*** NOTICE OF PUBLIC MEETING ***

INFORMATION TECHNOLOGY ADVISORY BOARD

LOCATIONS:

Legislative Counsel Bureau 401 S. Carson Street Room 3137 Carson City, Nevada 89701	Grant Sawyer Building 555 E. Washington Avenue Room 4412 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: August 11, 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: (Inaudible) now to order.

2. ROLL CALL (For possible action)

Joe Marcella: Would you please take the roll.

Lynda Bashor: Assemblyman Anderson?

Assemblyman Anderson: Here.

Lynda Bashor: Ernie Capiral?

Ernie Capiral: Here.

Joe Marcella: Welcome, Ernie.

Lynda Bashor: Senator Denis?

No response heard.

Lynda Bashor: Director Diflo?

Director Diflo: Here.

Lynda Bashor: Kevin Farrell?

Kevin Farrell: Here.

Lynda Bashor: Laura Fucci?

No response heard.

Lynda Bashor: Director Gilliland?

Director Gilliland: Here.

Lynda Bashor: Director Malfabon? And my understanding is he will be late, Joe.

Joe Marcella: Okay. Thank you.

Lynda Bashor: Joe Marcella?

Joe Marcella: Here.

Lynda Bashor: Director Teska?

Director Teska: Here.

Lynda Bashor: Joe, we do have quorum.

Joe Marcella: Welcome, Julia.

Director Teska: Thank you.

Joe Marcella: Am I supposed to be able to see the dais up there? Because all I think I see is Jeff, and that's because I'm old and I can't see that far.

Jeff Menicucci: I can certainly move if it makes it easier.

Joe Marcella: Okay.

3. PUBLIC COMMENTS

Joe Marcella: No response. Yeah. All right. Let me open the meeting up for public comments. I have some folks in the audience in the south. Do you have anyone in the audience up north? Does anyone want to speak?

Lynda Bashor: No one in the north, Joe.

Joe Marcella: No one in the south? Nobody's popping up, so I think hearing none, seeing none, please close the meeting for public comment.

4. APPROVAL OF MINUTES: May 19, 2014 (*for possible action*)

Joe Marcella: I'd like to see if anybody had any issues with the minutes. Call for a motion to approve the minutes from our last meeting.

Kevin Farrell: I move to approve. Kevin Farrell.

Joe Marcella: Thank you, Kevin. Second?

Ernie Capiral: I move to approve. Ernie Capiral.

Joe Marcella: No discussion. All those in favor?

Group: Aye.

Joe Marcella: All right. Good. Thank you. May minutes approved.

5. INTRODUCTION OF THE ITAB MEMBERS

A. Romaine Gilliland, Director, Department of Health and Human Services

Joe Marcella: Let's move on to the agenda item. It's introduction of the ITAB members. Romaine, I appreciate you not only doing this, but being here today. I also appreciate the fact that there is someone with your level of talent and expertise -- I read your bio -- to go ahead and take on human -- sorry, Health and Human Services. It's a big job, and you're so integrated with what we do from a technology perspective, as well as what EITS is responsible to deliver. I think it's paramount that not only do -- you're on the board, but a little bit of background would be very interesting for all of us. So if I could trouble you to go ahead and give us some of your background and maybe some of your intent and direction, it would be very helpful.

Director Gilliland: Thank you very much. I appreciate the introduction and it's an honor to be here. And, again, as you're aware, I took on the position of Director for the Department of Health and Human Services six or seven weeks back, when the prior director, Mike Willden, was moved on to chief of staff. Mike, having been in this position for 13-14 years, it's very humbling to be asked to take on a role for someone who is as well respected as he is. I think it's also a testament to Mike's leadership skill and the leaders that he surrounded himself with that were able to move forward and continue. I think we have a great staff in the Department, and I think it's a testimony to Mike as to -- for the staff that he managed and he was successful in putting together.

Personally, I'm a graduate the University of Nevada, Reno. I'm a licensed CPA. I've been in the private sector most of my life up until about 10 years ago when I came to work at the Division of Welfare and Supportive Services. I was the administrator for the Division for several years. One of the largest users of the state IT services. And so, again, it's a pleasure to be here and I hope that I'm able to contribute to the group.

Joe Marcella: Mr. Gilliland, I really appreciate you being here and welcome. Thank you. If I could trouble Julia Teska to just give us a little bit of background as well. And I didn't want to leave you out and I appreciate it.

Director Teska: No problem. Like Director Gilliland, I've been in my position since April of this last year, but I've been with the state for 11 years and in government service for about 22 years, mostly on the financial side. The last few positions I've had, the last several years, that has also included responsibility over information technology and I've done some project work in my work at the Budget Office with projects related to our budget system. I also am very happy to be here. I think this is a crucial element of state government. I see it as, essentially, we are three things. We are the people we hire, we're the technology and we're the facilities that we have to serve our citizens; and so this is one of the, to me, the three most important things that we do in government. So just happy to be here and I hope to contribute as much as I learn in this process. Thank you.

Joe Marcella: Well said and welcome. Ernie, can I ask you to just give us a little bit of background?

Ernie Capiral: Absolutely. I've been the chief of IT for the Nevada Attorney General's Office since 2011, and I've been with the AG's Office since 1993. So I've been in there since we didn't have any networks from the ground up, and I love the job and I've been there ever since.

Joe Marcella: Did you love the job before the networks came in or after the networks came in?

Ernie Capiral: Both.

Joe Marcella: I see. Welcome.

Ernie Capiral: Before was nice; after was still nice, but more hectic.

Joe Marcella: Yeah, that's the only reason I'm gray. I'm actually only 27 years old.

Ernie Capiral: You look good for 27.

Joe Marcella: (Inaudible) technology (inaudible) working well.

6. CIO UPDATE (for possible action) Presented by David Gustafson, State CIO

A. Feedback, and additional requests for Board recommendations, on BDR changes to NRS 242

B. Update on unclassified/compensation initiative

Joe Marcello: All right. Let me move on to the next agenda item, and it's a CIO update. And, David, I think you're on board. Well, I'd like to hear a little bit about what we want to do with

the BDR, and the second thing is, is we'll talk a little bit about a little compensation in your unclassified.

David Gustafson: Thank you, Mr. Chairman. Dave Gustafson for the record. I want to start off by saying that the BDR, while you -- everybody has a copy of what we have submitted already. I've worked through the Budget Office and through some of the Governor's staff, and we think we have something that we can all agree to that is moving forward. That does not mean that it cannot be changed. There's the introduction of the bill in the next legislative session. There's the amendment process. And so I really encourage the Advisory Board here to take a close look at this, see if there's recommendations or anything that you guys would like to recommend as far as changes or tweaks to the bill. We'll be happy to take those under advisement.

Joe Marcella: David, can I interrupt you just for a second? I didn't hear whether Jim is up north; that he would maybe fill in some of the gaps in your conversation. Is he available?

David Gustafson: Dave Gustafson. I do see Jim.

Joe Marcella: I just saw the back of the head.

David Gustafson: I did (inaudible). Okay.

Joe Marcella: Welcome, Jim.

James Earl: Welcome, Jim is --

Joe Marcella: Introduce, please.

James Earl: -- Jim is up north. Board members will recall that at the last Board meeting there were a number of suggestions and comments. And the BDR, which has now been distributed to you and has been submitted as part of the Governor's bill preparation process, does a number of things. The first thing that I want you to be aware of is that it incorporates the suggestions that were made during the last ITAB meeting. A number of those came from Mike Willden and several of them also came from legislature.

So before David began discussing the contents of the BDR within the executive branch, those changes and suggestions had already been incorporated. There were a number of other changes. Let me just draw attention to a couple of them. And these also are -- they were specifically mentioned in the last meeting, I think the changes that I will identify in addition to those that were suggested at the last meeting are certainly in line with the Board's discussion.

Board members will recall that at the last meeting one of the underlying precepts of the BDR, as it existed at that time, was to allow a two-year transition period, whereby individual departments would essentially have two years to analyze their services and decide whether they wanted to self-provision those services or whether they wanted to opt in completely and become a fully integrated entity -- a fully consolidated IT agency with EITS providing both their common and basic services. And after considerable discussion, it was decided to eliminate that transition

period and simply allow the Governor to exercise discretion, which was contained in the BDR as you last saw it, as the sole way to adapt and move forward within the executive branch.

And I'd like to point out to Board members that it's still open to the Governor to order consolidation either on an agency-by-agency basis or on a service basis. And in discussions with other executive branch representative, it's my understanding, and that certainly is not a perfect one, that the higher probability, in terms of any future consolidation coming from the executive branch, would be on a services consolidation basis. And I'd like simply to point out that this follows on from what is ongoing with regards to the enterprise-wide rollout of Symantec Endpoint Protection Services. It is consistent with the way in which we are moving on increasing the use of the new core telephony infrastructure.

And just essentially, as an aside, that was fully briefed in the last legislative session and legislators hopefully be aware that there was, essentially, a decision at that time made by both executive and legislative branch officials to transition as quickly as possible to a single-core telephony system. Additionally, since our last Board meeting, we have released a request for proposal for a replacement for the state e-mail system. And at present there are approximately 12,000 users of the single consolidated state e-mail system with an additional 3,000 or so that use separate agency-run systems. Moving forward under the RFP it would be open, for example, for the Governor to use this as one of the first service consolidations, were he so to decide that it was in the state's interest to move additional agency e-mail operations into a consolidated state e-mail system, assuming that the cloud RFP moves forward.

So using those three or four examples, we've already begun to move towards an IT consolidation on a services basis. And Board members will, of course, be aware that we have also moved forward on an agency consolidation basis as well, having absorbed some 55 members of the IT staff of Department of Public Service within the last year.

So, Joe, that's about all that I would want to say at a fairly high level, but I'd be willing to answer any questions that you or Board members may have.

Joe Marcella: Thank you very much, Jim. What I'd like to do is frame this from a high level perspective to initiate some discussion, because I think there should be some. One to recap the BDR 242, actually incorporate some housekeeping. And some of that housekeeping is particular to some changes in the provisions. One of the provisions is, is that the ITAB folks should advise on the entire tech spend for the state. Is that still in there, Jim? And that goes to the Governor for 2000 -- and you're talking about 2015 to '17?

James Earl: Yes, that's correct. The Board would essentially remain advising EITS, but there would be an additional representation of department heads, so the ITAB composition would change a little bit. And I probably should have mentioned this as well. In the previous draft, which you saw at the last meeting, the ITAB was -- and at least in that draft was modified so the ITAB was set up -- or would be set up to advise the head of the Budget Division -- chief of the Budget Division. And, therefore, that would consolidate both budget decisions and policy

decisions in IT. And after discussion within the executive branch, that particular proposed amendment was taken out and we essentially reverted to the existing ITAB language in NRS 242 with the provision -- or with the proviso that the ITAB membership would change a little bit to include more representation by department heads.

Joe Marcella: Thank you. And then the ITAB Board would ID and provide basic enterprise definition as to what the basic enterprise is. And you started to do that yourself, where you talked about communications. You talked about security, hardware, software, and any other items that are universal or affect the entire enterprise across the board horizontally. Is that what I understood?

James Earl: Yes, that's right. And the actual scope of the ITAB advice is likely to change should the Governor or, indeed, should the legislature make some decisions about expanding the scope of IT consolidation. And, obviously, previous reincarnations of the ITAB would not be overseeing an EITS/IT DPS scope of infrastructure and personnel. And so to the extent that EITS expands its practical mission through consolidation, the scope of advice that ITAB offers would be changed accordingly.

Joe Marcella: Thank you. And then what that tells me is that each individual agency, at their own discretion, can leverage those enterprise systems, but they still can manage the proprietary systems in a manner that's consistent with the business they're supposed to serve -- which they're supposed to serve.

James Earl: Yeah, that's pretty much the case.

Joe Marcella: Is that correct?

James Earl: We'll point out that there are some changes in the language, which I think should be interpreted as a change in underlying philosophy. Right now, the essential agreement has to be between the state CIO and agencies with regards to a mutual agreement and what services an agency receives from EITS. There are, in the present listing of 242, a number of agencies that are listed which, although, the statute does not identify them this way, they are usually spoken of "exempt" agencies, insofar as there is no statutory requirement that they receive all of their services from EITS. The fallback statutory division, at present, being that there is mutual agreement between the head of the Division of EITS and the agency head.

That particular section dealing with exempt agencies was drafted out in the last draft that you saw or would have sunsetted after two years. In the present version of NRS -- or the BDR that you have before you, that list of exempt agencies would be struck from 242, and the mutual agreement provision would also be struck. The services that would be provided to an unconsolidated agency would be at the CIO's discretion. And that's, I think…

Joe Marcella: Thank you.

James Earl: …a shift in philosophy whereby the executive branch, and by that essentially I mean the Governor, budget officer, and the state CIO, are exerting a little pressure on

departments to either move to the center or be very clear and have spent considerable time and effort with David convincing him that it's in the state's interest that they self-provision their services.

Joe Marcella: And the way I understand it then is that they can pick and choose, essentially, based on their business need and what they need to deliver within the provisions of the statute.

James Earl: Subject to the CIO agreement to extend their use of EITS services in an otherwise unconsolidated fashion.

Joe Marcella: Thank you. I'd like to open it up for discussion. Folks, in Reno -- I'm sorry, Carson City, let's start with you. Any discussion?

Paul Diflo: Yeah, this is Paul Dilfo for the record. Jim, maybe I could ask you to clarify what you said about the exempt departments. One, I'd be curious as what, you know, the criteria would be for a department to be exempt and not participate in the consolidated IT services.

James Earl: In the present statute, NRS 242, there's a listing of departments and those departments are not required to obtain all of their services from EITS. They can, but that's done on a mutually agreed basis between the department and the state CIO. And that -- it is not the case, even under the present system, that being on that list exempts an agency or a department from all of the provisions of 242. Those agencies are still using agencies as that term, "using agency," is defined in the present statute. The BDR takes out the term "using agency."

Now when you and I, in normal course of discussion, might identify somebody as a using agency, what we automatically think is that a using agency is an agency that uses EITS services. However, that is not how the term "using agency" is presently defined in the existing NRS 242. A using agency is statutorily defined, at present, as any agency that has a need to use information services. So an agency, even though it's on the list of agencies that need not use EITS services, is nevertheless a using agency for certain provisions of the existing NRS statute, which if read and if acted upon would give David considerable oversight authority or at least review authority over the operations of IT at NSHE and potentially in other branches of government as well.

The particular BDR, which you now have before you, eliminates the term "using agency." So we don't have this statutory not quite conundrum, but a definition of a using agency which flies in the face of what you and I would think of as a using agency. Now, coming back to your question, with most of that as background, the statute does not articulate a set of criteria for David or the Governor or department heads to use with regards to what services the state CIO would agree to provide any executive branch agency that seeks to use a service from the EITS service list.

Paul Diflo: Okay.

Joe Marcella: All right. Jim, I have one other question before I ask the folks from down south. By the way, is there any more discussion up north?

Director Teska: This is Julia Teska. I was actually part of the discussions on this bill draft request, the revisions. And I think the intent here was -- on some of these items is that the statute is a very inflexible document. It is something that can only be modified during a legislative session versus taking some of these issues and concerns and deferring them to a policy decision on the Governor's part allows for us to -- I mean, right now if you look at Chapter 242 and you look at the actual operations in the state, they're not aligned. And so we're essentially not following our own laws because we don't have the ability to change laws as rapidly as business practices sometimes would demand. And by deferring that to -- or referring that to policy established by the Governor's Office allows the departments to have more agility to meet its customers' needs and ultimately -- especially since technology is an area where things are changing so rapidly, it should enable the division to fulfill its mission more completely.

Joe Marcella: Thank you. And by the way, I tend to agree with your statement. I think this opens up our opportunities to make intelligent decisions based on conditions as -- and not be constrained by -- for me it's always Robert's Rules, but constrained by the legislature.

Jeff Menicucci: Mr. Chairman?

Joe Marcella: Okay.

Jeff Menicucci: Mr. Chairman?

Joe Marcella: Please. Yes.

Jeff Menicucci: Jeff Menicucci. I hope I'm not overstepping my role here, but I had a question regarding -- it looks like Section 242.105 relating to confidentiality of certain documents relating to Homeland Security has been removed. And, I don't know, was that going to be transferred to another part of the statutes?

James Earl: Jim Earl. That's correct. It has been removed in the BDR draft that you have before you. Our understanding is that this particular provision was added immediately after 9/11, and was not done at the request of EITS. It's an anomalous provision, from our standpoint, and is probably better placed someplace else. We have spoken specifically to Department of Public Safety and particularly those folks who are concerned with the Homeland Security Committee, and they are considering whether it is -- that's better to become a part of their statute, perhaps somewhat expanded.

This is the only time -- this is the only instance that -- which we are aware, that the Department of Information Technology takes an interest in the contents of information, which is somewhat anomalous for us. We are essentially agnostic with regards to the contents of other that -- you know, reside on our servers or that the mainframe processes. There's also the possibility, and we've discussed this internally, that it might also be appropriately transferred again with some possible revision to become a function of records and archives. And we defer to others, both in the executive branch and the legislature, as to where to put this or a similar section. We know

that it's being considered by department -- or, excuse me, by the Homeland Security Commission folks.

Joe Marcella: Could I ask Chris Ipsen to come forward and kind of talk us through what your opinion is, from a security perspective.

Chris Ipsen: Sure. For the record, my name is Chris Ipsen. I'm the chief information security officer, and my office has been responsible for maintaining these records over the years. My opinion is that it's an important function that government has. I think it needs to be maintained somewhere and I think that the discussion around where it should be placed is relevant. It does consume a lot of time and energy. One of the important considerations is that we're not actually taking all of this data and storing it. We're merely maintaining a record of those types of services and data that the state deems confidential.

So, for example, if someone wanted to do a Freedom of Information Act request against our configuration files on a server. Well, there's a security problem with that; also with passwords and other types of items that we may have in our possession. We're not concerned about those specifically. We're concerned that they remain confidential. And it does require a certain level of effort on my office's part. So if you're asking for my opinion, as the chief information security officer, I believe that the service needs to be maintained, and I want to say that pretty emphatically. I also want to say that it does consume a lot of hours that we could be using security professionals in other places more appropriately, rather than maintaining the list of documents, actually working on security functions.

Joe Marcella: Mr. Menicucci, I think -- and I'm making an assumption here -- your concern was is that whether the EITS folks have a fiduciary responsibility to keep that information secure. Is that really the question?

Jeff Menicucci: That's certainly part of it, Mr. Chairman. We may get asked -- as Mr. Ipsen suggested, we may get a public records request for information regarding the way our system is set up, penetration testing and results, things that we would be primarily concerned with. And then there are, I guess, other things which might more properly be placed in Homeland Security-type statutes.

Joe Marcella: So there's a difference, in your mind, between the business data record or privacy information versus those records that are necessary in the day-to-day normal operations of a technology organization?

Jeff Menicucci: I think so. And I just wanted to raise the issue to make sure that we've given some consideration to that, because every once in a while someone does ask for things like have you done a penetration testing and what were your results.

Joe Marcella: Thank you. Mr. Earl, is there any comfort level with including at least something within the statute that says they have a fiduciary responsibility to keep the information secure and maybe cite some of the examples?

James Earl: Well, EITS has an obligation, as do other agencies, to respond appropriately to request for records; question whether they are public or not. And I don't see the EITS response as being determinative as to whether the particular statutory provision exists or not. I think there are other organizations, other than EITS, that are in a better position to be repositories of lists that individual agencies feel need to be protected in some way. I'd also point out that if not at the last session, then the preceding legislative session, there was an amendment which the legislature considered to expand the particular scope of this provision to include counties and cities that could notify EITS and do it of records that they wanted to remain confidential. That particular amendment was turned down. Some legislative suggestion that this particular provision was not to be extended.

And so we've raised the very basic question as to if there are to be a list of records or records kept and maintained as to what individual agencies feel ought not to be run through the standard record review prior to release, then our recommendation as EITS is that another agency be found to do that.

Joe Marcella: Thank you. Mr. Ipsen, any additional comments?

Chris Ipsen: No, I don't have any additional comments to that.

Joe Marcella: Discussion from the Board down south? Assemblyman Anderson.

Assemblyman Anderson: Thank you, Mr. Chair. A couple of questions in regards to that .105 section. So what -- I guess the question is what sort of expertise is required to maintain and produce what documents are supposed to be on that list, and if not in EITS, what department might be best suited for that?

James Earl: My understanding, and I unfortunately do not have the statute in front of me, is that we're not making a judgment call, as Chris Ipsen indicated. We're simply taking an agency representation at face value. And I would suggest that there are better places, Department of Public Safety, and specifically and that part that deals with Homeland Security issues within Department of Public Safety and/or the Library and Archives would be better places to handle retention. And part of the reason I'm favoring -- I personally favor Homeland -- or the Homeland Security-type organization within DPS is some legislators may recall that the Homeland Security Commission statute involves the collection of data that relates to Homeland Security infrastructure.

And over the past three or four legislative sessions there's been considerable toing and froing between one and the other session as to whether that should be expanded or not or whether the Homeland Security Commission statute should be changed. And our present recommendation is that the records management function should be taken out of EITS and specifically out of the

Office of Information Security, which has no administrative staff, which is staffed entirely by Information Security professionals and it simply is not, in our view or at least mine, a function that IT professionals, particularly IT Security professionals, ought to be managing on behalf of the entire state.

Joe Marcella: Thank you.

Assemblyman Anderson: A follow-up to that, Mr. Chair. So I just want to understand the answer clearly. So what you're saying is essentially EITS does not have any criteria for what goes on or off the list, it simply is compiled by the various agencies that may be determining that. And right now you're serving as somewhat of an archive function and they go -- folks will come to you to see if something's on that list; is that accurate?

James Earl: That's certainly my understanding, and I defer to Chris Ipsen, there in the south, if there's any modification of that if I'm wrong.

Chris Ipsen: Thank you. For the record, Chris Ipsen. That is correct. We are a repository. And in addition to that, what we've done in the past is we've certainly provided agencies with some background around the vulnerabilities of these types of data sets and the necessity. We've followed up with those agencies and specifically where we know that there is sensitive data or that it resides that we make an effort to make sure that they follow up on those records. With that said, and as a member of the Commission for Homeland Security as well, I do agree that some of these records do need to be maintained as confidential. That's really an important point that I'd like to make.

I do believe that there is a place in Homeland Security for that. And I think it's important because many of the issues that we discuss, both at the Homeland Security level and also in the EITS, is a balance between privacy and confidentiality. So we want to, by default, make all records in the state public. I think that's an appropriate way for government to be maintained. However, as we begin to collect data that's sensitive about individuals that could affect their lives and also to adhere with federal compliance around these records and also private sector compliance around these records, certainly some of these records cannot be made public. And those are the ones that we want to focus in on.

And I believe that we could support the Homeland Security Commission if they chose to accept this. And I'm not saying that it will. I think that there needs to be an elegant pass off or a transfer of this responsibility. What I would not like to see is I would not like to see us eliminate it and then have nowhere to place it elsewhere in government. I think that's really critical that there be a graceful handoff of this. And I know that in having spoken with the counties and cities, they too fought very hard to have this authority to be able to do this. It's really to protect their data and their infrastructure. And I think that a discussion around that is also fruitful, and the Commission provides a vehicle for that. The Commission is not an internal service fund to the State of Nevada. It is really a statewide committee, so…

Joe Marcella: Cyber security, privacy, e-discovery, open data and all of that is still evolving and it hasn't been cleanly defined. So from my perspective, even though this isn't really definitive and you can't categorize everything and there has to be some judgments any time either data is requested or how it's stored based on best practices, what we understand today, it seems to be a practical approach until -- it's no longer a practical approach until it needs to be more formalized. Is that the approach you're taking? It sounds like that's the strategy.

Chris Ipsen: Certainly that is the approach that we are taking. And I'd like to say that all requests are reasonable. However, they are not. And I do believe in, as has been already presented earlier, data sets such as the results of penetration tests and -- would really -- would clearly define where our weakest points in our network are. And we still have -- that's one of the few advantages we have over the hackers, and they have most of the advantages, is that we know where our vulnerabilities are and we can apply resources to those vulnerabilities. So those types of records and data sets really need to be maintained as confidential.

Joe Marcella: So back to the original question from Jeff. He's got an Italian name and I have problems with it. I can't understand it -- from Jeff was is that there should be some provision that says that you're going to take a fiduciary responsibility for what you own. So is that -- Jeff, would that be sufficient?

Jeff Menicucci: That's probably a good shorthand way of putting it. I think there are two things that got discussed. One is EITS may come into possession of documents prepared by other agencies on which they have an obligation to safeguard them. And then there are some documents that EITS may produce on its own, which are confidential in nature and, of course, they would need to be safeguarded as well. So I think there's two sources that we may find for confidential information that EITS may have to handle. I don't know…

Joe Marcella: Then I think it would be the Board's…

Jeff Menicucci: Right.

Joe Marcella: Oh, I'm sorry. I think it would then…

Jeff Menicucci: I don't know if the existing…

Joe Marcella: …be the Board's…

Jeff Menicucci: I'm sorry, Mr. Chairman. I don't know if the existing statute is even adequate. And I just wanted to raise that issue for purposes of discussion, because I think it may come up more in the future.

Joe Marcella: Thank you. I appreciate it. One more comment. Is there anything from you, Ernie?

Ernie Capiral: No, (inaudible).

Joe Marcella: Right. Any additional comments? Mr. Ipsen.

Chris Ipsen: For the record, Chris Ipsen. One last comment around this is that this is not trivial legislation to get passed. Usually it goes through and I was there when originally it was passed. I wasn't a member of OIS. But I know that there's considerable effort that needs to be put into these types of legislation when privacy and confidentiality concerns are involved. And, again, I think it's imperative that we don't just eliminate it; that we have a mindful approach to place it somewhere else to make sure that the capability is still captured.

Joe Marcella: Thank you. Assemblyman Anderson.

Assemblyman Anderson: Thank you, Mr. Chair. I just -- I wanted to step back before when we were talking about sort of the elimination of these divisions that are -- well, essentially come under the auspice of exemption, I guess, or many of them feel that they are. The two that I see in there, the LCB for one, Legislative Counsel Bureau, and the Court of Administration I think could have pretty significant arguments being separate branches of government that would argue that they may need to be exempt. I guess the question would be -- well, I'm not making that argument at this point, but the criteria for consolidation versus the criteria for exemption, who would be making those decisions? What panel would -- or staff would be looking at those to determine what the criteria would be and then who ultimately would make the decision? And then lastly, I'll just give it to you, have we had any feedback from any of those folks on this draft?

David Gustafson: Mr. Chair, Dave Gustafson for the record. I wanted -- let me answer that with a step back. And that is this BDR actually introduces the concept of enterprise services, and those services are executive branch by their nature. But this particular statute allows the Governor to direct enterprise services for agencies. And that's kind of an important policy piece here. So let's just play a scenario. E-mail, since the e-mail was brought up earlier. If the Governor decided everybody was going to get e-mail in the executive branch government, then that's the way it -- he may direct that according to this version of the statute -- the BDR, I should say.

So everything else is, by default, negotiated. Only those enterprise services that the Governor may direct are those that they will get. Everything else is negotiated. And, Jim, you can correct me if I'm wrong, but that is my understanding of this.

Joe Marcella: Mr. Gustafson, then the question would be -- and this is sort of an aside question. The strategy, direction and the draft of -- or the redraft of 242 for the BDR, is it based on any national criteria changes, strategies from other organizations, advice from the Gartner Group or like organizations and agencies? Is this something that came about based on current circumstances, as well as best practices across the United States?

David Gustafson: Dave Gustafson…

Joe Marcella: And I don't mean to put words in your mouth, but that's the way I would approach it.

David Gustafson: Yeah. Mr. Chairman, thank you for your interest in consolidation. You know, I've been here in the state for just a little over five years and I've been going to every NASCIO conference every six months, and I can assure you consolidation -- data center consolidations, e-mail, the infrastructures, security, all these things are in the top three every season, if you will, every year. I think we're going to hear later on from the Hackett. We're going to look at the Hackett Report and you'll see just how well we're doing over here in our current state. And so what I would offer is the easy wins, if you will, through gaining economies of scale, saving some money, are clearly in the infrastructure area. And that's the areas that I wish to really be moving on first, which is, look guys, I just don't want to see more data centers popped up, you know.

I look around Carson City and there are probably 10 or 15 data centers, server clubs or whatever you want to call them, within a one-mile radius around the state's data center. And I just think that some of these things are wasting taxpayer money. And if we can just waste a little less in government, I'd be really happy about that. And so this is one way in which we can sort of do that. And if this current BDR is enacted, that will essentially allow the Governor to make those kinds of decisions for them.

James Earl: Mr. Chair?

Joe Marcella: Jim. Yes.

James Earl: Jim Earl. In the run-up to the last legislative session, David and I and members of the Governor's staff at that time, considered right of different consolidation options, as you'll be aware. In the course of doing that preparation, David and I -- and I will admit that I did it more than David did -- pulled probably the underlying information technology statutes from about four or five states that we thought might be construed, generally, as leaders in consolidation. Either because they'd had an effective consolidation years ago or they had moved very decisively in the last several years towards a much more consolidated model. And what I found was that it was very, very difficult to find a good legislative model.

As convoluted as NRS 242 is at present, many of the states that we looked to as examples in the consolidation area had statutes that were much, much longer than ours and much, much more specific that would allow for far less adaptability. So in terms of the very precise question that I think you asked, were there any really good legislative models out there, I can tell you that there may be but we didn't find any. And NASCIO, for better or for worse, does not have a single legislative model as to what a state who is looking to consolidate, who is looking to be responsive both to changes in agency missions and changes in technology. That simply didn't exist.

If I could go back to Assemblyman Anderson's question, which essentially was, okay, how are you going to handle the separate branches of government? The existing statute, NRS 242, is written to address the needs of using agencies, where using agencies are any agency in any branch that has a need for information technology. And then in that statute there's a specific

provision that exempts the judicial and the legislative branch from the necessity of having to obtain services from EITS or any of its predecessors. The draft -- or the BDR that you have does not have that same underlying premise of a universe of all state agencies that have a need for enterprise -- or have a need for information technology. The definitions in the missions, as laid out in the BDR that you have before you, are restricted to executive branch agencies.

So we don't have to have a list that exempts different branches of government, because that's done essentially in the purposes section and in the sections that deal with David's role as a state CIO. I hope that was clear. We took it very seriously.

Assemblyman Anderson: Yeah, that's the answer I was looking for; it was that criteria.

James Earl: Yeah, we took…

Assemblyman Anderson: Thank you.

James Earl: …yeah, we took very seriously the concerns that were expressed by legislators at our last ITAB meeting.

Joe Marcella: One last comment from me. I read the Hackett Study. This is a very good first step in the revision of 242 to actually start to break the back of many of those issues that are outstanding. And I also think it's a good first step to get your arms around what technology should be doing in enabling the rest of the communities, as well as providing the kind of umbrella technology that's necessary for all of the locals as well. So I'm pleased to see something like this moving forward. Understand that it's not perfect and it needs to be revised, changed, modified, and corrected, because nothing's right the first time.

Counselor, Jeff, what I wanted to know is could I call for a motion to accept the report on 6A? I know it says for possible action, so I'm allowed to do that?

Jeff Menicucci: Yes, Mr. Chairman.

Joe Marcella: Okay. Then I would like to ask for a motion to accept the report.

Assemblyman Anderson: Assemblyman Anderson. Motion to accept.

Joe Marcella: Anybody second?

Paul Diflo: Paul Diflo. Second.

Ernie Capiral: Ernie Capiral. I second.

Joe Marcella: Okay. And then I'll open it for any additional discussion. Hearing none. All those in favor?

Group: Aye.

Joe Marcella: Okay. All right. Let's go ahead and move on to 6B. David.

David Gustafson: Dave Gustafson. Thank you, Mr. Chairman. I wanted to also speak to you a little bit about the unclassified/compensation initiative. And you sort of threw me off-kilter a little bit, because I was going to go through some of these things in BDR. But what -- they were making a few changes to the statute if the BDR, as it is now, is enacted. And one of them is on Page 6. It's 242.080, the Creation; composition. "The Division consists of the Administrator and such personnel as the Administrator deems necessary and appropriate to carry out the provision of this chapter."

So then you go into -- that's a change and the reason why I'm talking about all this Human Resource stuff because it all goes together. And then when you get into -- what section is this, it's Page 7, it looks like 1E. "The employee means classified and unclassified personnel as he or she deems necessary to appropriate to carry out this chapter." We're looking to do this for a couple reasons. One is the classified status -- the classified system is very encumbering in terms of pay. And so we're not able to be agile and nimble enough to be able to go ahead and hire, recruit, and retain technology professionals, meaning -- and I learned this lesson through the downturn, and that is when we were hiring IT professionals -- okay, let me take you back a little bit -- 2009 or so, I think it was Governor Gibbons at the time who issued an executive order initiating a hiring freeze and a step freeze eliminating supervisor pay at 5 percent. There was another Hispanic speaking, I think it was, or multiple languages, do you see another 5 percent.

A lot of these things went away, but the tech industry never really slowed down. And so we were hiring technology professionals at step one, and we still have yet to get passed that. We still have furloughs. We still haven't had a COLA. And so -- but the technology world has moved on. Technology professionals in general are, you know, 3 to 5 percent unemployment. And so we're not able to be nimble and to hire and retain these technology professionals just because of the limitations of the government itself. So what I'm hoping to do is sort of thaw the ice a little bit and hire unclassified. I've asked for four tiers of classifications, if you will, in the unclassified service. And I'll go through those really quickly with you.

The -- I call it the regular IT guy, pay is up to $88,000. Then you have senior IT guy, which pay is $98,000 and some change or something. And I've worked these out. My proposal is not pulled out of the air. I've worked with HR as well on this one. So a senior IT guy would pay, you know, up to $100,000 a year that I'm asking for. IT managers at $107,000 and then senior IT managers at $117,000. And I think this will allow us the flexibility that we need to be able to hire and retain those individuals. So I want you to know why I'm asking for the things that I am and how we kind of got here.

The second thing -- or I should say an additional point here, is we are requiring -- in this bill draft under Regulations 242.111 on Page 9, we're requiring regulations, standards, and policies to manage the human resources of the Division. I don't proclaim to be a government guy through and throughout, I mean I'm just new on the government scene here. So I'm not a big fan of all

this serve at the pleasure of people. Even in the private sector you have three strikes and you're out or you've got HR policies. There's some mechanism there. So what I'd really like to do -- and I'd be looking for recommendations from the Advisory Board as well on this, Mr. Chairman, is I'd like to put in a structure that was, you know, three strikes and you're out or you have to have, you know, several managers agree that you need to, you know, you need to be terminated or something to that effect.

NSHE uses -- I think they have annual contracts with employees. The Gaming Control Board has some other mechanism they use to manage unclassified employees. I want to be able to ensure employees of the Division that this is just not a, hey, I don't like your shirt today, you know, you're out of here kind of routine; that there's some level of protection. It's just that in state government there is either classified, unclassified or nonclassified, which we don't want to talk about. But there's nothing in between. I think that in between there, somewhere between classified and unclassified, there's a happy ground there and I'm going to try and create that through regulations, and that is my intent. So I'd be willing to take any advice that you guys would like to give me on that, but that's sort of the intent and where we're going and how much we want to compensate.

Joe Marcella: Let me make one high level -- this is Joe Marcella for the record. I want to make one high-level comment and then open it up for additional discussion. What I'm hearing is that what you're really looking for is a competitive wage and a competitive position, and you're looking to update your skills inventory within your own organization. And you weren't able to do that based on certain constraints and some of those constraints are in the classified contracted employee ranks.

Now, I also heard you differentiate between the unclassified individual, who's appointive and that you have a little more flexibility with, versus those individuals within your organization that need to follow and should have strict rules. Like doors on Fords, you have so many to do. You have to manage that from a certain perspective. It has to be consistent and it has to follow the rules or it compounds by -- when you make that mistake, it compounds by the thousands within seconds. Is that how you're differentiating one from the other?

David Gustafson: Dave Gustafson. That is correct.

Joe Marcella: All right. So that frames our conversation. Ernie.

Ernie Capiral: Ernie Capiral for the record. I agree with Dave on this. I know that in the past our agency, we've lost people. We end up hiring people, training them and then they leave for higher compensation elsewhere. So if we can do anything to help out and get the good people and retain them, I think that would be a great boon.

Joe Marcella: And I just wanted to add one comment. I've been in IT a hundred and something years, and the truth of the matter is, is that this is the first time in my career that an IT organization, the technical professionals, are in a classified environment. So that makes it a little bit more difficult to do this intelligently and the level of flexibility, because the truth is, is that if

you do it today, tomorrow it will be different. And regardless of what you do it's wrong and it has to be adjusted. And there are no rules that could cover all of that. So you need a blend of both. And that's my opinion and that's an official opinion from the Board, at least from the Chairman.

Assemblyman Anderson: I'll second that motion as well, if that's a motion. You know, I'm all for this idea. I think even in the private sector we struggle to maintain good folks. We feel the same burdens of hiring people, training them and them finding great jobs with the training we just gave them. So sometimes every couple years we struggle with that. So with that, I think that the flexibility is critical. I'm wondering what other -- outside of 242, are there other restrictions that are placed on you that would not allow or would have to be changed in order for you to do this? And then is this enough to achieve the goal that we're after? I have one follow-up after that.

David Gustafson: David Gustafson. Jim, are you still at the table?

No response heard.

David Gustafson: We had -- this version you guys have here doesn't have Jim's notes on it. He's got some very interesting notes. And, Jim, I don't want to -- I can't see if you're at the table or not. But there is a provision in the human resources statute that if your statute exempts you from their statute then you can be exempt from their statute, essentially is what it says. And by us having in our statute that we're required to maintain and manage human resource regulations, then we are, in effect, sort of moving outside of the classified system. Jim, did I do that justice?

James Earl: I'm not sure that I'm the best person to say yes to that. I may defer some of that to your deputy of six to eight months now, who has a much stronger HR background than I. But essentially the state employee regime is divided into unclassified and classified services. And the classified service is very regimented -- very regimented and goes back, I think in the State of Nevada, to the late '40s or '50s. It's been around a long time and it was put in place as -- in fact, a comparable classified system was put in place in the federal government for excellent reason. It was to prevent -- or to do away with the spoils system.

And over time, a fairly strict and regimented regime has become even more strict. And, Joe, I think as you pointed out, it's very -- the sorts of regimentation and very tight definitions as to job skills and job requirements makes sense if you're trying to differentiate a rural postal worker from a postal sorter, who doesn't leave the post office. It's not real good and has become increasingly problematic dealing with IT and technologies that change, and it's problematic as well in an era of consolidation. We've experienced this firsthand with trying to absorb essentially 55 state IT classified workers from the Department of Public Safety. Any operation, any management operation, ought to have, I think, as its guiding principle the interest of putting all of its employees to their highest and best use. And it's just very difficult to do that in IT in the present time within the classified system.

Now, the particular language that we have in the BDR that talks about your ability or the ability of the CIO to appoint classified and unclassified, and then I think in that same provision it goes on to say, and I won't get the words exactly right, that the support staff remain in the classified service. So we're really only talking about IT professionals, and since, at present, each has very, very few administrative staff, we're talking about a significant number of each staff at least being eligible to move into the unclassified service. The language that you see before you has gone through about, oh, three or four different revisions with Amy Davey and I being advised very precisely by human resources staff. They and we have pulled the statutory provisions from a number of different agencies ranging from the Attorney General's Office to the Gaming Control Board to some smaller organizations, such as the Tourist and Cultural staff, to try and pick up the best language and develop a composite model. And that's what you see in the BDR. It may not be perfect, but it is, in fact, very carefully informed not only by the HR staff over the past several years, but also by our comparison of other statutory provisions with HR in tandem.

Joe Marcella: Okay. Thank you. I'd like to go ahead -- unless there's some more discussion. Then I'd like to call for a motion to, one, accept the report and provide some direction to EITS as to how they should deal with the classified and unclassified environment and how to move forward. Assemblyman?

Assemblyman Anderson: Okay. I'll make that motion. Recommend certainly that we expand the language in the BDR to review those changes of the classified versus unclassified. I'd also like to maybe better understand the HR impact, as far as how they would manage that, as well as the potential impact on agency costs if we had additional unclassified employees, would that affect our pricing to the agencies. It's kind of a long motion, but your discretion, Mr. Chair.

Joe Marcella: Okay. Is there a second?

Ernie Capiral: Ernie Capiral. I would like to second that.

Joe Marcella: And you're going to be on the list of all of the seconds, you know that, right? Thank you. And then any further discussion? And you were pushing your button, David. I'm sorry. Jim?

Director Gilliland: Mr. Chair, for the record…

Joe Marcella: Okay.

Director Gilliland: …Romaine Gilliland. I do have a question and I would like some clarification on the motion. Are we, at this point, asking Mr. Gustafson to come back to us with some additional thoughts regarding how we would like to see this proceed with specifics and to better understand those before they're added to a BDR or is there another step along the way that we should be anticipating?

Joe Marcella: David, what is the time limitations on all of this?

David Gustafson: Dave Gustafson for the record. Well, this is part of our bill draft request. And so agency request is going to be closing at the end of the month and then we're going to go into Governor's recommended, which is off limits to me. And so what I would do then is take any recommendations from the Advisory Board and run those through my chain of command. And if those are so to move forward, then what I'd probably do is when we introduce the bill we can introduce the bill with amendments. This is the IT guy talking, by the way, not our legislators, so let the -- we…

Assemblyman Anderson: I just know your deadlines and so I'll…

David Gustafson: Yeah. Yeah.

Assemblyman Anderson: …clarify the motion just to understand those deadlines better. So I would not recommend at this point that you bring it back to the Committee, but you incorporate the ideas, as discussed with the unclassified compensation, but take into account some thoughts in regards to the HR impact and the potential impact on agency costs. Obviously, there's a lot more discussion that goes beyond this to make this law or affect any changes. So I think those could all be brought up at a later time.

Joe Marcella: We'll consider it advisory. Thank you. All right. Then could I call for a vote? All those in favor?

Group: Aye.

Director Gilliland: And I'm going to abstain.

Joe Marcella: Thank you.

James Earl: Joe, did you pick up the abstention up in the north? One of your Board members abstained.

Director Gilliland: Okay.

Joe Marcella: No, I -- okay.

Director Gilliland: Yeah, for the record, this is Romaine Gilliland. I'm going to abstain. Had there been some additional discussion, I would have mentioned that prior to a vote on this I would have liked to have better understood the fiscal impact, as well as any other ripple unintended consequences that we might have throughout the state. Thank you.

Joe Marcella: Thank you.

7. EITS PROPOSED BUDGET AND BOARD ADVICE *(*for possible action*)* presented by David Gustafson, State CIO; Amy Davey, Deputy State CIO and Unit Chiefs

The Board shall:

(a) Advise the Division concerning issues relating to information technology, including, without limitation, the development, acquisition, consolidation and integration of, and policies, planning and standards for, information technology.

(b) Periodically review the Division's statewide strategic plans and standards manual for information technology.

(c) *Review the Division's proposed budget before its submission to the Budget Division of the Department of Administration. NRS 242.124.*

Joe Marcella: All right. I'd like to move on to agenda item 7. That's the EITS Proposed Budget and Board Advice. David, is that coming from you? Please.

David Gustafson: Dave Gustafson, Mr. Chair. Yes, it is.

NRS 242 requires us to present our budget to the Advisory Board for recommendations, you know, going into the Governor's recommended process. You've heard me say on the record before that that's not really how the government works and that's not really feasible. But what I've asked my chiefs to do today is to come up here to the Advisory Board, present sort of just quick and dirty five minutes of what they're asking for in their budgets, and certainly you guys can follow up with any questions you might have. But at least you'll get an idea of what we're asking for without actually presenting our entire budget to you.

This, I believe, is also one of the provisions that we'd like to scratch out, because the way the Governor -- I should say the way the budgeting process proceeds it doesn't allow us or afford us the opportunity to present to the Advisory Board our entire budget then have you guys contemplate, make recommendations before our budgets close. That's just not feasible. So what I've asked the chiefs to do is just come up here for five minutes each or whatever time they deem necessary, but not long, and just give us a quick and dirty as to what they're asking for in their budgets and sort of where they're going with that, so…

Joe Marcella: Please proceed.

David Gustafson: Thank you, Mr. Chairman. Dave Gustafson. Mr. Ipsen will be leading this off here. Chris.

Chris Ipsen: For the record, I'm Chris Ipsen and I promise to be brief. I have an opportunity to speak on cyber security and I know a number of the discussions that we're having today are surrounding cyber. So what I'd like to do is talk about the process a little bit. Generally, what we're looking at in the approach to funding key projects for the Office of Information Security in the current and upcoming fiscal years.

Right now our requests can be broken into two primary areas. One is to support the key initiatives that we've already established, those being continuous monitoring and also our Altiris deployment of Symantec products on the end point. Both of those are very significant moves forward on behalf of the state. And my goal is to capture the costs that we have incurred as a

result of those projects, and also to make sure that we have the appropriate maintenance of that infrastructure going forward. That's critical.

When we initially did this the legislature, I believe, noted that this project is saving the state $3.5 million -- the Altiris Project is saving the state $3.5 million. That's great. What we also found is that there were a number of other parts of the infrastructure that were necessary that required maintenance. For example, SQL licensing. Originally, the costing was not in there because the costing was lower. As soon as we procured the solution, Microsoft decided to increase the cost of SQL licensing, and as a result we incurred an additional $70,000. So those types of costs are the things that we're looking to maintain; not to augment, but to maintain going forward.

Secondly, we looked at personnel. And when in the scope of these two particular projects, we found that there were some key initiatives that needed to be managed correctly if we were going to be successful. I believe that's one of the questions the IFC asked me, and that was a really good and interesting question, is how do you intend to be successful with this project. And my answer to them was we don't have the option to fail. And as a result, what we did is we took the resources that we had available to us and did the best job that we could. However, given that they're our enterprise infrastructure and they affect every desktop in the state, it was imperative for us to place bodies around key components of this infrastructure.

We did an architectural analysis initially with this project. It was determined that 12 positions were required. We started with one, and in the upcoming proposal, we're looking at four positions, two of which are coming from other -- repurposing of individuals, two specifically dedicated to this project within the Office of Information Security. And those are around developing the packages that will be pushed to all of the agencies. Also around the maintenance of the key infrastructure that's associated with this particular project. This being the Altiris Project.

This is an essential project moving forward. This is not an arbitrary. It will touch every single desktop in the state. For us not to do testing and analysis on the packages that we're pushing out and to the configurations that we're pushing out, in my opinion, represents nearly malfeasance. I won't say malfeasance, but we really do have to do this correctly. Our agencies expect us to do it correctly. I expect us to do it correctly. So two of those positions are workers within this group.

Another position is one that I assigned one of my top people to manage this project moving forward. In addition to managing this project, he is also taking care of key infrastructure developments that we, as an enterprise IT services, have determined as necessary. For example, making sure that DNS is working correctly. DNS, without getting into the weeds too much, is the name to IP address resolution. If you don't that right, people don't get where they're trying to go. That's kind of important.

Additionally, we've found that active directory or directory services was essential to doing this correctly. If we don't integrate and identify ourselves in a common format, it doesn't work. So we've had to normalize that infrastructure. Additionally, we've also looked at time. When we

look at how we work within an environment, how we determine if something has happened. Synchronization of time across the enterprise is absolutely important to computers.

So what this project is doing is it standardizing desktop configurations. It's offering the four, now five controls that we've determined will reduce risk in our environment, those being patching of third-party applications, patching of operating systems, reduction of administrative privileges, and also application whitelisting, which is somewhat complex. And then, lastly, standardized configuration of desktop. We know that if we do this correctly, we will reduce risk to the state upwards of 80 percent. And when you look at breaches in the area of $50 to $100 million to a state, it's a good investment. And this also represents hygiene -- cyber hygiene moving forward. Systems will work better, they'll be more secure, and we'll have an accurate understanding of what we have in our environment.

So three of the positions that we are looking for within OIS and in review is one is the management position that I took out of my group to manage this project. I need to backfill that individual. He was fully burdened when I allocated him. As a result, my staff has had to take on the responsibilities that individual, which means each person just increased their already fully burdened load by at least 15 percent.

Additionally, we allocated two people into this group specifically to work on it. And then a fourth position that we are looking at is to effectively capture the Nevada card access system moving forward. Those of you who are familiar with the state know that we have badge reader systems throughout the state. Over half of the people in the state use this system to gain access to and from -- physical access to and from their systems.

Now, there has been some discussion whether this should reside in OIS or not, very similar toward our discussion around confidential records. And my position is I'm agnostic as to where it resides, but I'm fully committed that this position be fully allocated to this purpose and that we have additional support for this individual moving forward. We bill for it. We need to capture it, but we need to make sure that we allocate a full-time equivalency for it.

The scenario I would present to you is -- and we saw this -- when the snows are coming down and the holidays are approaching and it's a Friday afternoon, and the card access readers don't work, then the NDOT vehicles can't get out of the gates. The police and fire people cannot get into evidence lockers and/or other areas. And it's important that we maintain this position correctly.

Lastly, and in summary -- I think my five minutes are way up -- we're looking at support of existing software and allocation of four positions moving forward that are appropriately placed around security functions within the state. With that, I'll take any questions or are we waiting for questions at the end? What are we…

Joe Marcella: For the record, Joe Marcella. When you talked about continuous monitoring, is that SIEM?

Chris Ipsen: SIEM is…

Joe Marcella: I mean, is it grant funded? How is that funded?

Chris Ipsen: For the record, Chris Ipsen. One of the sources that we derive money is generally from grants. Thank you for bringing that up. I always look to grants first and look to the general fund second. I also look to federal compliance first; if the feds require us to do it, and we have funding from the feds then we take that money first. The SIEM, the Security Incident and Event Management Systems, we use that as a feed for our continuous monitoring project. We also have managed security service and we have a number of other feeds that come into the aggregate. So the answer is yes and more so, much of which has been procured through grants.

We've been very successful over the last biennium. We've received almost $2 million in grants, which is twice my budget. So we've been very successful in getting others to pay, primarily federal government, some of our security systems. But yes.

Joe Marcella: Is there a universal benefit not only for your own organizations and multiple agencies up north, but is there a universal benefit for the state and locals?

Chris Ipsen: Absolutely. Thank you for that softball question. Yes, when we deploy solutions in an enterprise fashion, everyone benefits from the solution. A good example of that is the legislature last time required that agencies report known or suspected incidents within 24 hours to the Office of Information Security. We do that; however, in excess of 99 percent of those incidents are not reported to us. They're reported from us to them back to us. So we are seeing it first as a result of this enterprise infrastructure.

Additionally, and if it's possible -- and we have legislation that allows us -- it is one of my personal goals to make sure that whatever we do in a standardized fashion, in an effective fashion, is also quantified and extended down to the counties and cities. So if we do something right, we want to give it to everyone else and share the cost across the state.

Joe Marcella: Last question, Mr. Ipsen. If you add bodies…

Chris Ipsen: Yes.

Joe Marcella: …is there a current statute in 242 or provisions within the state that allows you to actually leverage those folks so that you can do something intelligent rather than paying for three additional bodies? There's standardization across the board. You talked about active directory. You talked about standardized security, equipment, and the like. Three bodies doesn't do that.

Chris Ipsen: For the record, Chris Ipsen. You're absolutely correct. There's more work to do than we have people to do it. And I'm also mindful of the context that we're working in. So at the risk of everyone in the room cringing, I like to look at the budget as an iterative process. As we have needs, we find resources, and it's kind of like the "Raiders of the Lost Ark," you know, every now and then you've got to take a leap of faith and step over the cliff. And miraculously

everyone, including every significant body within the state has recognized when we have a need that we need to band together and do this.

And I'm not afraid to face the IFC for another three-and-a-half hour session to explain why we need the people. But I also don't want to put them out there and say if you build it they will come. I think you have to have discrete work for them to do that is obviously and unquestionable. I don't like to fail when I go and ask for bodies.

Joe Marcella: So what I just understood is that you don't know what you don't know, and sometimes organized intelligent folks can help you find that out.

Chris Ipsen: For the record Chris Ipsen. Yes. And I can tell you this; we need more, but I don't know how much. And as we need it, I'm going to keep asking. And we have a responsibility to produce as we move forward.

Joe Marcella: Any questions for Mr. Ipsen?

Paul Diflo: For the record, this is Paul Diflo.

David Gustafson: Dave Gustafson. I'd like to…

Paul Diflo: Hey, Chris. Paul. What is the proposed percentage variance over the previous budget?

Chris Ipsen: For the record, this is Chris Ipsen. I believe our projection -- right now the Office of Information Security has about a $1 million per year request. And I believe this is probably going to push that up by another 15 to 20 percent is probably a reasonable number, so $1.2 million. And if we can offset that with other costs and I always try to make everything cost-neutral, but it isn't. It's never cost-neutral, but I think it's cost-efficient.

Paul Diflo: Thanks, Chris.

Chris Ipsen: For the record, if I can answer that also. In terms of percentage of IT, IT and state government in Nevada is significantly lower than it is in the private sector, I believe. And I don't know what the report will say -- the Hackett Report, but I believe we're also lower relative to states. And a subset of that is IT security, and we're lower than that as well. So we are underfunding cyber security as it currently exists right now. That I'm very confident.

Joe Marcella: Either that, Mr. Ipsen, or you're a bargain. All right. Let's continue.

David Gustafson: Dave Gustafson. I'd like to ask Alan Rogers to come up. Alan is the chief of programming and DBAs.

Lynda Bashor: Joe, before Alan starts, I'd just like to let you know that Director Malfabon has arrived. Did you catch that?

Joe Marcella: Yeah, Rudy's here.

Lynda Bashor: Yes, sir.

Joe Marcella: Okay. Thank you. Welcome, Rudy.

Rudy Malfabon: Thank you.

Alan Rogers: Alan Rogers. I'm the manager of Enterprise Application Services, and our section provides application design and development and management, web services and database management services.

The majority of the resources in our application development group is spent on maintenance. About 80 percent of our efforts are maintenance on existing state applications. About 20 percent of our time is spent on either enhancements and sometimes new development of applications. These services are billed on an hourly basis and are requested by the agencies who we provide the services to. One of the things that have been pointed out this past year in the Hackett Study was that many of our agencies are performing manual services and those were deemed to be less than efficient. I think this is an area where the state could invest more to provide more automation and we could become more efficient.

However, my services are at the request of the agencies we serve. So we do make recommendations to add programming staff, but that programming staff would have to be added by those agencies. In this budget cycle, we're not asking for any new positions and, in fact, we are moving a couple of positions out to agencies that we've been performing services for, but those agencies would like to perform those services in-house.

Our web team is currently engaged in migrating all state websites that we support to our new content management system. I guess it's not new anymore, it's almost 4 years old now. Over a hundred of our websites have been converted to the Ektron CMS. It's been very effective, very successful as a project. The Nevada home page, the Governor's websites, most of the departments have all been affected by this upgrade. And I think if you've been on any of the state websites in the past two years, you'll have noticed a great improvement in the websites that we now have.

Some agencies who had traditionally been contracting their websites have also come to the state for their new websites. One of the successes we had was with the Attorney General's Office coming over onto the Ektron system. We are currently completing migrations with the Department of Administration and the Department of Public Safety. We're working with the Department of Health and Human Services on some of their websites.

The biggest problem we have in this area is we just don't have enough staffing to do the development as fast as agencies would like us to get it done. That's one of the primary reasons agencies go to outside contractors is because we aren't able to do it as fast as they want us to do it. I have in the budget requested one additional developer. We would also like to be involved more in mobile application development. In the last budget, we were given some seed money to

go out and look for a contractor to do some mobile development, but that didn't work out very well for us. And so we asked for a mobile position -- a mobile developer in this budget.

We are also integrating our web services group with our application services group. We feel that in the web and the mobile application area we can make a lot of improvements. This is the area in the future that will really tie the public to government and give us an opportunity to improve the services that we provide directly to citizens. And so we want to look at all of our applications as though they should be mobile compliant and effective on the websites, as far as how they look and how they're able to operate.

Our database management group supports primarily SQL databases and Oracle databases. In the past, our SQL databases have been billed primarily by a billing tier system and some hourly development work. The Oracle is primarily all hourly billable, and then the agencies own their own equipment and their own software and licenses. We would like to move all of our databases into a service model, where we're providing database as a service where agencies can bring their databases to us and we'll provide all the services for those databases on a tier level billing-type model. We think that'll improve not only the way we perform the services, but it'll give more agencies the motivation to move their databases to a more secure site. And consolidating databases is one way the state could save a lot of money by not spending money on disparate licenses and disparate equipment.

So with that, our hope is to eventually eliminate the hourly billing for database support and put everything in a database as a service-type model. Those are the three areas and those are the primary budget objectives that I have, if you have any questions.

Joe Marcella: Joe Marcella for the record. One of the things I heard is you're going to distribute some of your resources to individual agencies.

Alan Rogers: Yes.

Joe Marcella: Am I understanding they remain your employees but they have the keys to the kingdom? That means that they can do for them whatever needs to be done based on the matrix, resource availability, as well as rights and privileges of your organization.

Alan Rogers: No. These are three…

Joe Marcella: Or did I read too much into that?

Alan Rogers: Yes. There's three positions -- this is Alan Rogers. There's three positions that are really stovepiped into two agencies. Two positions work exclusively for the Department of Transportation. So we've agreed with Transportation that those two positions can move over to their agency and it does not affect any existing applications that we currently manage. There is one position that works exclusively for the Department of Education. It does primarily reports and updates to their applications. So that position can move over to Education and will not affect anything that we do.

Now, if those agencies wanted to consolidate, obviously those positions would come back, but these three positions will not affect anything that we currently manage within the Division of IT at the Department of Administration.

Joe Marcella: And I think my question is more as logistically could they be more effective by living and breathing within those organizations, but having access as well as rights within your organization?

Alan Rogers: No, because these…

Joe Marcella: They remain your employees but they live there.

Alan Rogers: Yeah. This is Alan Rogers. These positions aren't really pool positions. In fact, historically, the old do it organization tried to do a pooled application development group. And over the years that group dwindled down to just one employee, so the pool idea didn't really work. And we currently have -- all of our programmers are basically assigned in several different areas. They are stovepiped to a certain degree, but we are starting to do some cross-training and trying to use some people in different -- trying to group them by their core technology knowledge. And so these three positions basically would not have any access to anything that we're doing on the EITS side. They would strictly be on the business side in those two agencies.

Joe Marcella: Since the charge as an advisory group is to advise, typically organizations fair better when there is some level of relationship management both from a business perspective, as well as from a technological point of view, as well as sharing the resource, as well as sharing the rights in making sure that, as you mentioned before, vertical databases get not only to be expensive but get disjointed. Then it makes it almost impossible to do business intelligence from an enterprise perspective when that's what exists, unless you can organize in some fashion to get all of that information aggregated in some data warehouse.

We all realize if they're disparate systems, disparate databases, how difficult that could be. If it could be done through people, is there any advantage by still having the tie to those folks and they're still really supporting the other organization? It causes a relationship, and that's merely what I'm trying to say. Unless the problem you're trying to solve is vertical horsepower and really just labor.

Alan Rogers: This is Alan Rogers.

Joe Marcella: Is it a labor issue?

Alan Rogers: It's basically a labor issue. In fact, my position, in coordinating those three positions, I really take up more time than we actually get benefit from. So moving that supervisory function over to those agencies really benefits me and -- for the fact that we incorporated DPS this past year and other applications. The organization has grown so that getting rid of just a little bit of supervision actually will help us a great deal.

Joe Marcella: And I appreciate your candid response. Any discussion? Boards north and south? Paul, you always have a question. Kevin, you always have a question when it comes to money.

Kevin Farrell: All right.

Joe Marcella: Rudy, tell him he can't have any money.

Kevin Farrell: This is Kevin Farrell. So your opening comment you mentioned that 80 percent of your budget is in maintenance. Is that annual vendor maintenance contracts? Is that what you mean or is that in programming time just fixing defects?

Alan Rogers: It is the functions that we perform, both in database administration and application development. Most of our work is for existing databases, existing applications. And so some of them you might call legacy systems, but most of them are fairly current, modern applications that we're maintaining. I'll give you some examples. Advantage has been talked about a lot. That's the finance system for the state, and we do the maintenance for Advantage. NEATS is the HR applications that we use for time sheets, training, things like that for the employees. Those are maintained by us. We do some enhancement, but very little new development in those applications.

NEBS is the budget application. There are some modifications and some new modules being built this year in both NEATS and NEBS, and those are being done by contract. They're not being done by our internal staff. So those are kind of some examples. Of course, the website that's new development as building pages and things. The actual programming that's done has relation to new applications. Sometimes those are done by contractors, sometimes those are done in-house. But 80 to 20 is about the ratio of maintenance to new enhancements or new development that we perform. So it's not referring to outside vendors, it's the actual work that we're performing.

Paul Diflo: For the record, Paul Diflo. I don't want to disappoint the Chairman and not ask a financial question. But I think what I want to do though is wait until after all the chiefs are done and then I'd be asking David what the aggregate percentage variance is to the previous plan. Thanks.

Joe Marcella: What's marvelous, Mr. Diflo, is that youth can remember all of these things. You younger folks can do that. For me, I need to write it down and ask right away or I will forget. So thank you. I appreciate it.

David Gustafson: Dave Gustafson for the record. I would say, Mr. Chairman, that our budget is very much still in flux and we do not have those numbers available to us. There are certain decisions that are being held until the governor recommends phase, so we don't exactly know yet because everything is still -- so many pieces are still moving.

Joe Marcella: Joe Marcella for the record. Mr. Gustafson, what I understand, though, is you will be submitting priority items, things that you would like to do so at least the Governor, as well as the legislature, is advised as to what should be funded.

David Gustafson: Dave Gustafson. That is correct. And those items are typically prioritized when we get to the Governor's recommended budget, and higher priority items tend to get funded and lower don't.

Joe Marcella: In all of this is there a revision to the organization in how it looks, reporting structure, number of bodies, skills inventory, and its relationship to where you want to go? Because we're talking about classified/unclassified. We talked about three positions for Mr. Ipsen. We're talking about positions here being refocused and redistributed. I think the Board would like to see an overall organization and responsibility chart and incorporated in that maybe some of the skills that are necessary and your current organization and where you'd like to take it, unless that's not possible.

David Gustafson: David Gustafson. Was that for me?

Joe Marcella: That was for you.

David Gustafson: That was for me, I think. At the moment, we can't do that. My budget is still in flux and we're still in negotiations about what will actually be a part of the agency request budget. And certainly that will also change going into the Governor's recommended budget. At this time, I cannot provide that. I just -- there's just not enough…

Joe Marcella: I'll ask the question differently. If taking the budget issue out of the way, taking the legislative issues out of the way, if you had none of those constraints or didn't have to go through those processes, do you know exactly the direction you would like to take your organization?

David Gustafson: Yes. And?

Joe Marcella: Then would you then be architecting your organization, based on the direction you'd like to take it, and then asking for funding as well as staff, and the category of staff and the skills don't necessarily make that happen?

David Gustafson: Yes. And that's why the BDR is so very important, because it's the statutory foundation by which that plan would be built.

Joe Marcella: And you've made my point. This -- and I'm pointing to the statutory -- the BDR, is essential to set a foundation so that you can move the State of Nevada forward in an intelligent strategic way to provide technology and services to our citizens.

David Gustafson: That is correct.

Joe Marcella: Thank you.

David Gustafson: And we'll talk more about the Hackett Study and why some of those changes, I think, are necessary. Dave Gustafson, by the way. Mr. Chairman, are we ready for the next? Anymore questions for Alan perhaps?

Joe Marcella: Anymore questions from the Board? Please proceed.

David Gustafson: Thank you. I'd like to call up Catherine Krause. I'm just going in alphabetical order. I started with Chris because he was next to me and now we're going in alphabetical order. We'll go to Catherine, Ken, and then Tom.

Catherine Krause: Good afternoon. I'm Catherine Krause, Chief IT Manager with the Client Services Unit with Enterprise IT. Client Services is responsible for three primary functional areas; IT planning and project management, help desk and computer operations, and desktop support.

One of the consistent themes of discussion by the ITAB over the course of the past year, which is also acquit in the Hackett Study that you're going to hear about later is that we need to expand our project management and customer service capabilities within Enterprise IT, and that includes staffing and tools. And so my initial budget request which, of course, has to go through the entire process, does reflect those items. I think it's a modest but significant step in the right direction.

So Department of Administration applications development projects continue to be managed primarily by staff funded to provide billable applications programming services. Basically the staff that Mr. Rogers was talking about earlier. And that takes their focus away from those services. We have project management staff that came over from Department of Public Safety and then we have a few other planning staff that are doing some project management. We are recommending adding some additional professional trained, preferably certified, project management staff to handle project management duties, allowing programmers to focus on programming.

Also, as we discussed in at least one prior ITAB meeting, most of the metrics of reporting that we provide are produced using manual processes, fairly time-consuming, in order to provide easily accessible metrics and information on projects we are managing to numerous stakeholders and decision makers, from elected officials to senior management to staff within Enterprise IT and our customers agencies we support. We do need improved software tools and so we're proposing to add improved tools for dashboards, management reporting, project scheduling, tracking and resource allocation.

Another concept that's been discussed by the ITAB has been that of customer relationship managers of some type. That would be someone that would be the go-to person that understands the business of our primary customers and acts as the liaison with those customers in planning and providing Enterprise IT services. We're proposing to add two FTEs, one for each of our

current full-service customers, primarily the Department of Public Safety and the Department of Administration. Those (inaudible) their IT shop and providing more than just -- I shouldn't say just, more than the infrastructure services that really are the core of most of what Enterprise IT does.

And then finally in regard to planning and project management, somewhat related to that, we're proposing to add another FTE systems analyst to focus on additional design resources similar to the thing I mentioned earlier about programming and having programmers doing design work. We'd like to have another resource to focus on that area if we can do that.

I have a few other budget requests for Client Services that relate to the other areas of responsibility that are in my unit. Currently regarding desktop support, industry standard is around 150 to 180 devices per technician. In order to meet the industry standard ratio, we're requesting a few new FTEs and to upgrade one position to provide those services. There's a few positions that are contingent on other projects that are being proposed through the budget process that would increase the devices that we need to support. So if those projects are funded, we may need additional staff to support those as well. And that was the highway patrols' mobile computing devices tablets that was just approved, kind of a pilot project at the IFC. And so during that pilot we will learn how much desktop support that takes and whether we really do need to add resources. It's very possible that we'll learn through that pilot and the results of that pilot that that would not be necessary.

Another item currently impacting our desktop support service levels are the unique and critical support needs of the Governor's Office. There are many video conference meetings similar to this one that are attended by the Governor. We have found that in order to ensure that there are no problems with the video conferencing connection throughout the duration of those critical meetings, we need to have a desktop technician present for the meeting. Unfortunately, that takes significant time away from the support we can provide to our other customers, given our current lean staffing ratios. So we are proposing a dedicated FTE to provide this support and other support needs of the Governor's Office. That would be their primary customer. However, you know, should there be no support needs from the Governor's Office on a given day or for part of a day they could, obviously, supplement our other staff.

We have other requests for additional and updated tools for desktop support staff, as well as training for desktop support, help desk and operation staff and the technologies that they support that are constantly changing. Finally, we have two agency-owned vehicles that transferred over from DPS. We're proposing to replace those with vehicles leased from fleet services. Those services are used mostly for our desktop support vehicles and we should be using that centralized function. Just like we are the IT experts, they're the vehicles experts so we should be letting them handle that.

That's a real brief summary of the requests for Client Services. So with that, I'll ask if there are any questions from the Board.

Joe Marcella: For the record, Joe Marcella. Obviously, I'm going to have to say something. Project management, contract budget, and the actual implementation of systems and so forth and all of the timeline management and the rest of it is the heart blood of any organization. You never know what the right and the left hand are doing unless you have that. My question would be is do you have a comprehensive mechanism for getting those projects in, what gets prioritized? Do you have signature authority from the Governor and/or the other agencies? Just how does that mechanism work? How do they get in the door and how do they get back out? How do you know you're done?

Catherine Krause: Catherine Krause for the record.

Joe Marcella: Is that an unfair question?

Catherine Krause: I don't know if it's an unfair question. I would say we do not have a single comprehensive mechanism. We have some mechanisms that came over from the Department of Public Safety that did have a process like that. That was within the Department of Public Safety. It still exists. It's basically the business people. There's a board that's comprised of primarily the various division administrators and chiefs within the Department of Public Safety, and that is who decides which projects we perform for the Department of Public Safety. Those are not IT decisions. We provide information about, you know, what the cost would be, how long it would take, that type of thing that is input into those decisions. We hope to bring something like that to our other customers, such as the Department of Administration. We haven't done that at this point.

There are some other processes that are part of the budget process, such as the state's technology investment request process. We do manage that process. And so for major projects that are proposed as part of the budget process there is that type of mechanism. However, your question about does the Governor sign off and approve those projects, I guess you would say through preparing the Governor requested budget, yes, but not as far as a sign-off on a particular budget request in the way I think you're asking. Does that answer your question?

Joe Marcella: I think much of the question is, since we're talking about budget, is that you're talking about adding several bodies.

Catherine Krause: Mm-hmm.

Joe Marcella: And those bodies need to be a resource based on some identified work. And I'm assuming that that's been quantified so that you know exactly how much labor you need and how much is currently on your plate and what's coming in the door. That's why I asked. It's hard to judge and I'm asking how you can make a judgment as to how many project managers you need. And I'm not telling you you don't need them. I think you do. But it needs to be based on current work and future work, and I'm wondering if you've got a mechanism to figure what that is.

Catherine Krause: We do. I think it's primarily through some of what Alan Rogers described as far as the application development programming projects, and those are a lot of what we do

manage. In addition to that, my team may take on other projects on occasion. I mean, I will say there are many, many more projects than project managers available. You're right that we need to have that data as part of our budget request, and I think we -- between all of the different units within Enterprise IT, we can easily show that we have many more projects that we could use project managers for than our current staff or with the few additional resources we're proposing we'll be able to cover, so -- but you're absolutely right, of course. We will need data to support our request and we will put that together as part of that. I don't have those details with me today to present to you, however.

Paul Diflo: For the record, this is Paul Diflo.

Joe Marcella: This is the last question from me.

Paul Diflo: Oh sorry, Joe.

Joe Marcella: Go ahead, Paul.

Paul Diflo: Yeah, I think what the Chairman was asking are pretty relevant questions. And what I hear you describing is kind of spot project management rather a governance process and portfolio management.

Catherine Krause: Mm-hmm.

Paul Diflo: And I think maybe what Joe is getting at is somebody looking at the entire portfolio of projects and resource management rather than just the individual projects? Typically, a portfolio manager then can help drive an RLI for the projects and get the resources and get the funding and do you see that as your role as you develop this project management team?

Catherine Krause: Catherine Krause, for the record. Yes, I think that could be our role. That's part of the reason that we're asking for enhanced tools to do that. Today it's a very manual process and I would say we don't have full visibility into everything that Enterprise IT is doing. We need to build that and this is part of what we're looking for is to start that process. I'm not sure if that answers your question.

Paul Diflo: Okay.

David Gustafson: Dave Gustafson. Paul, if I may.

Joe Marcella: Please.

Paul Diflo: Yes, sir.

David Gustafson: So what we have is that a condition where in public safety they had several project managers. Enterprise IT had none. And so what we've done is we have moved the DPS project managers over to manage DPS projects, but recognizing the fact that there are other projects going on, including a lot of infrastructure projects, a lot of development projects, the ERP, system upgrades, you know, router systems, data centers, you know, all -- you know,

everything else. So when we look and when we speak of project management we're talking in the context of Enterprise IT only. And I think what you and Joe are saying is statewide is there something there, and that is not the case. This is to solve an Enterprise IT/DPS administration challenge that we have, not to solve a statewide problem of real project management and real PMO.

Paul Diflo: Okay. That helps.

Joe Marcella: Yeah, it just brings back the question of what the organization is today, which you have on your plate moving forward and what you're going to make the organization tomorrow. And whether enterprise project management or just EITS project management is necessary will be determined based on your vision and the direction.

David Gustafson: Dave Gustafson. Remember earlier I was referring to enterprise services that the Governor may direct? That is a condition where we can begin, through whatever means the Governor may see necessary, to go ahead and to build those enterprise capabilities, because outside of that -- I just want you guys to know, outside of that our budget requests are for our agency only. I am not to budget for everybody else's stuff. This is just our own agency. So that's why when you hear the chiefs that's using the context of just our own things.

Joe Marcella: Now, a question for Ms. Krause. Then what you're telling us is that the staff that you're recommending is to fill the gap, not necessarily for that next level of enterprise?

Catherine Krause: Catherine Krause for the record. Yes, that's correct. So as I mentioned earlier, but I'll reiterate. Primarily, the resources will be focused on our development projects, but we also intend as really, you know, we determine we also would use these resources for infrastructure projects that we determine that we would like -- think these resources would be useful for. The number of staff that I'm proposing could not even come close to managing all of the projects that are handled by Enterprise IT, particularly in the infrastructure area. And so what we're trying to do, I guess in a summary, would be take some of the processes that we had developed for Department of Public Safety, I'd say merge it with processes that have been used for the Department of Administration, determine, you know, which of those to take across the enterprise, but it's definitely only focused on Enterprise IT projects, not the entire state. So I apologize if that was not clear.

Joe Marcella: Thank you. Any additional conversation, discussion? North, south? Okay. Let's go ahead and move on. Thank you very much.

Catherine Krause: Thank you.

David Gustafson: All right. Thank you. Thank you, Catherine. Let's call up Mr. Ken Adams.

Ken Adams: Good afternoon. I'm Ken Adams, Chief of Communications. My areas of responsibility are the statewide telephone system, statewide network, which is SilverNet, and also the statewide microwave system. And basically what I want to go over today is just most of the things in my budget are end-of-life replacements and also -- just mostly end-of-life

replacements and continuing with the phone system to move that out. Pardon me, I'm a little bit nervous. I don't do this very often. I spend most of my time with the technologies.

So basically on the phone system…

Joe Marcella: Neither do I, Ken, so it's okay.

Ken Adams: Okay. Basically, what I wanted to go over is the status of the phone system that we did get approved through the legislature last year, is that we've got the northern core infrastructure installed and we're in the process of converting the northern sites. And I think that we've done about 15 of the northern sites. And this is where we have to reconvert all the telephone lines from the old system through our service providers into the new system. So it's really quite a labor-intensive process. Our expectation is, is that we'll be wrapping up the north in November and starting on the south. And we have a total of about 49 sites, 25 being in the north and the remainder being in the south, and 3 over in Elko.

So that project is moving ahead and we're -- as far as what we're looking for out of the budget is we're looking for the continuing operation and maintenance of that system, as well as any endorsements that we could get through the Budget Office and the legislature to add new people onto the system that are on old key systems that may be in the neighborhood of somewhere 25 years old or better. And there are a lot of key systems. They're still using local dial service in the communities and especially in Las Vegas. A lot of folks are still using the local phone company for their phone service, so any long-distance calls that they make up to the north aren't actually long distance when they can come onto the state phone system that would be all in-network calling, which would reduce cost there. They also would need trunk lines and all the other overhead. So we're looking to get them off of those systems, one, because the age of the cost and also the security, because those systems are vulnerable to hacking from other countries.

With regards to…

Joe Marcella: Then your efforts -- please continue.

Ken Adams: Okay. I'm sorry.

Joe Marcella: I was going to ask you a question, but I don't mean to interrupt.

Ken Adams: Oh no, that pretty much covers the phone side of the house. If you have any questions I'd rather compartmentalize it before I can go on to the next one.

Joe Marcella: On the process and considering POTS, plain old telephones, my question would be are you providing any services? And I apologize for not knowing. You providing any services for county and city government?

Ken Adams: No, no.

Joe Marcella: From a state perspective?

Ken Adams: No, not at this time.

Joe Marcella: So this is just for the state agencies?

Ken Adams: This is just for the state, yeah. We have about 9,000 users on the state phone system now that we're in the process of doing the upgrade on. And there's still a hefty number of other ones that are still there that are -- especially in the Las Vegas area -- that are on POTS lines, although they may have DIDs and direct, you know, multichannel sets back in the phone company. However, any calling that they do intrastate is all long-distance and we'd like to see them get on the state phone system, because not only the economy of scale, but also reduce those long-distance charges.

Joe Marcella: Ken, do you find that you're diminishing the desktop phones and folks are using alternative communication devices?

Ken Adams: You know, at this particular…

Joe Marcella: Are you still planning for the same amount of devices on the desk as you've always had before or is that being reduced?

Ken Adams: No. One of the beauties of going to newer technology or past technology -- it was essentially '80s technology -- was that we couldn't do that. One of the advantages of the new core systems is once we get them up and installed is that we can offer a lot more mobility options with regards to phone. You know, a person can do all of their business with a cell phone rather than having a desktop phone. So that will open up, basically, a technology door to the state that's been shut for quite a few years based on not funding or not upgrading the old system.

Joe Marcella: So everything will be digital and voice over IP?

Ken Adams: Yes, sir. In the end that's what we would hope.

Joe Marcella: Thank you. Continue please.

Ken Adams: The next area I'd like to talk about is SilverNet, and really what we have is a couple initiatives in SilverNet. The first one is, is that we're looking to upgrade our distribution channels or pipelines, if you will. We've just gone through some bandwidth augmentations in the north for our internet service, as well as for our north/south service. And we're going to need to continue to do that based on user demand. They're just -- you know, there is not a permanent growth stop checkpoint. Growth and data is continuing to move. Databases are getting bigger. More agencies are using more technology. And in doing, that they're wanting to replicate more data north and south, and they also want more internet access.

Well, what's happening is, is that the applications are getting more sophisticated, more bandwidth intensive and now what we're running into is the rurals, which don't have a lot of services for increased bandwidth. And so one of the things that we're going to be doing is wanting to upgrade -- just basically because our circuits are full now or approaching full, is

upgrade places like Winnemucca, upgrade a community called Ely, which is in desperate need. And we'll talk a little bit more about Ely later. Winnemucca and some of the other areas that we have that need increased bandwidth to support the applications that the agencies are serving their programs on. So that's one of the big things that we're looking for there.

Also in Las Vegas, we have a space problem with where our network is currently housed and we'll be seeking to do that -- move from our current location to another location in more of a data center concentric facility rather than where we currently are. And so that'll be another part of our budget. One is for disaster recovery. The other is for interoperability with some of our sister agencies like NDOT and NSHE. And so by doing that, that'll open up a lot more connectivity options that we have between those three groups where we share a lot of expensive, high-value fiber optic infrastructure. And we share that rather than building independent long-haul infrastructure. So that's pretty much what we're looking at doing on the SilverNet side of the house. Any questions on that?

Joe Marcella: Yeah, and Ken, thank you. What's driving you from a capacity perspective? When you're done you're going to have 10 percent, 20 percent, 40 percent excess capacity? Do you know if it's based on contingency or what it is?

Ken Adams: I don't think…

Joe Marcella: I mean so that you can…

Ken Adams: Yeah.

Joe Marcella: Are you projecting for growth? That's the question.

Ken Adams: We always project for growth. However, since we're in a biennial legislature, we always run up against the stops at the end of the process. I mean we just ran up against the stops and we were just able to get past it. So we're already preparing for the next budget. I have a crystal ball out and I have to rub this thing every three, four years in advance to find it -- to try to think what it's going to be. As part of the processes that we go through with customer agencies, one of them we like to try to find out what they're expectations and utilization might be.

However, that never really comes to fruition on our part, so we end up having to, just by being in the nature of the business that we've been in for so long, forecast those growth patterns. Sometimes we do very well and sometimes we don't. But we all know in a high capacity network when we're at 70 percent we're essentially full. So sometimes it's hard explaining to management, well, you're only at 70 percent. Well, in a data network that's full, so…

Joe Marcella: This is a question for Mr. Gustafson. Since your obligation to the community is going to be social, mobile, information provision based on the needs, maybe a little bit of cloud in those communications, are you projecting through communications enough bandwidth over the next two years to at least grow those disciplines and channels?

David Gustafson: Dave Gustafson. I don't think we would be able -- we would not be able to budget enough for those capabilities. And what I mean by that is as we look at cloud technologies, which is a part of the overall budgeting -- theme of our budget overall, I don't think we can estimate that capability yet, because we just don't know. So I've asked for some pilot money in our budget to start testing out services like Amazon's Cloud services and things to sort of understand what those bandwidth requirements would look like and sort of the toll that it's going to take on our network.

If we went, for example, to an off-site cloud-based backup environment, let's say where we're trying to back up 100 terabytes of data or 200 or 300, that's going to have a dramatic difference on our capabilities versus, hey, we're just hosting some small application in the cloud. So it is, as Ken says, you know, it takes a bit of crystal balling. So I'm asking for, in the overarching budget if you will, a little bit of money to start looking at some of these cloud services to understand the impact on what they have on our infrastructure.

Joe Marcella: Innovation doesn't happen unless you have the infrastructure in place, so that would be the question. Any questions or additional discussion from the north?

Kevin Farrell: This is Kevin Farrell. Is there anything you wanted to mention about Ely? You said there was an issue there.

Ken Adams: Yeah, I have one more part which is the microwave system, the network transport system. And I was going to cover Ely in that because that's really important. Should I continue?

Joe Marcella: Please.

Ken Adams: Okay. The last area that I have responsibility for is the network transport services or the state microwave system. It's comprised of 114 sites around the state. Its primary mission is to provide public safety voice traffic back to dispatch centers, not only for NDOT, but for the highway patrol across the shared radios -- the Nevada shared radio system that NDOT administers. As part of what we do is that we provide the basic infrastructure, which is the communication lines to the mountaintops back to dispatch centers, and we also support every single state and county entity, as well as federal. We have a lot of federal customers, as well, with site space so that they can put their transmitters and radio equipment on our mountaintops. They lease rack space from us, and we're basically administering the site. Most of them are through BLM grants. And then what we do is we take care of the power. We take care of the generators. We take care of all of the infrastructure that keeps those radio systems running and support this infrastructure in a 24x7 environment due to the need for public safety.

One of the things that we did is in 1999, we were funded through the legislature for a three-phase system improvement, which converted us from analog to digital. We're now at the time where the system is approaching end-of-life, and the equipment going end-of-life in 2008. And so at this point what we're doing is we're going to reapproach -- fortunately, we don't have to build new sites, but what we need to do is we need to replace the electronic components that are in those sites.

And so we're advocating, again, the same approach that we did with the first system revamp is that we're looking at phase one, phase two, and phase three. Phase one would be from Carson City down to Las Vegas. Phase two would be -- well, Carson City to Las Vegas and a fiber access point in Ely. That's where Ely comes in. We have access to fiber in Ely, but we need to get the cross-connects done. And why Ely is so important is for a few reasons.

One, there's a prison out there, and that prison doesn't have any access to high-speed bandwidth for medical services and other things that prisons need to have now that they're doing telemedicine. And so one of the things we want to do is we want to be able to provide that service to the prison. That would also allow us to -- by doing the first phase from Reno to Vegas, would allow us to pick up the prison in Las Vegas/High Desert and that whole prison community. And, again, they're bandwidth challenged and there isn't any fiber optic remedy at this point due to expensive build-out from a CO or a phone provider to the destination. Those are millions and millions and millions and millions of dollars of build-out cost.

So we can close those gaps for those agencies with microwave. Is it a long-term epitome solution? No, that's not where we want to be. We want to be on fiber. But it is a stopgap for these agencies, and especially Department of Corrections, to solve some issues that they have with healthcare, also arraignments. Some of the things that they're now spending quite a bit money on, multiple T1 circuits too. We can consolidate that, put that on microwave. And working with our NDOT partner, bring the fiber into NDOT in Ely and set up a radio downlink so that we can bring the systems together.

One of the advantages of doing that partnership and tying back to the Highway 50 fiber across the state is we will double the capacity of the microwave system by doing that by having essentially two reins, one north and one south. What that'll help out is a lot of folks. It'll help out some customer base that we can't get to because our system is now in excess of 90 percent utilization. It'll also help us with being able to deliver different rates of bandwidth, which now we can only to T1s. We'll now be able to support Ethernet services. And so those backhaul connections to some of those data-starved communities could be met with the microwave system and the tiebacks to the fiber that we have with the partnership between NSHE, EITS, and NDOT.

So phase one is from Reno to Vegas. Phase two is Vegas to Elko, and phase three would be across the top along I-80 where we're actually doing a project with NDOT right now on ITS radio distribution. And so we have a lot of microwave equipment that goes across there that is end-of-life or will be by that -- doing this over three bienniums. By the time we get to the 80 piece, we'll probably be using some of our old equipment as spares to keep 80 running.

But we're just trying -- we can't physically do the whole thing in one biennium, so we phase it in three bienniums. That way when NDOT -- and we've been working with our partners there -- they are facing a radio upgrade then the infrastructure will be in place for their radio system upgrade. So that's one of the things. What we can't do is let the microwave system go like we did with the telephone system where it's unsupported, I can't get parts and it dies. That will directly affect public safety.

Joe Marcella: Thank you, Mr. Adams. Any additional discussion?

Rudy Malfabon: I have a question. This is Rudy Malfabon. I had heard that there was a challenge with getting some of those old parts and they, you know, as agencies change over their systems they have these old parts that are available for a short amount of time, basically like an eBay-type of thing or internet auction. Have we resolved that issue with state purchasing so that we can be nimble and getting some of those spare parts from some of these other agencies that are redoing their systems?

Ken Adams: You know, I don't know about the eBay or the, you know, that method of purchasing, but we have used third parties in the past to acquire parts that are no longer in production or out of production and people are wholesaling those old spare parts. The problem with that is, is that we're just continuing to -- you know, eventually we're going to run out of those spare parts because they are finite. And a lot of those systems get sold to other countries and they go away.

Joe Marcella: Thank you. I appreciate it. Any additional questions? Well, I have one comment and then we can move on. In Texas, they solved the prison problem. They just execute everyone. Any other discussion? Okay. I'd like to -- we've run a little bit long.

Unidentified: One more (inaudible).

Joe Marcella: Okay, please.

David Gustafson: Dave Gustafson. One more, Mr. Tom Wolf.

Joe Marcella: Oh.

David Gustafson: Tom is the last one here. Tom, if you don't mind keeping it a little bit short for us. We're running out of time.

Tom Wolf: Good afternoon. I'm Tom Wolf, Deputy Chief of Computing. David saved the best for last because he knows I'm fast. I'm going to talk about three hardware platforms and I'm going to talk about facilities. Those are the four business units I have.

The first thing I want to talk about is the mainframe. The mainframe is my workhorse computing power. It's got 5,000 users. It has very predictable growth. The welfare systems, DMV, systems like that, all their caseworkers and desk clerks use those systems. It consistently runs at about 12 percent growth. We balance that against the customer needs. We meet with the mainframe customers about once a month and do capacity planning. We have a pretty stable projected growth path for the mainframe. We're investing about 18 percent growth in the mainframe this year. Next year, we're projecting about a 12 percent growth and the year after that another 12 percent.

It's kind of unusual. It's the first time I think that I've been in the business here where the customer expectations and projections are pretty much in line with mine. Romaine and I have

had issues before where projections are like this and my projections are like this, and we kind of negotiate in the middle. So I think going into this legislative session, I'll have good customer support for the projections. I think it's a real solid plan. It is a million dollar plan every year as far as growth, but once again very much in line with the user growth projections.

A lot of the growth has been spurred on by healthcare reform and healthcare exchange, some of which ends up on the mainframe or the workload ends up on the mainframe. So it's looking like it'll be about $1.5 million in '16 and a couple million in '17, but I think we'll keep those customers happy.

The second hardware platform I want to talk about is our Unix customers. Those are financial customers, the DPS computer-aided dispatch system is on Unix, and a lot of the newer welfare systems are on the Unix platform. We have consolidated from 12 disparate systems down into 1 system called a PureFlex. The PureFlex is a concentrated hardware platform that has storage and engines and networking all kind of within one box. We will putting all the applications on that one box and using virtualization to slice it and give it to all the different customers. This saves us in labor costs. That platform is managed by four technicians, which can look across all those platforms and do the backup and the recovery and the storage management.

The last platform that we manage that we're budgeting for is the Windows platform. We used to have hundreds of Windows servers all over the state. We're slowly bringing those into the computing facility and putting them in a VMware environment, which is more servers on cards that go into big boxes that then are managed by one software application, and that allows our technicians to be able to reach out and do the work in a much more productive fashion. We really haven't increased that manpower in the Windows server environment for four years now, although we've increased the number of servers 300 percent.

So we've got a very stable workforce and a very growing -- it's my new business piece of the business. The mainframe is pretty stable. The Unix is pretty stable. The Windows stuff we grow when we grow. DPS added another hundred servers -- actually 200 came over. We'll consolidate them down on the new hardware to about 100. So we're asking for, you know, some storage, some bandwidth down to Las Vegas, and some of those blade engines to complement that.

The last piece of what I manage between the three platforms is where those platforms live. So I manage the computer facility here in Carson City, and we outsource those facilities down in Las Vegas to a place called Switch Communications. Switch has been a nice outsourcing opportunity for us. We didn't have to build a building. We didn't have to have that infrastructure down there and it does all our disaster recovery, our off-site backups. A lot of our storage is mirrored down to Las Vegas into the Switch facility.

I'm asking for two additional staff in that area. Because of some of the healthcare reforms, the exchange requirements, the feds are now asking us to do more security and disaster recovery auditing. They want better disaster plans. They want it to be more comprehensive, to be a little

more tolerant than it was in the past. And we really don't have the manpower on staff to do those backup, storage recovery, disaster recovery kind of operations. We're just doing kind of the basic you back it up and you restore the whole thing if you have to. There's two additional staff that really cover the gamut from mainframes all the way down to Windows to cover those kind of activities.

But also the facility in Carson City, one of the considerations on the table is really to kind of outsource the building and its maintenance to buildings and grounds, like most state buildings are. So in a nutshell, we're doing some mainframe upgrades and we're doing Unix upgrades. All those are bundled into one package. So if you look at the mainframe or the Unix or the Windows there's hardware, there's software, there's tools, there's storage, there's backup capability all within one budget request. So they look big, but there's a lot of components underneath each one of those requests. And there is, basically, one for each one of those categories so it's pretty simple from a legislative standpoint. Any questions? Is that five minutes?

Joe Marcella: Sounds like you're -- it was well done.

Tom Wolf: Okay.

Joe Marcella: And it sounds like you're in charge of life cycle management from a technology -- from the hardware/software infrastructure perspective.

Tom Wolf: Yes, sir.

Joe Marcella: And then you're managing for the next two years, is what I also heard.

Tom Wolf: Yeah, actually three because…

Joe Marcella: And that's…

Tom Wolf: …I'm in one.

Joe Marcella: Right. And that's based on everything that David's telling you he's going to do for the next couple of years.

Tom Wolf: I try to keep him happy.

Joe Marcella: Thank you. Any discussion up north? South?

Rudy Malfabon: I have a question. This is Rudy Malfabon. You mentioned using Switch Communications down south. Is there anything on the horizon for considering that as alternative in the north too or you're pretty much satisfied with what you have with the setup up in the northern area?

Tom Wolf: For the record, Tom Wolf. Well, the facility here we own. It's been in existence 35 years. We've upgraded it from time to time, but it's a class facility. It doesn't compare to a Switch as far as its disaster recovery capabilities, but it certainly meets our needs. It would be

hard to leave a state facility and do it competitively. But we're always looking at outsourcing opportunities. We outsource a lot of software maintenance. The CAD system I mentioned, the computer-aided design at DPS is outsourced to a technical team like mine and we want to leverage that contract and try to keep that outsourcing kind of model alive. We think it has good return on investment. So if there were a competitive facility in Reno or Carson, we'd look at it.

Rudy Malfabon: Okay. Thank you.

Joe Marcella: Okay. Thank you. Any additional questions? Sorry. Thank you, Tom. I have two things real quick. Lynda, do I have to end the meeting at 4:00 or can we go over a little bit?

Lynda Bashor: Hi, Joe. You can go until…

Joe Marcella: 4:30?

Lynda Bashor: …4:30. Correct.

Joe Marcella: Okay. Thank you. So I want a motion to accept the report. Can I have a motion?

Kevin Farrell: Kevin Farrell for the record.

Assemblyman Anderson: Motion to accept.

Kevin Farrell: I move to second.

Joe Marcella: Okay. Thank you. Anymore discussion? In favor?

Group: Aye.

Joe Marcella: Thank you. I'd like to call for a very short recess, five minutes, and then we're back here and I'll call the meeting back to order. And then we'll hear from Accenture. That gives you guys a couple of minutes, at least, to get yourselves set up and wipe all the cobwebs from all of my discussion and rhetoric up here. So thank you.

Off the record.

8. ACCENTURE PRESENTATION (for possible action) presented by Accenture

Joe Marcella: Two things. One is, is the next item is agenda item number 8, and we're going to hear from the Accenture folks. But the other item is, is we're going to go ahead and abbey [sic] the Hackett Study for a couple of reasons. One, it's huge. Second, it sort of parallels much of what we've already talked about today. And third, is I honestly believe it's going to be a huge amount of discussion that'll go along with that. So let me advise the Advisory Board to take a good close look at that study, because it identifies much of what we've been talking about. It also does a good job of showing some direction and it does a peer analysis across the United

States to show you where we actually stand as a state, and it gives you a hint as to how we can correct some of those things that we're not doing well. And it also gives you a good feeling about some of those things we actually do do well.

So it's important that you take a look at it. David Gustafson will give us an overview and I think we'll open it up for some conversation. Go ahead and go through the slides, mark those things that you want to talk about, and we'll have a lot of the next meeting to discuss those items and try to give David some direction based on that report, which is intended to give David some direction. So if I can turn over the meeting to the Accenture folks. Please identify yourself and proceed.

Lalit Ahluwalia: Thank you, Chairman, for the opportunity for us to come and present. My name is Lalit Ahluwalia and I'm part of the Accenture security practice, and I'm also responsible to lead our public sector security group, where I am really going and watching over some of our key states like California, Texas, and all. Plus I'm also responsible to really, you know, provide an overview and oversight over different initiatives that we do in this phase. So with that, I'm going to pass over to Kevin. Oh, okay.

Michael Montalto: Mr. Chairman, gentlemen, thank you for the time today. I'm Michael Montalto and I'm the managing director responsible for infrastructure security for Accenture's Health and Public Service Practice. So many of the things we've talked about today in this session and we'll talk about specifically the security (inaudible) in my purview for delivery to our state business. Pleasure to be here.

Kevin Richards: And, Mr. Chairman, I'm Kevin Richards. I'm the managing director with Accenture. I lead our North American security practice. And so I get the pleasure of working with these two every day and helping our clients across North America with solving some pretty significant information security challenges. Just by way of background, I've been in this space for 25 years, both on the private sector, as well as with our defense organization. So I've been able to see a lot of interesting things. And so hopefully over the course of today, if it pleases the Advisory Board, we have some materials that we made available. I think the PowerPoint presentation has been distributed across the group.

What I'd like to do -- we'll go through this as a starting spot, but really I'm interested in hearing your questions and making sure that we're giving you some insights, as well, along the way. So if I may, as we walk through this, just by way of the overview, talk a little bit about what we see within the public sector. Through Accenture's efforts, we've come up with a few key challenges, some core themes that we've seen be pervasive in this cyber security challenge. We have some perspectives on how to move into kind of a new approach. We're calling it an intelligent security, but some ideas of strategies of how to move a program forward, and then we'll wrap it up at the end with a quick discussion and a summary and, of course, we can do Q&A at the end or we can do it along the way, whichever pleases the Board.

So if we fast-forward, this is now on Page 4, we think about the headlines. I think we all see this day in, day out. The one that came in last week was this significant breach of 1.2 billion passwords. Relative to the headlines, I think there's -- I don't know if we're desensitized to this at this point, but we're seeing very, very big numbers. Now, I don't know really know if it was really 1.2 billion real passwords or if it was test accounts for maybe a test site or a development environment. The point is, is that when these things happen we react. Our leadership team says stop everything, go see if we were hacked, were we part of it, did we cause it, are we responsible, are we going to be sued.

The headlines have changed the landscape of where cyber security fits into an enterprise, because it's not just a technical conversation, it's a business conversation. It's a reputation conversation. And in your context it's about a trust conversation. So it's changing the landscape of this conversation. Now, in a very material way, however, online fraud or cyber fraud costs the U.S. citizens -- I've seen numbers ranging from $55 to $60 billion a year annually. This is the individuals having to go buy credit services, clean up credit card issues, having to clean up their credit reports. And that's a significant amount of money. So it's not just inconvenient, but it's costing literally billions for our citizens.

The other material impact is that when these breaches happen there's a material impact on using up budget that you frankly had earmarked for other things. You're walking in with a set number. Mr. Ipsen talked about your proposed request for next year. We're seeing per breach five times that amount is what it costs to clean that up. So if we look at some of the breach data that we do have, the average cost of remediation, that's hard cost of sending out the letters and the notification, the potential legal components, the other credit services that happen with that, are in the $5.4 million range per breach, on average, based on some statistics that we had last year.

Joe Marcella: And, Mr. Richards, I'm trying not to interrupt. But one of the things that you'll cover is cyber security…

Kevin Richards: Yes.

Joe Marcella: …in this conversation?

Kevin Richards: Yes, absolutely.

Joe Marcella: Thank you.

Kevin Richards: So it's both our reputational impact and a very real financial impact to businesses that's being caused by cyber security and cyber fraud. Okay. So if we go to the next page, why is this different or why is this special for the public sector? And we -- I'm sorry, cyber security.

Joe Marcella: I apologize. What I was -- I said cyber security. What I was really asking you was cyber insurance.

Kevin Richards: Oh, about cyber insurance?

Joe Marcella: Right. Will you touch on that during this conversation?

Kevin Richards: I will…

Joe Marcella: What you just mentioned is there's a huge knot and expense that goes right along with any breach.

Kevin Richards: Yes.

Joe Marcella: And a trend recently has been the purchase of cyber security. In the past -- there you go, cyber insurance. In the past, folks avoided it. It hasn't been very effective, but I'm seeing today that there seems to be more of a need for some level of protection, particularly for government, because we're a target.

Kevin Richards: Sure.

Joe Marcella: So if you touch on it even a little bit, I'd appreciate that.

Kevin Richards: And this is still Kevin Richards. I don't know if I'm supposed to say for the record every time if I keep talking, but I will. Cyber insurance is -- it's actually been around for maybe as many as 8 to 10 years. There are some commercially viable plans that are out there. I think that there's an interesting component around cyber security that allows for specific losses where you can -- when you can quantify the loss in a very material way, that could be a very effective medium. I think many of the challenges that we have when we talk the cost of a breach may not be as obvious when we think about people time, the amount of your resources that consume focusing on a breach, as opposed to doing their day job.

When I think about cyber insurance, we're not necessarily regaining trust because it doesn't fix. It just helps you with the financial impact, which is huge, but it's one component of a larger impact. So I think it's a viable medium. I think that there are some significant organizations that are putting together good cyber insurance policies, but I think that insurance is only one component of -- the financial impact that you're going to recover is going to be limited as compared to the total cost or the total impact of that breach, if that makes sense.

Joe Marcella: Yeah. I think the point I wanted you to make, and you did, is that it's not a safety net. It may offset some of the security, but it actually might be counterproductive, because now I feel safe and I've answered all of the questions on the questionnaire for the insurance so that I know that I've covered all of that in security, but it isn't necessarily targeted, focused or going to solve whatever breach or issue or problem…

Kevin Richards: Correct.

Joe Marcella: …I might have.

Kevin Richards: That's absolutely correct.

Joe Marcella: In fact, it might make my folks in the back room a little lax.

Kevin Richards: There could be some that would believe if I have an insurance policy I don't need to go do these other things, and I think that would be a false assumption.

Joe Marcella: That's one of the points I wanted to make. Thank you.

Kevin Richards: Perfect. So in addition to the challenges -- so I think from a public sector perspective, you've got kind of -- a bit of a general underinvestment in the information security budgets. Public organizations are just easy targets, and we'll talk a little bit about the threat actors and what they're going after. But there are a lot of politically motivated hacking groups that want to make a statement. And so going after a government, whether it's state, city or local, become very easy targets.

I think one of the biggest things that we're seeing right now in the marketplace is the accountability is now moving straight up the organizational hierarchy. As CEOs and CIOs and CCOs are being fired for breaches, I think it's making a lot of elected officials go how is this going to impact me. If something like this happens on my watch, does that impact my ability to get reelected? Does it have a negative impact on my ability to build confidence in my citizens? As we think about things like digital or e-Citizen kind of services where I'm trying to build a macro aura of how citizens interact with state and local government, whether it's paying my taxes, requesting permits for a building or whatever it happens to be, we want to collect that data because there's a lot of value in that. But implicit with that is a trust that you're going to protect it in the right way. So I think that it's a complicated topic.

So as I mentioned before, we've spent a lot of time talking with our clients, looking at the market on some of the core themes. And we're not going to get into specific attacks, because I think that there are a number of fundamentals that are kind of pervasive across kind of why this situation is right for these cyber security attacks to be so successful and so prevalent. So if we can go to Page 7. So we've come up with five core themes that I think are -- as you put them together, really help illustrate why the cyber attackers have been as successful as they have.

The first area is a growing gap, a chasm if you will, between what the business units want and how they go about doing their business and what the security organization is providing. When I look at statistics about shadow IT or services that are procured outside of the control of the CIO, some statistics show that this is as much as 40 percent of an organization's IT landscape exists outside of the control of the CIO. Many of the business units or groups see that the security organization is the world I call of Dr. No. Here are all the things that you can't do and put prohibitions on the way that they are able to do their services.

So for just lack of -- or get away from the resistance, they go and they do their own thing, maybe because they feel that their department is special or they just simply don't want to have to live within the specific confines, which I was really excited to hear some of the discussions earlier about, no, we're going to put this all under one mandate under the Governor. That's a fantastic thing, because consolidation is one of the solution points. But this gap appears to be growing wider, unfortunately, not getting smaller. And I think that's -- as a security professional, as we

try to protect the entire organization, the more that chasm grows the harder it's going to be for me to protect it.

On the next page, this is Page 8, we needed to have our organizations think beyond a compliance domain. One of the conversations that I have with many corporate executives and boards of directors is there's a pretty sizable misunderstanding of what compliance is and what security is. And when I look at the macro differences -- well, I'll change it slightly. And by the way, I really applaud what Nevada has done for data protection. The Nevada Data Protection Law was an order of magnitude better than what I thought was out there between Massachusetts and California, and really changed the conversation away from just about encrypting data at rest, but talking about intent, how are you intending to use the data, mandating that if you're going to collect credit card information, you know, it's now going to be part of the law that you shall be PCI compliant as opposed to making it an optional thing. So I really applaud the state for bringing that great thinking to the market.

But it's not good enough. If you think through the last four or five major credit card breaches, every one of them had a passed report on compliance, so they passed their audit for PCI. And so the question that I get asked by many executives is I don't understand, I have every piece of paper, every certification. I've got my PCI report on compliance. I'm SOX compliant. I have my HIPAA certification. Whatever -- how am I still being attacked and how am I still being unsuccessful? And the biggest area is around the fact that compliance is a backwards-looking kind of thought process in its foundational element. I'm going to create controls and I'm look back over the past -- whether it's 6 months, 9 months or 12 months, and did I do what I say I was going to do?

In some of those scenarios, the event may have happened 9 months ago, but it can take a long time, and in the cyber world that's an eternity. The compliance world builds a set of expectations, we call them controls, and these are intended to be the, you know, minimum standard by which we're going to evaluate these different capabilities. In none of the compliance realms are they saying that this should be your risk tolerance. This just says here's your basics. If you do nothing else, do at least these and at least you're going to raise the bar from a risk perspective.

Unfortunately, within most compliance realms, in fact almost all compliance realms, I can build a fence around what I can actually include into my audit. So I can suggest look at these five servers, but don't look at this one over here because that's not relevant. What we're seeing is that not only is it relevant, it's material. So if I can put a fence around it and that becomes part of my audit domain, it's a glimpse of quality, which I think is fantastic. Did you do what you said you were going to do around this particular domain? But it's not a glimpse of security. So I think there's a different there.

And then I think the other piece is just the evaluation of your timing of that review. If I'm looking at this on a quarterly or annual or every six month basis, it's simply not sufficient when it comes to am I protecting my business. So the wrap-up statement to this is that compliance

doesn't prevent a cyber attack. Compliance does a great job of reporting on a past cyber event that's already happened. From a security perspective -- and we're going to think about this from a holistic perspective, we have to think about around not an audit domain or a control domain, but I need to think about it from the threat, I need to think about it from my business, how I interact across the landscape. It needs to be driven by my departmental or business unit requirements, not by an audit domain. The scope has to include all of those things that interact within my enterprise, because like the chain it's the weakest link is what causes the door in. And we have to evaluate this literally on a real-time basis. We're seeing attacks in the nanoseconds and milliseconds, not months and years. So we have to change our viewpoint on this.

And so if you go to the next page, which is Page 9, the net result of this is the box on the left we have our perceived risk, which is -- this looks great in PowerPoint because it builds up and not so good when it's on a printed page -- most executives will believe that compliance risk is a macro part, you know, that's the major part of my security risk. In actuality, the box on the right, my enterprise security risk is sometimes two to three times bigger than my compliance exposure. And then there's this big box of implicitly accepted risk. And, frankly, that's that white space where a lot of these cyber-attacks live. The attackers aren't going in the front door that's highly fortified. They're finding ways around outside of your audit domain to find that soft entry spot. I'll pause there. Any questions on that?

Joe Marcella: No, I think it rings true. When you talk about PCI compliance, most of the time you're in compliance if you can garden wall your PCI environment off.

Kevin Richards: Mm-hmm.

Joe Marcella: So I understand this clearly. It's just -- and that's only one component. But if you ask my management if we're secure, most of them will parrot back that, oh, yeah, our financial transactions are just fine. We're PCI compliant. So…

Kevin Richards: Right.

Joe Marcella: …I think I understand.

Kevin Richards: Perfect. And then beyond that, if I look at where the money is being spent, if I look at the percentage of the budget -- the annual budget that's spent on compliance activities versus the other activities, it can be as much as 90 to 95 percent of the budget is applied towards compliance-related activities as opposed to the rest of that space. So we see a sizable misalignment of funding to the actual risk of exposure.

Joe Marcella: So when the state says it's doing some SIM auditing of continuous monitoring and some of the components, channels, that Mr. Ipsen talked about, they're headed in the right direction?

Kevin Richards: Certainly, that's a big part of it, and we'll talk a little bit about some ideas of how to move forward with that. But that's one leg of the larger agenda. It's still one piece. It's

still -- hopefully, all of his budget isn't going just into monitoring. There needs to be some other components around that.

Joe Marcella: And Chris will have lunch and the rest of it, so…

Kevin Richards: So if we progress forward, the other challenges that we're seeing, this blurring of the enterprise. So where does cloud, where does mobile, where does social fit in into the larger protection domain, and how do I get my arms around this device, the iPads and smartphones and how they interact with -- in your world, with the state or with the city? So when I look at the e-Citizen efforts that are out there and if I'm going to allow people to use their tablets and their PCs at home, what's that covenant of trust and how do I ensure that across the edge of all of that interaction? And it gets very, very challenging. Obviously, many organizations struggle with just getting a good inventory of what they think they own, let alone to where it gets extended out.

And by the way, this was slide 10 that I was going to. And I'm looking at the clock and I'll pick it up a little bit. I'm just going to slide 11. Right now we're seeing this significant rise in cyber-attacks and we're looking at these persistent threats and we're able to put them into three macro buckets for what we're up against from a threat landscape. We have these opportunistic actors. These are the people that understand some technology and they're going to run their exploits. They're not necessarily looking at a particular server. They're looking for a trait and then they're going to go try to exploit that particular trait.

In parlance, one of the attacks is SQL injection, my ability to inject a command into a web URL that was not expected by the application. If I'm an attacker, I might have a little applet that just goes and checks hundreds of millions of these websites, and if you don't have that vulnerability they move on to the next one. So, frankly, they're actually easy to deter and fortunately there's 900 million websites out there, so they've got a target-rich environment. They're easily dissuaded, easily understood. I'm not really worried about.

I look at the next area, which is we call the mob or the crowd swell, and these are the organized hacker groups that are really trying to forward a political agenda. And they're not necessarily there to steal any intellectual property or credit card numbers or identities. They're just there to prove a point. And we see a lot of this more in a disruptive category. So when we were painting up a few of the health information exchange environments we saw a huge swell, just to try to take them down, from people that didn't like the law.

So it's a different problem. It's a big reputational challenge. It's a money challenge because it costs a lot of time and money for people to get it back up and running again. We see these mob groups going literally industry by industry. There was a group that took out the banking industry in Norway. I'm not sure why they chose that, but they took out a banking group in Norway two weeks ago, and they took out 14 banks. Just to take them offline. They didn't steal anything. They just wanted to disrupt it. Our oil and gas companies go through this every summer for people that are protesting, whether it's offshore drilling or pipelines through Canada, or wherever

it happens to be. Our retailers see this right after the Thanksgiving holiday when they're coming into their busy season. So it does have a material economic impact, but they're not stealing, they're not committing fraud. They're just being challenging and annoying.

The third area which is, I think, the most insidious and probably the most expensive are these determined actors. And many times these are state-sponsored or criminally organized groups that are actually going after something very, very specific. These are the groups that are very, very patient and they're going after -- whether it's credit card numbers, identities, things that they can monetize in the market. And, frankly, they'll sit in an infrastructure for years and collect. They're not there to break. They're not there to disrupt your application. They're there simply to collect.

And we think about this in terms of some of the retail breaches, where you've probably seen some of the headlines. That was an organize effort. They knew the environment and they were collecting credit card numbers to exfiltrate and then put out on to the open market. So these are the ones that are probably the most difficult to catch, which is where the monitoring component comes in, because that's a huge part of that. They're also the most expensive internally and to consumers, because they're siphoning off billions of dollars of data.

Joe Marcella: (Inaudible) Joe Marcella. Is there -- can you talk about proportionately -- if you were saying 100 percent of the population that's concerned -- or involved with trying to breach or disrupt or what have you from an opportunist to mob to determined actors, if you were to take 100 of those folks, how many are there proportionately?

Kevin Richards: In percentage?

Joe Marcella: Yeah.

Kevin Richards: I would think, and this is just rough order of (inaudible)…

Joe Marcella: I'm asking who is the biggest threat?

Kevin Richards: Yeah. This is probably -- well…

Joe Marcella: In numbers.

Kevin Richards: …as far as quantity, I would say 70 percent of the activity are these opportunistic. It's probably 20 to 25 percent mob and the rest in the determined actors. That's in quantity of attacks.

Joe Marcella: I would understand the bigger risk is disproportionate to the number…

Kevin Richards: Right.

Joe Marcella: …to the number of bodies.

Kevin Richards: Right.

Joe Marcella: But from a systems perspective, because you have to protect against all of that…

Kevin Richards: Mm-hmm.

Joe Marcella: …that brings to mind his continuous monitoring, opportunities, the PCI compliance, and everything that's particular to each one of those then you have to protect against all of it. So that was the nature of my question.

Kevin Richards: Yeah, absolutely. And the other good thing is that that wide number of opportunistic actors, you can eliminate a lot of that noise through the things that you're probably already doing; effective patch management and effective upgrades. You can deploy some technologies so that your signal-to-noise ratio gets better. And the things that you're worrying about are the ones that are actually the most risky to your environment, so, absolutely.

And then to the next page, the other piece, and I think you've already hit this a little bit already, is there's a huge supply, demand, and balance in the security space. There's actually negative unemployment in the security space. One report that I saw said that there were 23,000 defined but unfilled security roles in the United States. So we just don't have enough people to satisfy all the roles that we need to do this the right way. And then when you layer that on top of the fire drills that you go through, many times when there's a compliance issue, it's the drop everything, go run and go fix that. There's a big imbalance of people and we spend a lot of energy maybe not doing the most effective things, but it might make an auditor go away or it might make a particular political issue go away. So that's a big problem.

Okay. I'm going to speed up a little bit because I think that this is -- everyone's nodding yes and it seems that this seems to be resonating. And I'm going to probably spend the rest of my time -- I can do it on Page 15 and then we can talk through the various components. So when you think about, okay, now what? So, yes, we all agree with the problem and how do we get better? And as we look through this the five phases assess the current state. And this isn't about doing a compliance assessment. It's not yet another PCI assessment. This is really understanding where are we good from a capability perspective, where are there opportunities for us to leap ahead, where are there opportunities for us to take the technology that we've invested in and do more with it?

One of the areas that we look at, we call it active defense or intelligent security, machine-to-machine style protections. So are there abilities to take this monitoring environment with the rest of my environment -- I know every time that that is, for example, a phishing attack. Why can't I let that technology reconfigure my firewall to stop it? Why do I need a person for that? And the answer is we don't. And so are there opportunities across your infrastructure to look at the instrumentation that you really have and is the machine learning to make decisions at nanosecond and millisecond speeds, as opposed to putting it in a queue, create a ticket, and then someone goes and fixes it whenever they get to the next item.

Joe Marcella: Spend some time in my shop.

Kevin Richards: Absolutely. Evolving a security program vision to move from a control-centric world to a threat-centric world; what things can we be doing differently to understand the adversary and how we can most effectively defend against those that are going to cause me the most harm, as opposed to just the firefight du jour? There's a big component around focusing that energy to those items that are going to impact you the most.

Incorporate IT agility is looking at how do we leverage cloud; how do we leverage the different delivery mechanisms so that we can be more effective, but also getting our security people close as possible to those business units. And I heard this conversation a little bit earlier as well. So that IT isn't a monolithic Dr. No, but it's an enabler to maybe it's the digital identity for e-Citizen, maybe it's a new way of rolling out digital services to mobile and social. But integrating security people closer to those initiatives so that security isn't bolted on at the end, it's integrated into the core in the beginning.

Accelerate towards security intelligence is taking all of the instrumentation that you have, whether it's the SIM monitoring that you're already doing, the networking traffic data that you already have, to build a vision, a picture of what is actually going on so that I can get a good feel of where the real problems are. The gold, if you will, is in the noise and we can use analytics tools to pull the gold out and make some very good business decisions. And they're probably going to be very different than what you thought they were. And then the fifth piece is looking at different ways of delivery these services to your IT and your business consumers. Whether it's as a service cloud delivered security or creative uses of outsourcing arrangements, we have to figure out a way to deal with the supply imbalance, because the notional element that, well, we'll just leave those roles open is causing a lot of exposure and we need to come up with a different way of doing it.

So I'm looking at my clock here and I think I've hit my time on that. But the next slides really go into each of those into more detail. But I'll pause there and answer, really, whatever questions you may have.

Paul Diflo: For the record, this is Paul Diflo.

Joe Marcella: Anyone from the north? Paul.

Paul Diflo: Yeah, Kevin, let me ask you a question. My background is from the private sector and, you know, what I'm used to is having a couple tiers of IT security governance, the top tier typically is the board of directors where we articulate the risk and ways to mitigate that risk. But then the next level down is a group of business leaders that not only listen to and understand the articulated risk, but then make the decision on what level of risk they're willing to accept. And I'm wondering what you see in the public sector like that, and is it appropriate for Chris's department to be accepting that risk or is it a broader group of maybe agency owners that should get together to do that?

Kevin Richards: So I'll start with the consulting answer. It depends, but no. I think that the business unit leaders' departments have to be actively engaged. When you go back to that chasm

component, while I think -- whether it's Mr. Ipsen's department or the larger the CIO team in general, they need to be active, informative, and be significant advisors to that progress or that program. The various business leaders need to engage in a meaningful way. So I think that when you're dealing with governance from the public sector, you've got the elected officials, you've got the appointed officials and you've got the people that are hired. I think that there needs to be some shared vision on what that looks like and needs to be engaged in that into what's acceptable, how much exposure is okay, because I think there is no such thing as perfect security in any capacity, short of turning everything off, which is actually not perfect at all because then nothing gets done.

And while I think that your CCO and your CIO organization, they can own -- I think they can own the advisory process. Very similar to how your corporate counsel owns legal advice, that governance layer still gets to decide should I follow my lawyer's advice or not. That elected official could choose, no, I listened, but now I'm turning left. It might not be wise, but they can still choose to do that. I think that the CCO's role is very similar. They're your subject matter advisor. They're your guidance on those security challenges. And while I think that there's a lot of deference that should be given to that insight, at the end of the day the business has to agree, yep, it makes sense for us to turn left or turn right.

Paul Diflo: Okay. Thanks, Kevin.

Joe Marcella: Assemblyman.

Assemblyman Anderson: Thank you, Mr. Chair. Along those same lines, I think that, you know, the problems that we run into on the state level -- and I come from the private IT background as well, so I don't have as many of these limitations as the folks do on our state level. But agencies themselves are built around compliancy. They have Nevada Revised Statutes that they're forced to sort of abide by, and sometimes that certainly ties their hands as far as thinking about how can I best accomplish this goal versus how do I stay in compliance. So I think that that's something I'd like to hear about how we overcome that if you've seen experiences in that.

And just a couple comments. I think the shadow IT portion, in our state anyway, is significant. Folks that just go out and buy stuff and put them onto the network. But I don't think that that's in and of itself just the problem when it comes to that shadow IT realm, because as you expand services out to that e-Citizen, for example, you do become device agnostic, you have less control and certainly have to, you know, consider those issues as well on the security side. And that also leads, I guess, to the value of the data that's sitting out there. You know, we see entire business models wrapped around the data itself, not necessarily credit card data and what I can get with that credit card data, but simply the knowledge of what's going on. I mean, I think your social media networks and Google itself are fine examples of the value of just having data. We certainly use it in the political realm quite a bit, right?

Kevin Richards: Right.

Assemblyman Anderson: So I think, you know, the value of that data is changing, whereas it's not just credit card numbers and what the state absorbs in the data realm on the citizens that it -- or those folks that are trusting us to keep it. That could be a school district. That could be a lot of different things on both the local municipality levels. So I've kind of jumped around there, but I guess the idea of compliance…

Kevin Richards: Mm-hmm.

Assemblyman Anderson: …and how we overcome the thought, mindset, of doing something more proactive than opposed to just compliance side, as well as, you know, how we really overcome some of these threats.

Kevin Richards: Sure. So when I think about compliance, if I build a sound security program -- and there's a number of frameworks that are out there, whether it's ISO 27002 or the NIST standard. There's a few actually very, very good ones. If I build a complete program, compliance will already be satisfied. So if I do it right, I shouldn't have to do anything extra to be compliant. So a holistic security program will be compliant, but a compliant security program may not be holistic, if that makes sense. So I think that compliance should be an outcome, one of your outcomes that you desire. But ultimately there's about how I protect the state, the city and the citizen are also outcomes that become part of that. So I think that you can manage through that and that just becomes one of the requirements.

The next area you talked about, shadow IT and how that's growing, and that could be very good from a social/mobile. There's a lot of things. There's goodness in that. When I think of the channeling, though, the corollary is we also have a covenant of privacy. And just because the group or the agency did their own thing didn't mean the privacy expectation went out the window. And it's hard. This is a hard problem. What data is -- you know, we talked about the value of data. What's acceptable to accept and how can I use it, and in what context can I use it?

And you're right, the heuristics that I can pull out of, you know, what this -- it's almost a little bit Orwellian that you can get to depending on who has access to what cuts of data and whether it's predictive. Well, you've sped four times through this area. Here's the fifth time. We're going to proactively just send you a ticket. Of course, that would never happen. Or things like we have this person who is on welfare or Medicaid, Medicare. We have a lot of statistics that are on that. Should medical service providers or drug providers be able to market certain things to those people? Well, right now the answer is no. I mean HIPAA does a good job of that, but there are some areas that, depending on how you slice the data, I can determine heuristic behavior even though I don't touch HIPAA data.

So I think there's a really slippery area that that's where that changing value of data is happening. So I think that you're right, the credit card number itself -- I don't know the exact numbers, I mean at one point it was something like for every hundred valid credit card numbers it was five bucks that you could buy it in the black market. So just -- and it was in lots of 100, which I thought was great. So that's not the real money. But what we're talking about some of this other

information and how I can correlate this to -- whether from a marketing perspective or other uses could be quite valuable.

Lalit Ahluwalia: And if I may add just a couple to number one, compliance piece, to your question. It's a very valid observation, especially from the public sector where a lot of the agencies and departments are still struggling to even be compliant and don't even like have a holistic security program. But the prime example is the health insurance exchanges recently that we have seen, which came up with a lot -- you know, and established framework, which was NIST established framework and then map the (inaudible) state different regulations, and then use that as a leverage to drive the security program. And that's partly to the success of the health insurance exchange and the security that (inaudible) CMS put on that was more like driving security and privacy rather than just driving compliance part of it. So compliance was a byproduct of it, not like a compliant is the only driver there.

Joe Marcella: And maybe I misunderstood. What I've heard so far is that we talked about the threat landscape today. Are you prepared to talk a little bit, and I'm just talking like three minutes worth as to where this is all going? We've got a gap today for where we currently are, but if you wait 12 to 14 seconds that will change.

Kevin Richards: Sure.

Joe Marcella: And my concern is, is what is coming?

Lynda Bashor: Joe?

Kevin Richards: Sure. I'm sorry?

Lynda Bashor: Joe, unfortunately we can't…

Kevin Richards: Is there another question?

Lynda Bashor: …we can't go any longer. We're past.

Joe Marcella: Well, then thank you.

Kevin Richards: I'll hold my comment then. Thank you very much for having us. We really appreciate the…

Joe Marcella: Talk offline. Thank you very much. The next meeting, is either in October or November.

9. HACKETT STUDY BRIEFING (for possible action) presented by David Gustafson, State CIO and Alan Rogers, Chief IT Manager of Development

10. INFORMATION SECURITY UPDATE - LESSONS LEARNED FROM RECENT VIRUS REMEDIATION presented by Chris Ipsen, State CISO

11. PUBLIC COMMENTS

Joe Marcella: I want to ask for public comments. Is there anyone up north? Anyone down south that wants to make a public comment? Hearing none, seeing none, I'm going to close the meeting for public comment.

12. ADJOURNMENT

Joe Marcella: And I want to get a motion for adjournment.

Assemblyman Anderson: Motion to adjourn.

Joe Marcella: Second?

Ernie Capiral: Second.

Joe Marcella: Thank you. We're adjourned. Appreciate it. Thank you, Lynda, and folks up north. I certainly appreciate it. Everyone on the Board in the Northern Division, I kind of missed you. I normally would get lunch from David, and I didn't get that today. So I think I'm just going to have to buy the man dinner. Thank you. Appreciate it. We'll see you in November -- or I'm sorry, October or November.

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/dtls/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.