Governor to look at the most efficient and effective way to deliver IT services to business units in departments, and ultimately on to the Nevada citizenry, realizing that virtually all state-delivered services have an IT component somewhere or else among them.

And our use of the term, strategic sourcing -- David used it in his introduction and I used it as well in terms of describing what we were about -- is an attempt to use some term other than consolidation, which is susceptible to a meaning of -- that implies a total cost of ownership, what's the most effective way to deliver IT services approach, and would envision both a decision to consolidate along the lines that we have seen to date with DPS IT personnel becoming members of EITS under David's direction, but also would include the type of services-by-services consolidation that we have already begun.

David mentioned a couple of those. He talked about -- and the legislators with us today will recall that during the last legislative session, the budget director, midway through session, pulled out of agency budgets all separate funding for anti-virus software. And that was replaced with an enterprise buy of Symantec Endpoint and Network Protection Suites. And David gave you a little bit of overview about how we are successfully moving on that implementation.

The example of replacement of our core telephony switch infrastructure, both hardware and software, is another example of where we are gradually, without naming it, beginning to pull certain core services into an enterprise solution where we expect eventually multiple and increasing number of agencies to make use of them. The same is true of our cloud email and document production R&P. Right now not all state employees are on the state consolidated email system. A number of very large departments run their own email systems, and then there are a variety of different email systems in smaller agencies.

And what we're proposing, we've already moved in the direction of putting on the table a state-consolidated email platform, simply when the legislature approved in the last session expenditure of funds for a cloud replacement. And we're trying to encapsulate a terminology and a methodology that would allow us to build on those types of services where there's been some type of finding that the best way to provide them is across multiple executive branch agencies.

**Joe Marcella:** Let me repeat what I've heard or summarize what I've heard. Joe Marcella, for the record. What I've heard is, is that the proposal takes into account that there are strategic and nonstrategic components to a technology service delivery. Comes to infrastructure, communications, servers, security, in a very common, consistent fashion, tends to be more of a horizontal infrastructure. And what I'm also hearing is that you're allowing for the ability of each individual agency to leverage that, but preserve the vertical nature of their business, so that they can continue to deliver those things that are unique and specialized without having the brain damage, if you will, of the technology that actually provides those services. So strategically source the nonstrategic component of technology. Is that what I've heard?

**David Gustafson:** Dave Gustafson. That is what you heard.

**Joe Marcella:** Okay. Let me open it up to the Board for some questions.

**Mike Willden:** Mr. Chair, thank you. Mike Willden, for the record. I don't know if they're questions or comments or statements or whatever. But I've got five or six of them before I've got to head out. And I will need to noodle on this for a little bit. Now I understand your email to me, David. David and I exchanged a couple emails this last week, and I was like, huh? What? Huh? What? And I was like -- now I understand why we're going to lunch next week. So anyway, I...

**David Gustafson:** Who's buying?

**Mike Willden:** Probably me. Probably me. But not page numbers, but where you talk -- I'm in the long document to start with. And so just a couple comments. Where you talk about the chief of the Budget Division being the ex-officio Clerk of the Board. Just a comment, to me, I mean, the Budget Chief is one and the same as the Department of Administration Director, at least now. It's the same person. So we're going to have somebody as a Board member and the Clerk of the Board?

**Jim Earl:** That is correct. That person is one and the same. However, statutorily, they are distinct with different duties. Now, there's a particular statutory provision that specifically allows them to be the same person. And so we've got a problem in drafting and how this relates to another statutory scheme. And so the words that you see there are an attempt -- maybe not the best attempt -- but an attempt to take into consideration both the possibility that they are separate -- and in fact there have been some recommendations internal to the executive branch to...

**Mike Willden:** Right.

**Jim Earl:** ...to separate them -- as well as to accommodate the present situation, which might be extended in the future, where they're the same person. And quite frankly, in terms of the language which you read out that talked -- and I won't get the terminology exactly right even myself -- that comes from a description of how the chief of the Budget Division relates to another executive branch special agency.

**Mike Willden:** My comment in pointing that out -- and, you know, we do a lot of these. We generally have moved away from the ex-officio Clerk of the Board to more of a -- somebody's designated to provide the administrative support to the Board. And so just a comment or a thought there.

And then on the next page -- and, again, no page numbers. On the next page, where you define the five big directors and their five big budgets. I just think, you know, I don't know what budget means to you and means to other people. A lot of people just look at -- I don't want to sound technical, but Category 26. Then they look at Category 26 and budgets and say, "That's your IT spend." Well, that isn't our IT spend. You got lots of other places where money is spent. So you might -- we may want to define what's an IT budget. You know, I mean, I think we know who the big five are, but there might be a race in the future as to who's the fourth, fifth, and sixth or something like that. And so I just would want to be sure what we mean by five big agencies budget IT spend.

**David Gustafson:** And if I may, Dave Gustafson. And what we really wanted to capture here was if our budget's only 15 percent of the IT budget, how do we get the right people at the table to be advising the person who makes the decisions? And advising me on decisions of other people is not really germane and not really relevant. So how do we bring the biggest players together to advise the person who actually makes the decision?

**Mike Willden:** I get it. I just want to make sure we know how to count.

**David Gustafson:** I agree.

**Mike Willden:** Because, again, I don't want to dominate the discussion.

**David Gustafson:** Yeah.

**Mike Willden:** In HHS, we have Category 26 spend. We spend a ton of money in grant categories that we get federal funds for IT stuff that isn't in Category 26 and it's in other places. Or we have major contracts, like with J.P. Morgan and other people that we spend huge dollars on contracts that are up in Category 4 that aren't in -- you know, and so those are IT expenditures where we're buying a service from somebody else. So I just would want to make sure we're clear on that. And then I just, you know, an old friend, Ann Wilkinson, in the Governor's Office, said anything over 11 on a Board becomes too inefficient. So I don't -- we've got 19 on this one. I just would want to look at that to make sure that's the right players.

And then just a couple of technical things. We sort of interchange the use of the Division of Information Technology and the Division of Information Services. I think you mean Information

Services. But I see we probably have called it -- there's not two divisions, right? You have reference to two different divisions: Information Services and Information Technology.

**David Gustafson:** Dave Gustafson. And the intent here is to change the name. That if we're not going to be an enterprise service provider that we should take it out of our name.

**Mike Willden:** Right. But you intend to go to IS, not IT, right?

**David Gustafson:** Correct.

**Mike Willden:** There's both an IT and an IS in here. And Mr. Chairman, if you'd just indulge me for just a couple more minutes. The last couple comments I have is in switching to your other document, your short document. And so I want to make sure I'm really clear on this. And this deals with your 242.064 and your 242.065. If I think I heard you right, the HHS or whoever is going to have until 2017 to be in the club or out of the club. You used the term, I think, self-provide or join IS. And if I heard you correct that we have to -- if we're self-providing, we have to self-provide both common services and specialized services. So you have to be -- it's like the hokey pokey, you got to be all the way in or all the way out. You can't make a decision to provide common services and then ask for you to provide specialized services.

**David Gustafson:** David Gustafson, for the record. Thank you, Mr. Willden, for that opportunity. And the reason why the -- the other provision about the Governor is really important, because the Governor may direct those services which will be enterprise. So if the Governor decides everybody's going to get email, then we move forward with appropriations in our budget and the service offering of everybody's going to get email. We're trying to get out of the 45 services that we have, the billing, the accountability, all the accounting stuff that has to happen in a -- it creates a tremendous amount of overhead. And then when we go to provision services, sometimes we find the troubleshooting. Oh, it's not my network, it's your network, and so we spend days trying to sort out where the problems really are.

And, you know, I came back to my staff and I said, but you know what guys, you know what's really easy? When the Department of Public Safety IT has a problem, guess what? It's really simple to me. It's our problem. I own it and there's no question about it. The staff knows it. There's no debating it. There's no troubleshooting. There's no -- I call it the -- my friend calls it the triad of denial. It's everybody pointing fingers at somebody else. That's all completely gone, because you own it -- we own it, if you will.

And so if we're not going to have staff and funding to increase our footprint, if you will, to do some of these things, then we have to start shrinking the box. The only way I can shrink the box -- and remember back to my original opening statement here which is my number one priority is to advance information technology in the government. We spend a tremendous amount of time and energy trying to figure out whose fault it is and whose problem it is, and we don't have these people anymore to do that. So, if you will, I need to either own it or not own it, because it will make everybody's life a lot easier.

Now, one could ask, is that the right decision, yes or no? We can certainly talk about that. But the intent of this is to really start to let agencies do their thing. And, you know, I'll just close with this and then I'll be quiet. But some agencies are doing great things. And I can't be the guy holding information technology back because I can't secure funding or I can secure resources or I can't find the right contractor, or procurements are taking too long on my end, or what have you. I need to enable people, because my number one priority is to advance information technology. And if I'm in the way, then I'm going to get out of way. And right now I'm finding myself that I'm the guy in the way a lot of times because we don't have the money, we don't have the people, we don't have the authority anymore to get the job done. And so I'm trying to find a better mousetrap here, if you will.

**Mike Willden:** So, Mr. Chairman, I'll be quiet now. But I heard you say then it's all in or all out, unless the Governor says something different. So...

**David Gustafson:** That's correct.

**Mike Willden:** ...so common services, specialized services, you're all in or you're all out at 2017.

**David Gustafson:** Yes. And unless the Governor -- whatever services the Governor says everybody's going to get...

**Mike Willden:** Right.

**David Gustafson:** ...potentially.

**Mike Willden:** Thank you.

**Joe Marcella:** Additional comments? Kevin.

**Kevin Farrell:** Just a question. Within the common services or maybe specialized, is software development, new application development within common services? Because I'm not sure if that's just intended to be an infrastructure or desktop and mobile computing capability would mean application development.

**David Gustafson:** Dave Gustafson. I think it would depend on what it is. If it's a specific licensing engine for a specific board, then clearly that's a specialized service. If we find that there's a common platform, say, enterprise timekeeping system, well, then that would be more of a common services.

**Kevin Farrell:** Mm-hmm.

**David Gustafson:** So depending upon what it is.

**Kevin Farrell:** I'm just imagining an agency participating in the common and specialized services being all in...

**David Gustafson:** Mm-hmm.

**Kevin Farrell:** ...yet having an agency-specific application need. And do they still have the ability to develop their own apps?

**Joe Marcella:** Yes.

**David Gustafson:** Yes. Dave Gustafson. And that's the same thing with the Department of Public Safety. We just provide the manpower and they tell us what they want.

**Kevin Farrell:** That sounds like the business providing requirements, not them developing their own apps.

**David Gustafson:** That would be true.

**Kevin Farrell:** Okay.

**David Gustafson:** Did I contradict myself?

**Kevin Farrell:** Well, I think, yeah.

**David Gustafson:** Okay.

**Kevin Farrell:** Because what I'm asking is could an agency have its own software development team; coders, people doing testing, QA, rolling out their own software applications, if they're also participating in common and specialized services?

**Jim Earl:** Let me start off where we are. Right now we do application development largely for the Department of Administration...

**Kevin Farrell:** Mm-hmm.

**Jim Earl:** ...in the large enterprise applications we run, NEATS, NEBS, so on and so forth. We typically do not, at present, do applications development or patching for those applications that are run only within a single agency. And we would not seek to do those sorts of things in the future. And one of the things that that responds to is one of the comments that we heard from agency heads, when we talked about IT consolidation in the past, was that they did not want to lose the programmers that they controlled and were active in updating and modifying the applications that were critical to their agency's performance. And some department heads would say, well, it's okay if we outsource to EITS our email. But what we don't want to lose is we don't want to lose the application developers that are responsible for modifying our internal software, which is unique to our agency. Does that help?

**Kevin Farrell:** Yes. And I would think that that would be a strong selling point for those agencies considering jumping in with this.

**David Gustafson:** David Gustafson. And to me, it's really more about having IT staff that are accountable to the policies and procedures of the IT people, if you will, so we don't find servers under desks, we don't find servers in the wild that we don't know, you know, where they come from. And these are real events, unfortunately. And so, you know, to me it -- let's say you're an

all-in agency, it doesn't really matter to me if -- I mean, the IT people always report to business people somewhere, somehow. So to have our developers reporting to business people who are telling them what to do, matters not. But there's still accountable to the IT policies and procedures of the division so that we don't have rogue systems and programs running around and personally identifiable information on, you know, free servers and stuff like that. So I would just say that the IT staff would still report to IT, but they still would be accountable to the business.

**Joe Marcella:** Okay. Additional questions? Assemblyman?

**Assemblyman Bobzien:** Thank you, Mr. Chairman. And boy am I glad I dropped by today. No, thank you, Dave, for bringing this forward. And this is a very provocative discussion, obviously, and we will have lots more discussions. But I do think that, you know, overall, this is incredibly valuable to have this conversation going so that we're not doing this a year from now on, you know, the 120-day deadline. But in a lot of ways, I mean, this is the response to the challenge that many of us gave you last session, and so for that I'm very appreciative. And certainly the discussion we just had really kind of nails it. And I'll sort of share my legislative perspective about frustration with past application development projects, large project procurement, black holes, endless nightmares of money thrown after bad money, just, you know, on and on and on. And how you strike that balance is really the meat of this.

And that is, I think, the number one widely shared motivator for legislators to see some sort of consolidation go forward. Because it's always, well, how come this department didn't understand that this department across the street was -- you know, with similar business requirements, however in a completely different policy or issue realm, why could they not have gotten together to bring, you know, leverage their needs, get a better price, make sure that we were at a higher standard. And so, you know, I don't know if this right here solves that. I don't know if anything absolutely solves it. But, you know, that's what we're shooting for, I think, in a lot of ways.

And I think this is very telling that, you know, obviously a draft like this is going to produce some immediate clenching and holding back and some resistance. And so here is mine, just to validate everyone else's, and I don't have a right answer for this, but I just want to flag it. Because I think the more we can have these conversations and maybe put some of these issues to the side, by the time we get to session, the better off we're going to be. As I look at the list of the agencies, certainly if there are opportunities across this entirety of agencies for consolidation and, you know, being able to jump on a common platform, et cetera, and absolutely from a security standpoint, you know, if we can do it, great.

You have some very real constitutional issues here that you need to look at. I will give you my immediate legislative branch response that, you know, I'm thinking I'm not the only legislator that's going to be a little bit hesitant about turning over our information services to the executive branch. Just saying. And certainly, you're going to get a similar response from the Nevada System of Higher Education. Of course, I would be the first to say they may overdo it a little bit with that. But nonetheless, these are real issues. And so, you know, you have your business needs, agency autonomy needs that are real.

And certainly, you know, with Director Willden gone from the room, I can say that, you know, yeah, he's going to be your -- it's going to be a good lunch that you have. But nonetheless, for these other areas, because we've sort of identified it's either all in or all out, you may have to think about that, because for those constitutional hurdles, you know, there may be chances to say, oh, okay, this service is clearly one that could be provided across the entire enterprise of state government and does not run us into constitutional issues. You will have others where it's like, oh, email, shared document storage, I could see some people being nervous about it.

So I just want to -- again, I don't have the solution to that. I don't have even my own judgment as to, you know, where I would want to go on that. I'd just flag that as obviously that's going to be something that we should try to work to address, so that when we get to session, we have either a cleaner list that takes us out of that kind of jeopardy, or we have some ideas and some plans to address those hurdles.

**Jim Earl:** If I could respond just very, very quickly. Jim Earl. Right now one of the terms of art in existing statute 242 is the term using agency. Now, most of us, if we had to define the term using agency, we would think, well, a using agency is an agency that uses the services offered by EITS. That's not the definition of using agency in our present statute. The definition of using agency in our present statute is any agency that has a need for information technology services. So at present, NSHE, although it is not a using agency in the sense that we don't provide any services to NSHE; nevertheless, NSHE is a using agency under the definition of the present statute.

And if you look at what that means, David, at present, in a statutory sense, has managerial authority over all IT infrastructure at NSHE, because that's what the statute says. And David should be approving any purchase made by NSHE over \$50,000. Well, David hasn't done that and neither have the heads of DoIT for the past 50 years. And so one of the suggestions right on the front page of this is a red line through the definition of using agency. And so we're trying to eliminate some of the ambiguity that exists in the present statute. Although -- and from a statutory construction standpoint, it's not ambiguous at all. The statute says, hey, these guys are using agencies. This is what it means. And so David has this authority over using agencies, despite the fact that no such authority has been exercised for decades.

**Assemblyman Bobzien:** Mr. Chairman, if I might, just a quick response to that. Yes, absolutely. And since they're not here, but maybe perhaps someone is watching this hearing from NSHE. And if so, I'm sure I'll hear about it a little bit later today or tonight. Boy, talk about leveraging resources and getting a good package. If we could bring in all those .edu email accounts across the Nevada System of Higher Education and get a better price for the entire enterprise of state government, I'd sure like to see NSHE give me the constitutional argument for why we shouldn't try that.

**Jim Earl:** And if I could just follow up on that, one of the things that we -- one of the provisions that we managed to get into the existing NRS 242, not last legislative session but the legislative session before that, was the ability for EITS to bundle demands for services, software, and

equipment across the state, upfront, now. At present and even prior to that time, individual agencies at all levels of government, both local and county and municipal, had been able to take advantage of the contracts that EITS negotiated with a particular vendor. But that really isn't enough. What we need to do is we need to bundle all of that purchasing power at the front end, not at the back end. And so you negotiate a contract that is for two million Microsoft Office licenses instead of negotiating a contract for 10,000 that somebody else can then buy from.

Now, in our draft, that particular provision, which occurs in 242 as it exists right now, is moved out of 242 and is moved into the statute -- and I forgot the number of the statute -- that deals with either the Department of Administration or Fiscal Services. What we essentially wanted to do -- we didn't want to lose that ability to bundle upfront in advance of a negotiation. We simply moved it to a different place in the NRS scheme, so that effectively the head of the Department of Administration, who controls both EITS and State Purchasing at present, remains capable of bundling and negotiating on behalf of whoever wants to join a particular enterprise buy.

Now, unfortunately, we haven't been able to take advantage of that provision as applied to EITS in the last two budget cycles. And the reason for that is because we don't have the procurement people any more. And quite frankly, we don't have the bandwidth to assign a present member of EITS staff as an additional duty to go out and try and recruit to do, you know, buys. But I was very conscious of that particular provision, didn't want to lose it, but wanted to transfer it in a way that it could be implemented perhaps more effectively than we've been able to implement it to date.

**Joe Marcella:** Rudy?

**Rudy Malfabon:** Thank you. That's a lot to digest and definitely more discussion back at my agency. Just had a question about maybe the requirement under NRS 242.181, there's paragraphs and then it has a capital E with a circumflex punctuation mark. What is that? Is that just a reference that got lost in translation?

**Jim Earl:** No. No. What happens is that if you look very carefully at certain NRS provisions as they appear online, you will see that despite the best efforts of LCB legal staff, there are occasionally paragraphs that are not in a particular number or letter series. And in the printed statutes, there's very often a little arrow that indicates that that's a follow-on from the preceding paragraph. And that particular artifact, when picked up by Word, is translated in the particular way that you just described. So it adds no meaning, and if you look at it, you will simply see that it's a continuation of one of the paragraphs above it.

**Rudy Malfabon:** That's what I could see. That's what I figured, that it was just lost in translation from copy and pasting. So, thank you.

**Kevin Farrell:** Chairman, I know that we have more on the agenda to get to, but right now AAA is pivoting the entire company around customer experience. And it seems that we have an opportunity and I'm not sure if it needs to go into this BDR. But when it comes to citizen experience, mobile applications, I would suggest, need to be handled in a common, uniform user

interface, so that that citizen experience is well designed and uniform throughout. So I just offer that.

**Joe Marcella:** Now...

**Senator Mo Denis:** Chairman?

**Joe Marcella:** ...Joe Marcella, for the record. What is the -- oh, Senator, please.

**Senator Mo Denis:** Thank you. I just wanted to make sure -- I didn't know if we were going to move on and I wanted to make sure to ask some questions. And I appreciate all of the questions that have been asked. Many of those I would have asked, so one that my colleague, Assemblyman Bobzien, didn't point out also would be the court. Where it says the court administrator, I'm assuming that's the Supreme Court, which is another constitutional issue. But I think the one thing I just want to make sure I get out there is the -- the question was asked about the largest users and the definition of those. I'd be interested to see on that, how that would work out.

But, you know, having been an employee for the state in the IT Department or in IT for 17 years, I worked with some of the smaller agencies that had some IT people. I mean, what kind of input was received from the smaller folks? And I think you've answered some of the questions in, you know, what if they developed special programs and those kinds of things. But even things like desktop support and maybe talk a little bit more about the comment that was made that, you know, perhaps the IT people would be responsible to the business unit or to that agency, but fall under IT. Because I think that there's a lot of maybe smaller ones that don't have the huge departments like, you know, Department of Transportation and those, but that have current folks that are IT people. So can you talk about that real quickly?

**David Gustafson:** Dave Gustafson, for the record. That is really interesting. When we set off early on to sort of address this challenge we have -- and I'd also like to come back to Mr. Farrell's point -- I, as a central IT provider, need to find a way to get out of the shotgun weddings. And to my surprise, every session there is one person who will go to the legislature and blast me in front of, you know, god and country. And then I will go back and say, who are these people? What services do we provide them? And then more often than not, it's a free website or something like that.

And I'm trying to find a way that we can give people an option to opt in or opt out. If you want us to do those things for you, that's perfectly fine. Or if you don't, then you can do it yourself. And it's pretty simple to me. I've tried to, over the last five years of my career here in state government, tried to encourage people to use more centralized services, to do more consolidation, to save money so we can leverage economies of scale, and we can be a little easier on the purse. And people don't want to do that. What I do know is that doing what we're doing now is probably not going to work, not for the long run.

And when I look -- Jim asked me one time, he says, okay, well then when we start talking about strategy and where we need to be, let's talk about the forces of the world and where are they going? I said, well, it's very simple. I mean, when you look at cloud technologies and strategic sourcing and everything, the world is decoupling. It is not consolidating, it is decoupling. It is decentralizing, if you will. And so, I said, okay. So when we look at all these cloud options, whether it's whatever your favorite piece of software is, right? They're all decentralizing in a way.

The strategic sourcing is allowing agencies to sort of outsource pieces of their IT, whether their infrastructure, whether their applications, whether their programmers, whether their server guys or helpdesk or desktop, whatever they may be, cloud is sort of this enabler of decentralizing. And I said, okay, well then why are we still beating on the dead horse of trying to get people to consolidate then? Because of those agencies that want to join our team, if you will -- you know, I can't remember how Mike put it, but it's something to that effect -- then we're going to be doing exactly that. I'm going to find the businesses that we no longer need to be in and I'm going to start outsourcing those. But I can't continue to fight everybody, especially with shotgun weddings. I just can't do it. It consumes too much of my time and my staff's time to do that.

Let's get back to my Public Safety comment earlier. If Public Safety has a computer that breaks or a hard drive that dies somewhere, we don't have to worry about who to call. We already know who to call. You can look at the guy in the mirror every day. You already know exactly who you need to be calling. And so it's really simple, it's really fast. It's actually faster for us and more efficient for us to deploy information technology services because we already know who to call. And a lot of times it creates a lot of delay in service. It creates a lot of staff time. And ultimately ends up the cost per resolution is actually greater, because we spend more time trying to figure out whose problem it was. And I just don't think that's an efficient way of running government.

And so, I'm sorry Senator Denis, I probably went off rambling there. I probably didn't even answer your questions. But that's sort of my take on this. And we're trying to find a better way to build a mousetrap. And I'm not saying this is the right way. And I think, you know, Assemblyman Bobzien sort of said this earlier, this is kind of a provocative throw here, and I know that. The whole point of this is to really start the conversation. Let's throw it all out there. I am -- people didn't want the Plan A, so I'm going to Plan D, E or F over here, and let's throw this out there, and let's see what happens. Because I am convinced though, that what we're doing now is not the best way to move forward. And if we do nothing, if I don't throw a big splash in the pond somewhere, we're going to continue to do the same thing over and over again. And that, I don't think, is healthy for our residency. Senator?

**Senator Mo Dennis:** No, and I don't disagree. I think it's great to throw it out there, because then we can have those discussions. And because, you know, as Assemblyman Bobzien said earlier, you know, I mean a year from now, to try to have this during the 120, that, you know, it won't work. It's got to start now. And we've got to make sure we've got input from all the folks so that we can get it all worked out by the time we get there. But, you know, we obviously need

to do this. And we just need to figure out a way that we can get everybody to understand what it is. Because I'm sure a lot of people will see one little provision and say, well, what about this? And then that's the only thing they'll focus on. But I think this is -- I mean this is, I mean, great, because you're just throwing everything out. In a perfect world, this is what we would do. And then let's figure out what, you know, what in actuality we can get to work. And, you know, so I appreciate you putting this together, because I think it definitely will get the conversations going. Thank you, Mr. Chair.

**Joe Marcella:** Please.

**David Gustafson:** Mr. Chair, let me go ahead and answer Mr. Farrell's question and one of the reasons why I'm starting to talk about mobile apps. So as we look at things that we should be doing -- I go to NASCIO every six months -- I know what we should be doing. And we're not allowed to be that flexible. Our budgets are fixed. Our personnel is fixed for two years at a time. The world changes faster than we can adapt.

And so when I get back as a state CIO and I think about what is the best way for our government to move forward? Is it through me or is it around me? Because if I -- and this is something I've struggled with through my government service here -- that is, if I can't be flexible and agile to meet the needs of my business, my customers, then I need to get out of the way.

And so agencies come to me and they say, hey, we want a programmer to work on mobile applications. And the short answer for me is, I don't have it in my budget. It was never contemplated. I have no staff. And you can come back two years from now and I'll maybe, if god willing, maybe I'll have something in my budget that I might be able to throw at it. But agencies will come back and say, but I have this federal money or such, and so what I'm trying to do now is say, okay. So the world that I live in is very rigid. It is not flexible. It is quite the opposite, more like concrete. And so how do I enable agencies to do some of these things that everybody should be doing? And in some cases, I just have to let it go. And there is a little bit of a hope and a prayer behind some of these, because you are going to find areas of excellence. Some agencies are going to really excel, and agencies won't. And that's sort of the risk that comes with this proposition. But at the same time, I feel that that risk is worth taking to enable agencies to get some of those things done, because mobile is one of those things -- we should have a heavy investment in mobile infrastructure and we have very little. So, I apologize for the rambling.

**Joe Marcella:** Joe Marcella, for the record. One of the things or all of what I've heard today is that what you're looking for is, one, support from the ITAB Board. You also want to give us a little bit more authority -- or raise it to a level of awareness where -- or authority where folks -- not only the participants, but the folks that receive that information can act. The other thing that you mentioned over and over again, but didn't quite say it, is that there are a lot of different services that need to be provided. And they can't all be provided by your agency, but consistency across the board. A level of cooperation and enabling legislation could help get us closer to those goals. And at this point, Mr. Earl, we can't vote on anything and I can't make a

recommendation, but we can have further discussions. I'd like to hear your recommendation for our next ITAB Board and also for consideration of what you proposed today.

**Jim Earl:** Jim Earl. My recommendation would be that Board members, after having listened as attentively as you very obviously have, reflect on the basic proposal. You've got a little more time to go through the line-in/line-out version and understand where we're recommending certain provisions be placed and why we recommend certain provisions be deleted or added. I think that it is open to any ITAB member or indeed any legislator to write to David and to me during the interim between now and our next ITAB meeting, with issues that you'd like to have us think about or prepare a response in advance or whatever, so that at our next ITAB meeting we'd have perhaps a more fuller discussion not only of what we put on the table -- because David and I fully realize that, you know, we live with this stuff, if not every day, then at least every other day, and we're asking people to take our work product in a very condensed form.

So we could have a discussion next ITAB not only around what we put on the table, but on any possible changes, modifications, going from drafting to a philosophically different approach at the next ITAB meeting. And to the extent that we can exchange information between now and then, I think that would be something certainly that I would want to encourage.

**Joe Marcella:** Mr. Earl, could I ask you to be the point of contact?

**Jim Earl:** Yes, indeed you can. And my email address is jearl@admin.nv.gov.

**Joe Marcella:** Thank you. Any other recommendations from the Board? Additional discussion? Let's move on to the next agenda item. Thank you very much for your presentation.

## **8. PERSONNEL SALARY STUDY AND RECOMMENDATIONS - Amy Davey, Deputy State CIO (for possible action)**

**Joe Marcella:** Ms. Davey?

**Amy Davey:** Yes.

**Joe Marcella:** You will be presenting?

**Amy Davey:** We're going to be talking about IT Workforce Improvement. I have a very short presentation for you this afternoon. And I don't use the word consolidation once. So we should be on safe ground. We can just plow right through this.

When I came to work in IT a few months ago, I was issued an iPad, so I want my boss to know I have my iPad with me at the table. But in HR we usually carry around policy manuals -- great big policy manuals. So I also brought my notes with me because I find that I'm still shaking off those habits.

So good afternoon, Chairman, members of the Board. Thank you for your time today. And in the 2013 session, members of the Nevada Legislature urged us, during our budget presentation, to address workforce improvement. So this agenda item addresses this request and continues the

theme you've been hearing this afternoon regarding proposals for next session; specifically, modernizing our staffing model and improving our ability to attract the technology workers we need to move the state forward.

We have two objectives: to benchmark our IT personnel compensation with a goal of being more market competitive; to propose IT professional level positions within EITS become unclassified. I'll tell you a little bit more about each of those two proposals.

The Division of Human Resource Management within the Department of Administration supports these proposals and has partnered with us, Enterprise IT Services, in purchasing an IT professional compensation report from Foote Partners, a research group specializing in IT salary data. Included in this report are job descriptions that allow us to closely match our employees' duties, skills, and qualifications and salary information for select geographic regions that are comparative to our own. We have targeted in this report, Las Vegas, Sacramento, Salt Lake City, Portland, and Denver as relevant comparisons for the Reno area, all western region cities, including some state capitals. We will also use data for local government IT wages as we make our comparisons.

Most IT personnel -- moving on to our second proposal -- most IT personnel within the executive branch are in the classified system, within multiple classifications, such as IT Professional, Master IT Professional, IT Manager, IT Technician. In many cases, these classifications have not been reviewed or updated for several years, some since 2006. The current state IT job classifications are not reflective of changing technologies and expanding and contracting IT market demand. Therefore, we propose to take our IT professionals and IT manager positions into the state unclassified service. This would equate to approximately 62 percent of EITS staff. And as you can see when you get into our proposed PDR language, would not include clerical or administrative support positions or IT technician positions. Additionally, we will align our positions with the Fair Labor Standards Act, as it relates to employees in computer-related occupations.

Moving our professional staff into the unclassified service assists us in the following ways. With recruiting difficulties it helps us attract and retain employees with the skill sets necessary to support state infrastructure and to advance business technology. It promotes hiring flexibility and speed by allowing us to specifically tailor job announcements and requirements and allow those with IT technical expertise to drive the hiring process. It allows us to modernize job descriptions and identify required skills and qualifications. It allows us to address pay flexibility by supporting our ability to match compensation more closely to qualification skills and agency requirements by utilizing the entire pay range. So in the unclassified service we have a pay range up to a maximum amount you're allowed to pay. It helps us modernize our -- oh, I'm sorry, let me skip over that one. It allows us to adjust salaries then in response to increased responsibilities and accounts for changing requirements in the workforce. And it encourages continuous engagement and enhances professional accountability in our organization.

There are existing models for organizations in the executive branch that are largely staffed by unclassified professionals, such as the Department of Tourism and Cultural Affairs, the Gaming Control Board and the Attorney General's Office. And in the 2009 legislative session, the State Public Works Board moved their professional public works project managers into the unclassified service. I want to assure you that we are and will continue to work hand in hand with state human resources to properly develop these salary and staffing proposals within the state system. We have some preliminary data on our early analysis regarding IT salary within state service. I'd be happy to discuss that if you have any questions about that. Though I know, in the interest of time, I'll allow your questions to direct where you'd like to go from here. So please let me know if there are any questions or recommendations from the Board.

**Joe Marcella:** Any recommendations from the Board? Any questions from the Board?

**Kevin Farrell:** Well, just generally, are the state salaries lining up as average, as below average? Where do we sit?

**Amy Davey:** Amy Davey, for the record. So we are looking at a variety of positions, everything from security to desktop support to network administrators to system administrators to programmers. And what we're seeing is that by and large we are under market, in some cases fairly significantly. You heard the gentleman from Deloitte speak earlier about the market demand for certain IT professionals, in that case, security professionals. And so we see that in many areas, we're quite a bit lower.

We're not attempting to fix all of those. We understand that there's -- you know, the state has been going through multiple years of recovering from a serious economic and budget situation. And we're not attempting to outpace or even necessarily draw, even with private industry, but we would like to be a little more market competitive for our market and in our location so that we can continue to move things forward. We can continue to hire and retain people and train people and -- yes?

**Joe Marcella:** Joe Marcella, for the record. The move from the classified environment, is that to provide a new skills inventory, more flexibility within the organization, and the ability then to hire in particular to what the business needs are as well as how -- I'm hearing that David needs to adjust his backroom regardless of what legislative changes we make. What does moving to an appointive exempt status do for the organization?

**Amy Davey:** Amy Davey, Deputy CIO. Yes, I believe it will address all of those elements to some degree. Additionally it allows us to be -- what I don't -- moving to the unclassified service doesn't change our budget account structure. So it doesn't change our ability -- we'll still need to work within our budget account structure and within the requirements that we have in terms of being an internal service fund, but it does allow us some flexibility.

Right now with the number of IT classifications, with the age of those classifications, with the changing needs in technology, it's just not really effectively addressed in our classified system. It's not effectively addressed in our recruiting processes, and in the unclassified service you have

more pay flexibility. Up to your budget approved amount, you can say, this individual skill set -- it costs more to hire a Java programmer than it does another type of programmer. It costs more to find a Unix system administrator than it does to find a Windows system administrator. And it gives us the ability then to react a little bit to those kinds of requirements -- what the market requires for IT skill sets.

**Joe Marcella:** Along with that will there be a revised organizational structure?

**Amy Davey:** Our organizational structure -- we're always revising to meet the demands of our customers. Yes. The short answer would be yes. And we're only looking at the professional level series. So we're not talking about our technicians. We're not talking about our support staff. Those are appropriate for the classified system. We're talking about the IT professional and higher series, master IT professionals, IT managers, which we have a lot of in our organization because we're an IT organization. But, yes. Thank you.

**Joe Marcella:** Part of what I'm getting at is that there needs to be a foundation for the definition of who these folks need to be, what their skills should be...

**Amy Davey:** Oh, absolutely. Yeah.

**Joe Marcella:** ...and what direction the organization is going, and how these folks will help you get there.

**Amy Davey:** Absolutely. And, you know, we intend to develop a very comprehensive program around this. There are other state agencies that are primarily unclassified. So if you look at the Gaming Control Board, I believe almost all of their personnel are unclassified, with the exception of their clerical. They've developed a very good, a very robust internal policy, HR policy system that reflects who their personnel are, what their staff are. And so we absolutely would be the same and follow along in that regard.

And additionally when, you know, when people, when you move positions from the classified to the unclassified service, employees always have the option of remaining in the classified service. So it's up to the employee when a position changes, if they wish to change in to that position or stay in a classified position.

**Joe Marcella:** I would tend to agree. IT, contrary to popular belief, is not an exact science and it's consistently evolving. And it takes folks to make those things happen. Can we move on to the next agenda item? Are there any questions?

**Amy Davey:** Thank you.

**Rudy Malfabon:** Just definitely know what you're talking about because we've faced those challenges with the -- the personnel system tries to have a one-size -- a practical, but one-size that fits for several departments, and sometimes it's difficult. So we've run into those challenges with the classified system.

**Amy Davey:** Thank you.

**Joe Marcella:** Thank you very much.

## **9. COOP/INFORMATION SECURITY UPDATE - Chris Ipsen, State CISO**

**Joe Marcella:** Mr. Ipsen?

**Chris Ipsen:** For the record, my name's Chris Ipsen. I'm the chief information security officer for the state and it's my honor to be here. And I have two commitments to you. One, to be quick, and, two, to be positive. You know, a lot of times when we talk about security, it's a negative paradigm. And I can't help but -- and I'm going to deviate from my second commitment to you, or maybe it was the first -- just to make a quick...

**Unidentified Male Speaker:** That was fast.

**Joe Marcella:** There has to be a story.

**Chris Ipsen:** Well, there is. You know, I was listening to the story around consolidation and all of the challenges that we face. And I think they're all very real. And it's what we live with every day. And if I could use my own best practices, when I start out a presentation, you start with the good stuff and you recognize that the rest of it may not be heeded as closely. Two things that I take away from that, and as we discuss consolidation and the methodologies moving forward -- and having been the enterprise architect for the state, I also am mindful of the opportunities of enterprise buys and the consolidated approach and a unified vision. I'm absolutely committed to that.

When I went to security, there's a little bit of a different discussion that needs to be had, and I haven't heard it, and I think it's my responsibility to bring it out. Is that if we do an enterprise buy -- which we did with Altiris, and it's been hugely successful -- what we do is we end up saving money and we standardize our approach. That's a really good thing. When it comes to security, our motivator is avoiding bad outcomes, because the state is always responsible. We talked about NSHE or NESHE [sic] or however we refer to it. If there's a breach at NSHE, who pays? The state does. If there's a breach in the legislative branch or in the courts or wherever, the state still pays. So when it comes to security, I think it's important for us to capture the understanding that we're trying to avoid bad outcomes for everyone.

And the way that we do that or at least the most successful methodologies -- this is that important thing that I was talking about that we have to take away -- one of them is we need to standardize to best practices moving forward, those that avoid risk. So irrespective of where you are, we need to be able to say what it is. We need to be able to communicate how we do it. And we need to be able to measure it. And then the second thing we need to do -- and this is a hard thing to do, but I recognize it's absolutely essential -- who's responsible? You know, what is that triangle thing we heard earlier, you know, pointing the fingers. Well, we need to have somebody who's responsible for the outcomes, because if we don't do that, we don't have security. And with that I'm going to give you some examples.

And I'm going to jump to -- with the fact that I've deviated from my discussion, I'm going to jump to the middle part of my discussion and give you one statistic, and that is that our continuous monitoring program for the state has been extremely successful. And I have got the statistics to prove it and the metrics to prove it moving forward. One of the most interesting ones is that the legislature, a couple of legislative sessions back, mandated that agencies, within 24 hours, report into a central entity -- the Office of Information Security -- incidents or suspected incidents within 24 hours. That reporting is happening. However, more than 99 percent of those reports are not coming from the agencies in, it's coming from our monitoring program out and then in. So what I mean is, we're seeing it first, because we have a standardized approach, we've developed infrastructure moving forward that measures what an incident is. We're actually seeing it on the wire and we're able to do something about it. I'm going to share with you -- I'm going to save it to the last. You know, I've been listening to a little bit of radio. I'm going to save the best for last in my presentation today.

But our continuous monitoring program continues to move forward and it has tremendous success. What we are doing is we've taken a grant from the Department of Homeland Security. And over the last four years, we've gone from -- I should say seven years, from being literally shunned from the meeting of the Commission of Homeland Security, because how dare we in cyber security, challenge the authority of or the necessity of, you know, police and fire and so forth. And I don't mean that negatively, because police and fire are our most avid supporters now, but to a time when cyber security was nonexistent to a time now where, this last year, this is one of my key updates, the Commission of Homeland Security for the State of Nevada has listed cyber security as the number one priority. This is a commission that's chaired by the Governor of the state, has on its commission the sheriffs from both north and south, air guard, national guard, the Nevada National Guard, and other key -- Airport Authority, I mean, significant people. We recognize that we have an issue and we've actually been able to secure over \$2 million in grants over the last three grant cycles for cyber security. So I'm really excited. That's one of the positive messages I'm here to tell you about.

Some of the things that we've received grant dollars on are continuity of operation business impact analysis in the south. We've also had access management. We've started to discuss that issue. Continuous monitoring and statewide assessment -- we're finishing that one up, we've deployed it and we're beginning to see results. We're augmenting existing infrastructure and common approaches. We're also seeing the first vestiges of a statewide cyber security operation center. So feeds will go into the counties and cities, a common methodology for measuring what's happening in our state. Extremely exciting. Federal dollars being used and we're able to leverage it on behalf of both the state and of the other governmental entities, including the counties and cities, so that we can begin to standardize our methodologies and begin to provide some very relevant feedback to everyone involved as to what the cyber posture of the state is.

This last grant cycle we were able to secure funding, most recently as the number one priority, by 20 percent, money for firewall optimization, kill chain technologies -- that's kind of a cool name and I can tell you about that at a later date -- intrusion prevention software and also services for both the entities and also outsource services as necessary. Also received a grant that

we're maximally utilizing around centralized logging. So we got a grant. We're also able to leverage, through healthcare reform, an expansion of our Splunk infrastructure for consolidating our grants. And we've also been able to extend that into one of counties and cities. So a standardized approach. So we have opportunities. We come up with an idea. We say this is a good way to go, and everyone is beginning to go in common directions. So we can compare apples to apples and oranges to oranges. And then we've also been able to extend our grants into an incident response capability. So once we determine that there's a problem, the next practical question that people say is, what do we do about? So we're actually deploying an incident response methodology.

All right. With that, I'm going to move into the functional aspects of the state. With this common strategy moving forward, we mapped it to the federal guidelines. Since we spoke last the White House has come out with a presidential directedness to come up with a cyber security framework. We're absolutely in line with that framework. We're also in line with the DHS maturity model. So we're doing our things in a manner that allows us to leverage grants, ask for grants, but then also when our agencies, like Health and Human Services, I wish Mr. Willden was here right now, because he has to comply with BSMA and other federal requirements. We're mapping our strategies to the federal strategies so that when they go to ask are we compliant, there aren't two different regulatory agencies that we're working with. We're working on a common hymnal. We're singing from a common hymnal. So this really talks to a unified approach moving forward.

What are the key initiatives that the Office of Information Security is doing and what's the relative status of those right now? Well, as I mentioned earlier, we have an Altiris program going. I know that the legislature asked us when we were doing it, one of the most poignant questions I was asked at the Interim Finance Committee was how do you intend to be successful with this, given the decentralized nature of the state? Well, I'm here to say that over a third of the state is now integrated into our Altiris system. Over 5,000 endpoints from nothing about a year and a half ago. We're now up to 5,000. We had a systematic approach. We have a centralized methodology for building this out. We're giving agencies the capability to manage their own environments. But then we're able to gauge how they're doing against the whole. So we're building -- we're giving them the tools.

This is -- you know, I heard Winston Churchill's granddaughter give this speech at a NASCIO conference. And she said, "My favorite Winston Churchill line is -- my favorite from my grandfather is, 'Give me the tools and I'll finish the job.'" Well, that was the approach we took with Altiris. How can we set policy if we know there are agencies out there that don't have the tools to do the job. How can we say you have to secure your environment when you don't have the tools to do the job? Well, these are the tools to help them do the job. And it also helps them do a number of other things, which builds towards maximum efficiency. So our performance metric was how quickly could we make antivirus for the cost of antivirus? We provided them with the industry standard desktop management suite, analytics, and other capabilities. We're over a third of the way there. Huge success story.

And I'm really proud of my staff. They're doing a fantastic job going forward. And above and beyond the call of duty, to do things that -- sometimes -- there's always pushback. When you create change, there's pushback. And they're doing a great job. And they're winning over people by the successes as we go. So I'm just really tickled. We're applying a few more resources. We didn't get it completely right, so we're looking to apply personnel so that the system is sustainable. But the bottom line is that we're moving forward and that it's extremely successful to date.

A second component of the strategy of the Office of Information Security, for which I'm responsible, is the continuous monitoring. We've got a solution where we standardized the approach using Altiris. And then we come back in on the backside and say that's for the things that we know about. And then for the rest of the environment, how do we validate those things that we don't know about or those things we assume are done correctly? So our continuous monitoring is going out and systematically scanning the state infrastructure -- three million miles, tens of thousands of endpoints, server farms and connections -- against the bandwidth limitations that we have. So we're systematically moving out. That too is moving ahead swimmingly. We've got -- almost all of our environment, we're looking to extend it out so we can optimize bandwidth. Additionally, we're also extending that service out into the counties and cities, so that they can do the same thing that we're doing, and that was through the federal grant. So that's a huge success story.

How are the metrics, the incidents that we're seeing? Well, what we have seen, and I don't know if you remember from the last presentation, but we talked about a curve of incidents going up that precipitated our call to action around Altiris. What we saw was that there was an alarming rate in increase occurring, which caused us to do something. We had to do something moving forward. Well, I'm pleased to announce that those from the measuring point of our border gateway firewalls, that number has been dropping precipitously since we deployed the solution. And we deployed continuous monitoring to the extent to where we're beginning to tighten the noose around the state infrastructure. We're starting at the gateways where we interface with the internet and we're working our way closer to the data. These controls are beginning to reduce the amount of incidents that we're seeing out on the perimeter and we're moving them in closer and closer and beginning to categorize and manage them.

Without getting in the weeds, what I can say is that we're looking more, we're seeing more, but the outward result to the internet is sharply reduced, and that's a really good thing. To the extent that for the very first time -- this is probably the most important thing -- I have many other things to talk about, but I'm going to be brief. For the first time -- let me take a step back. Normally, when we talk about an incident, we see someone respond to a phishing email -- someone sends an email and it says click on this. And they do to the extent of about 80 percent of the time, most people -- and the sophistication of phishers now are -- most people will click on this thing. So when they click on this, something happens. Usually, if they have administrative privileges, which we're trying to reduce with Altiris, but if they do, then software gets installed and then it tries to phone home. We see the phone home. We stop it. So something happened and we stop it as it's going out, hopefully. For the very first time, we saw it and we were able to catch an

advance persistent threat, in our environment, before it called home. That is huge. To know that we have one and that we were able to catch it.

And the way we were able to catch it is back to the thing I started with. And I promise to put a big bow on this. We talked about how do we standardize our approaches? Well, because we deployed the solutions that we have, we had 90 days of historical records of where endpoints were talking and we also had a larger base from our partner, Symantec, and others, (inaudible), that we know where the bad sites are. And because of these low bandwidth connections, we were able to see that something existed without it actually doing a bad thing. So we were able to catch something before it did something bad and --

I don't, you know, it's kind of geeky for me to say this. But it's really cool when you see a plan come together. It's starting to come together. And there are many threats out there. I just looked on the news today. Chinese spies are being prosecuted for cyber espionage. If you go on Google News today, very top story. And it's every day we hear the bad news. Well, I'm here to say that it's still bad news. We are not without our risks and we need to be mindful of those. But we're doing better. And the more we work together, the better things are going to be.

So with that, I'll entertain any questions you might have, knowing it's the end of the day and it's 4:00. I'm sorry, I probably went a little longer than I should have.

**Joe Marcella:** For the record, Joe Marcella. You need to be congratulated on your inroads, also for paying attention to security, and obviously being able to get everyone's attention across the enterprise. That's huge. And it's a good beginning. So, one, thank you for your presentation, again, and certainly appreciate it from a state perspective. From a local entities point of view, the state taking a parenting or lead position, particularly on continuous monitoring and identity management, as well as being a participant in contingency planning is not only appreciated, but long overdue. And I think it's helped in the south as well as in the north. So again, that's another thank you. Any other questions or discussion? (Inaudible) --

**Chris Ipsen:** I just want to say thank you on behalf of my staff. They really appreciate it. You know, they're the quiet people in the background that do all the work. And they do a lot of it. There's a lot of work to do. And you don't get to hear about them. I just want to say that they do a fantastic job and I appreciate that, Mr. Marcella.

**Joe Marcella:** Thank you.

## 10. PUBLIC COMMENTS

**Joe Marcella:** This is a public meeting. I wanted to open it up for public comment. Is there anyone in the south, besides you, Senator?

**Senator Mo Denis:** No one's coming forward.

**Joe Marcella:** All right. Thank you. Anyone up north that would like to speak? Hearing none, seeing none, I'm going to close it for public comment.

## 11. ADJOURNMENT

**Joe Marcella:** Can I have motion for adjournment, unless there's some miscellaneous comments or questions? Motion?

**Rudy Malfabon:** So moved.

**Joe Marcella:** Second?

**Kevin Ferrell:** I second.

**Joe Marcella:** In favor?

**Group:** Aye.

**Joe Marcella:** Thank you, everyone. It was a long meeting. I appreciate it.

---

*Notice of this meeting was posted before 9:00 a.m. three working days prior to the meeting pursuant to NRS 241.020, in the following locations:*

Legislative Building, 401 N. Carson St., Carson City, NV 89701  
Blasdel Building, 209 E. Musser St., Carson City, NV 89701  
Bradley Building, 2501 E. Sahara Avenue, Las Vegas, NV 89158  
Carson City Court Clerk Office, 885 E. Musser, Carson City, NV 89701  
Washoe County Courthouse, Second Judicial District Court, 75 Court Street, Reno, NV 89501  
Nevada State Library and Archives, 100 Stewart Street, Carson City, NV 89701  
Grant Sawyer Building, 555 E. Washington Avenue, Las Vegas, NV 89101  
And the following web locations:

[http://it.nv.gov/Governance/dtIs/ITAB/Information Technology Advisory Board \(ITAB\)/](http://it.nv.gov/Governance/dtIs/ITAB/Information_Technology_Advisory_Board_(ITAB)/)

<http://www.notice.nv.gov>

The appearance of the phrase "for possible action" immediately following an agenda item denotes items on which the Board may take action.

We are pleased to make reasonable accommodations for members of the public who are disabled. If special arrangements for the meeting are required, please notify Lynda Bashor in advance at (775) 684-5849 or you may email your request to [lybashor@admin.nv.gov](mailto:lybashor@admin.nv.gov).