*** NOTICE OF PUBLIC MEETING ***

INFORMATION TECHNOLOGY ADVISORY BOARD

LOCATIONS:

Legislative Counsel Bureau 401 S. Carson Street Room 2134 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: September 24, 2012, 1:00 p.m. - 4:00 p.m.

Below is an agenda of all items to be considered. **Action will be taken on items preceded by an asterisk (*).** 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

Joe Marcella: Call to order.

2. ROLL CALL

Lenora Mueller: Let's do roll. Assemblyman Bobzien?

No response heard.

Lenora Mueller: Mr. Breslow?

No response heard.

Lenora Mueller: Mr. Casazza?

Cory Casazza: Present.

Lenora Mueller: Senator Dennis?

No response heard.

Lenora Mueller: Mr. Diflo?

Paul Diflo: Present.

Lenora Mueller: Mr. Farrell?

Kevin Farrell: Here.

Lenora Mueller: Ms. Fucci?

No response heard.

Lenora Mueller: Mr. Marcella?

Joe Marcella: Here.

Lenora Mueller: Mr. Mohlenkamp?

No response heard.

Lenora Mueller: Ms. Parker?

No response heard.

Lenora Mueller: Mr. Willden?

Mike Willden: Yes, in Carson City.

Joe Marcella: Okay.

Lenora Mueller: That does not constitute a quorum, Mr. Chairman.

Joe Marcella: We need one more?

Lenora Mueller: Yes.

Joe Marcella: Okay. So the only thing that's an issue is obviously approval of the minutes and adjournment. So hopefully somebody will show up or we're going to be here all night.

3. PUBLIC COMMENTS

Joe Marcella: All right then. Public comments? I don't see anyone down south, and there's no one to tell me whether there's public comments or not. How about up here in Carson? Same, hearing none? Okay.

* 4. APPROVAL OF MINUTES: July 9, 2012

Joe Marcella: Let's move on to approval of the minutes. We'll go ahead and table that for now, and then I'd make a couple of quick comments to sort of frame this meeting.

5. CHAIRMAN'S OPENING REMARKS
-Joseph Marcella, CIO, City of Las Vegas

Joe Marcella: In front of you, you have an Agenda. There's three salient points and components with the Agenda that I thought would be important, one of which is I'd like to talk a little bit about strategy forward for the state's IT organization, and more or less what the communities have been doing across the United States, and I've asked an individual from -- Dr. Mechling from Gartner to do that. We've provided to the Board some thoughts and processes forward according to what we thought would be important for cyber security, to sort of round that out and give us a little bit more of a framework that's necessary and some background as to where cyber security was, where it is today, and what our opportunities are in the future. And I'm not so sure we're supposed to say opportunities. I've asked Mary...

Mary Siero: Siero.

Joe Marcella: …Siero, thank you, if she would talk us through that. The other item I wanted to provide was to go over very briefly the Technology Advisory Board's Advisory Document, and just what's contained, and then submit it for either discussion, or to submit it for discussion and for the record. And then lastly, I wanted David to, if he would towards the end of this, just to talk about the current status of the security -- I'm sorry, your technology strategic approach, and anything that is popping up with budget because we're getting very close to the legislature.

6. SUBMISSION - Board's Recommendations/ADVISORY Document

Joe Marcella: That said, if you'll bear with me, I'd like to talk a little bit about the Advisory Document and what's contained. For the last five meetings we've had folks up here getting together to talk about five priorities, and then discuss in detail what those five priorities might mean to the State Information Technology group. In that we categorized four -- I mean, the five areas where we think there might be some benefit. So we were advising on consolidation. We've advised on the opportunity for consolidation. And there are several pages in reference to security as being an important component of the strategy forward for the state's IT, governance obviously. Let's wrap some rules around all of that. Application, modernization, and life cycle, and the citizen's applications, obviously there's some use for all of the products that are produced at the state level. The thing that's important about the application and modernization life cycle is somewhat of the benefit from having all of the rest of these things accomplished and some strategy forward.

So to move forward, I'd like to submit this to the state as our Advisory Document and open the floor for any discussion about the document. Anyone at the Board? Did everyone read it? You did. Exciting reading, yeah. There's a cover of what we believe on the five major objectives

that need to be addressed at the state. Does it reflect the priorities that we've talked about overall?

Unidentified Male Voice: I think it does.

Joe Marcella: Does it seem to represent the Board's thoughts and we haven't left off anything, at least for today? I think standardization and other things will come up later on in other meetings. Okay. Then we respectfully submit that document.

7. GARTNER - NATIONAL TECHNOLOGY DIRECTION -Jerry Mechling, Vice President, Gartner

Joe Marcella: At this time I'd like to introduce Dr. Jerry Mechling. Everyone has a biography in front of them. I can read this real quickly. Dr. Mechling is the Vice President of Gartner Research, focusing on -- can everybody hear me okay, because I don't have a microphone? Everybody's hearing me all right?

Unidentified Male Voice: Yes.

Joe Marcella: Vice President for Gartner Research focused on helping government and their corporate and non-profit partners, issues of strategic planning, work process, innovation, implementation, governance, information management and analysis. Dr. Mechling is also a recently retired lecturer in public policy at Harvard University, John F. Kennedy School of Government where he's written a series of policy papers.

Laura Fucci: This is Laura. I wanted to let you know I was here.

Joe Marcella: Okay. We can now -- Laura, welcome. It appears now that I have a quorum and we can now adjourn at the end of the meeting. So welcome.

Laura Fucci: My apologies for being late.

Joe Marcella: It's okay. Finishing up. There's eight imperatives for leaders in the network world at finding and funding IT initiatives in the public sector. What I wanted to do is I've asked Dr. Mechler to talk -- Mechling, I'm sorry, to talk to us about national technology trends, the evolving best practices in government and at the state level. Dr. Mechling.

Jerry Mechling: Thank you very much. I'm glad to be here. Harvard University is a very interesting place to work and that many people come to the university. One of the good things Gartner is it gives me a much better opportunity to come out to where people are working (inaudible) so I enjoy this kind of session. What I'd like to do briefly is talk (inaudible) chunks

of ideas. One is the similarity that many governments are facing in terms of the problem. Technology, even professors can sometimes figure it out MIC, what does that stand for. Talk about the similarity of the problems, talk about the fact that not all jurisdictions are responding to those problems in the same way. There is a great variety, some that are leading and some that aren't so leading, but of those that are leading, I'd like to point out five things that we're seeing happening in a variety of jurisdictions, and then hopefully have some opportunity for a discussion of the degree of fit or not degree of fit of those ideas out there, how they might apply in here.

First thing is, what is the problem that we're facing? Many people are noting that the conditions that government is facing recently, often referred to under the shorthand new normal, are different, and what's different is not just that the financial pressure is very high. We've been in situations like that before. But when they are cyclical situations, very often governments find that the smart thing to do is to basically hunker down, to not do anything foolish, to wait until the conditions come back, and to resume the standard operating procedures that you had before. What's different now is the sense that not only is the current financial pressure generated by a financial set of conditions that are slow coming back, and they're slow coming back in many places, but we have stacked up deficits in a demographic situation where many people, sort of my generation, are retiring, about to retire, or about to hit the Medicare and Medicaid situation, so that the longer-term solution to this is not going to be solved by simply waiting and hoping that we can get back to the other situation. More and more jurisdictions are recognizing that something pretty serious must be done to change the fundamental economic model of their government, and in particular, where possible, to make those services that are very important to be sure that they're the right services and that they are delivered as efficiently as possible. That's really what's different, and it's a situation that we see all across the country, and in many cases all across the world, although there is a variety in terms of how hard the economy is currently pressured, and some have seen these pressures for a longer period of time than others.

And that brings me to the second point. Facing the new normal conditions, and the fact that technology itself continues to explode in its fundamental productivity. Moore's Law that gives us processors that can process twice as many instructions this year as they could two years ago for the same dollar invested, and Metcalf's Law that gives us the economies of scale and networks. It's hard to imagine the world without the internet and how important it has become in the way we organize a lot of our activities. Those underlying trends for technology productivity are very, very, very important. However, and I say this as a ex-budget director in governments, that a lot of governmental folks fail to recognize, having many, many years where technology was important, but important primarily to do the financial calculations, and to do those repetitively well-structured pieces of work that were like financial management and reporting. We have had specialists handle the technology for those limited functions for which it was valuable for many, many years. And as a budget director, I can tell you on average it's rarely more than one percent of the budget that goes to technology, and rarely more than five percent of the budget that goes to all of the staff that provide that technology in the technology services.

And much of conversation in groups like this is how do we make sure that that five percent keeps up with the continuing revolution of Moore's Law and Metcalf's Law so that those services themselves are cost effective? What's different now is that many, many more jurisdictions are seeing that the real impacts of the technology are not in making the five percent more cost effective, it's will that allow you to reorganize the 95 percent of government that goes into public safety, into education, into tax collection, into the internal services like human resources and financial management. The kind of single story of what has happened and is about to happen that I find most both persuasive and instructive is to step back a bit, and I will tell you of a jurisdiction that has made technology reform in the 95 percent a serious investment for a long period of time.

The jurisdiction, a little different from most counties in Nevada or states in the United States, is the city state of Singapore, which some years ago, when I graduated from college, had an average income of $511 a year. Their average income in 2010 was more than $56,000 a year. They did that without oil, without gold, without any major natural resource, but they did see that the economics of the globe were going to bring multi-national corporations into Southeast Asia, and they did say that there would be a need for the headquarters kind of work, the knowledge work for that. They would need people who would handle the advertising, the management, the healthcare, the education, the logistics, the information infrastructure. And so they're economic development strategy was to say how can we have a cost-effective governmental structure that will work well with the private sector to make sure that the jobs that are increasingly going to go all over the globe and be knowledge based could be located in our jurisdiction. It's that fundamental shift in attention from the 5 percent efficiency goal to the 95 percent effectiveness goal that in some places is making technology a catalyst for very important productivity improvement that can change the long-term outlook for dollars per capita, life style, stability of the economy in that context, and that's what I really would want to talk to.

I would point your attention to Singapore as a place that has done this, to Michigan as a place that is doing this, not because -- I mean, in some ways very much like Singapore. Singapore was threatened to its core by not being able to sustain its economy and so it tried to understand and respond. Well, the auto industry, you know, ten years ago and more, created enormous pressure that everyone could see coming for Michigan. And in their regard, with technology, they went to consolidate and to try to bring efficiencies there and have won lots of awards over the years of having been the leading group in both identifying what's possible, working on it, often not succeeding the first time, but coming back to make very successful a number of things that they have done. The city that I grew up in, Columbus, Ohio, was interesting as a long period of time as the only city north of the Mason-Dixon Line and east of the Mississippi River that was growing its economy, and it was doing this largely around CompuServe, LexisNexis, the Ohio State University complexes, information age stuff. So having made two points, let me spend most of the time on the third, which is substantively what these jurisdictions are doing. I do believe it's important to recognize the conditions have changed and the fundamental problem has

changed, which is turning some leaders to look at the 95 percent, not the 5 percent, and there are examples of people who are out trying to make this work.

The five things I would like to discuss a little bit are those that are continuing to explore the scale economies of technology. Call that consolidation or movements to the cloud, that's one major theme I see in lots and lots of different jurisdictions. A second one, more recently, is the fact that many of the workers that need to be supported with information and good decisions are not at their desk. They're moving somewhere, and governments in particular have lots of work force in the field and lots of our clientele in the field so that mobile applications and infrastructure is another theme that people are turning their attention to. It's very important.

A third theme extends what's really been the big success for information technology in government over the last 15 years, which I would boil down to the phrase online not in line. That is for the public served by the government, can you reach it 24 hours a day by an internet connection instead of having to come in face-to-face in person, stand in line, forget to bring the pink form, have to back and go through it again. We have had success in that area, but there is a tremendous amount of unexplored opportunity for online service that becomes self-service, and I want to give an example or two of that one. That's the third big idea.

A fourth big idea is the utilization much more fully of the information that government has, not only sharing that program to program by performance management improvements inside the government, but by opening up that data to open government and making it available to the public and to those industries they could apply that information cost effectively to grow the economy so that the idea of open government is the fourth idea.

And the fifth one that will sort of wrap it all up and come back to the theme of the 95 percent, not the 5 percent, is the fundamental recognition that the decisions that are hard here, and important here, are only partly about technology itself. They're very largely about institutional change that has to be negotiated through a political process. It is getting the general managers of government, the budget directors, the department heads, the elected officials, the legislators to engage in these issues because that which makes them successful or that which make them fail is only rarely the technology itself and getting it to work. Yes. The technology is very powerful and it will create problems as you first come to grips with it. Like anything new it will be frustrating, and it will probably take longer and cost more than you originally hoped or thought, but the show stoppers are not there. These systems that come back there, they're much like shopping centers. If you take a look at most shopping centers that are created, you very often have a third owner of the shopping center who made a lot of money on it when it finally brought all the factors together in good work, and then we don't go back beyond that.

So those are the five things. I might give maybe one example in each of those areas and then just stop to see if there's any useful in back and forth about what we're seeing here and what you see. The first idea was scale economies, consolidation in the cloud. It is true that information

technology has enormous scale economies. If you program something once, it's very expensive. Windows 8, Windows 7, any of the Microsoft products, or any product, to do it right is a labor-intensive, intellectual property, huge effort, but the calculations that can be made, the transactions that can be handled once that's done are at a very low marginal cost. So the fact that we can now have an operating system that serves the globe, and not just one program in one jurisdiction is very important, and the same is true for networks. So while in the past we had every department and every program with a little bit to support their own, that is a luxury that needs to be reconsidered. Where can we get standards that will be the same across? Where can we have scale that operates? And classically this is consolidating, but it's also beyond that, going beyond the size of any one jurisdiction to, again, the cloud.

Ten years from now, much of what is information technology work will be organized by units that are larger than any one governmental department, and the role for government will be in adapting their work process to those new capabilities more than programming and delivering those capabilities themselves. So that's a big theme people are working on. Almost everybody I know has a consolidation and a cloud effort, and they often keep them as very different things. They're really making smart choices about a transition that is coming and will come. That's the first one.

The second on the mobile, I think we can all think about the mobile and the away-from-the-desk kind of applications, and the large quantity of time that life as a worker in government, or life as a citizen in any state is spent away from your desk, and the ability now to be supported with information is very, very important, and will become increasingly a game changer. Yes, the iPhone 5 is interesting for lots of reasons, but it stands as only one step in a pretty big movement that a lot of governments do need to think about. I would offer the phrase ready to hand as an important phrase in that what we're talking about is people making critical decisions based on the information they have available. Many doctors are making many decisions based on what they learned 25 years ago, but now many doctors in their walks through their hospital (inaudible) with an iPad have the information about the patients, the patient's family, the particular recommendations they are making to improve the character of those interactions and decisions. That will be a very big thing to think about as governments say where are the important decisions made and can we support them through mobile activities.

The last three ideas. Self-service, let me give you just two, I think, very powerful self-service ideas that people don't categorize as self-service. The first is to know that education is a huge deal. We've talked about technology and education forever and not seen very much progress, but if you read Clayton Christensen, a professor at Harvard, has written a lot about disruptive technologies and what they are, and particularly in education, and came out with some data that I found very interesting and would draw your attention to, and that's the fact that his prediction is that between 2012 this year and 2014, some 25 percent of kindergarten through 12th grade credits are going to be given not through the schools that are the local neighborhood schools that have been there forever, but those schools under cost pressure are increasingly saying if you

want to take Italian at this school this year, we can't afford it anymore. There weren't enough people signed up, but there's an online state virtual high school that will deliver, and what it means is that your time one on one with the professor or the teacher in a small classroom is being shifted to one teacher for more students, more of the students' time is interacting with the software and other students. It's much more a self-service educational opportunity where the interaction with a governmental professional is mediated by smart software that helps that take place. It's a much more self-service education, much more cost effective, and will be big.

The second idea I would give you is criminal justice. If you've been to Washington, D.C., you know it's not got a reputation as the safest city in the world. They have tripled the closure rate on violent crime over the last six to seven years. It used to be that only one in four of those crimes was solved in the sense that they caught somebody, put them through the criminal justice system, got a decision and brought punishment to bear. It's now happening three times out of four. And if you talk to Kathy Lanier (sp?) as I have who's the commissioner there, it's basically digital communications that they've used very, very significantly, and the new technologies. Partly through basically neighborhood watch on steroids with communication to groups in churches and in various communities that want to help the police solve problems and will provide information if they feel it's needed and used and they are protected. And she says the little old ladies still know everything that's going on in the streets if we can reach them, and they're trying to do that, and using the technology to do that, it's neighborhood self-service.

But in addition, they found that many of these crimes are gang against gang. They won't -- nothing will happen for two months and then something happens and three or four things happen in a period of five hours and that's retaliation one after the other. But they say we know how these gangs communicate because we come across them. They're on the same cell phones that everyone is on. The difference now is that in D.C. when we see a crime that we suspect is a gang crime, immediately the phone calls go out to every gang member saying that we're the police, we've got this, we know who you are, we know you may want to -- you better stay in for the next several days, because if we catch you doing anything that we possibly can, we're going to be as severe on you as possible, stay out of this until the police have solved it. She says now there are issues about the American Civil Liberties Union around this, but I'm just pointing out that in areas we don't think of as self-service, there is a technology-based opportunity to engage external parties in solving public problems like policing and like education that we need to be aware of as emerging and think about taking care of them.

The last two examples. The open government as information out there, there's a small piece of information I try not to take too personally which is the Gallup polls ever since I got out of college ask Americans do you trust your government to make the right choice, and they would give them four options, you know. How often does your government do that? Almost never, some of the time, most of the time or almost always. When I got out of graduate school, I started -- my first job was as an assistant to John Lindsay who was then the mayor of New York City. Very exciting time to be in government, very exciting time to be in New York. Eighty percent of

the American people said most of the time they do the right thing. We don't agree with them a lot, but most of the time. That figure is down in the teens and the low teens. It bops up and down. But basically around the globe the trust that government is trustworthy and accountable and is a good agent for the needs of the public, that trust is eroded. So much of what we need to do is not only convince ourselves that we're cost effectively delivering services and using technology for that, but over time, can we re-engage the public in some way that's respectful and effective.

Last idea behind scale economies and, you know, consolidation in the cloud and mobile work and self-service work and open government, is the fact that to make any of those changes happen, the governance structure inside government needs to be not just the Chief Information Officer, the technology staff and the vendors that support and provide the technology and the staff that runs it. These are really issues about will the people who are educators and in the classrooms, will the people who are policemen and protecting the streets, will the people who are collecting taxes and doing human resources transactions, will they change their mode of work to make it more transparent, accountable and cost effective? Technology is opening up those possibilities, and the jurisdictions that I think are providing leadership that will make the government respond to the new normal pressures more effectively and make their economies respond to the global pressures for where will the good jobs be 10 years, 20 years down the road. Those are the issues that I see as I look at governments around the country as leading-edge concerns. I hope that's interesting and would enjoy any interaction on those issues.

Joe Marcella: Well, you know I can't shut up. Joe Marcella, for the record, the one that can't shut up. A couple of things that I heard from you, Dr. Mechling, was one, we have to have a clear understanding of what our community's needs are, and everything else, whether we're talking about security, we're talking about delivery mechanisms, you talked quite extensively about alternative delivery systems.

Jerry Mechling: Yes.

Joe Marcella: You also talked about, and maybe this is my own interpretation, but the community out there, citizens, residents, they become part of your workforce, and they're participating. All of that needs to be clearly understood, analyzed, sorted as to what's the priority and which is the most important, where the best benefit is. And that's based on a community that's changed. That should drive a change in the back room essentially as to how those services are going to be delivered, which also has to change the mindset and also has to change your culture. So it's not a technology issue.

Jerry Mechling: Correct.

Joe Marcella: It's a community issue, and it's a delivery issue, and it's a matter of doing that in some consistent fashion, meeting the needs and keeping it in some level of government security and so forth just to make sure that it continues once you've made those decisions.

Jerry Mechling: Yes. No. I support that very much. I would come back and suggest that many of these things are new enough so that even though we want to be as clear as possible, we're going to have to take the courage to make certain decisions where absolute clarity is impossible. We can't prove beyond a shadow of a doubt the things that we are learning, and much of learning is those steps that didn't work out the way we hoped to. So part of what I'm suggesting is -- well, let me step back many years now because the program that I started at Harvard had to raise money, and I got some from government as policy stuff, but I got a lot of it from the standard technology firm community, and they were generous, and I can remember early on saying, okay, we're all trying to create value here. But we in the private sector have an advantage over you guys in government in that if it's valuable, we're going to charge our customers for it. So we tried to very carefully try costs and sales, particularly the sales.

Joe Marcella: Not to interrupt, but I understand David charges Michael quite a bit of money.

Jerry Mechling: So that's okay. So in looking at sales, the important thing that they told me was that in many technology firms, as many as half of our sales this year are from things that weren't even available five years ago. They've been invented in the last five years and everybody knows that. And everybody knows that five years from now, if we don't stay up with that new possibility, we are toast. So we're willing to put serious effort into the innovations agenda even though we have to stand up and admit that some of these things didn't work the way we hoped they would. Now, you in government don't have to be that close to the leading edge, but if you fall too far behind, you're a third of our total cost structure. The globe is going to push our work away from you unless you also learn where the leading edge is and how to get close enough to it, you know. The phrase I heard a lot in government is we'd rather be third. We don't really want to be first where if we're successful it's nice, but what really gathers attention is if we're not successful. But on the other hand, we don't want to fall too far behind, or ultimately we become a ghost town. So that was my thought.

Mike Willden: I'm Mike Willden and I serve as the Director of Health and Human Services. And so I'm kind of interested in your comments or thoughts along two of your areas, the mobile workforce and the online/in line.

Jerry Mechling: Mm-hmm.

Mike Willden: And for, you know, 70 years, my type of organization has been in the business of the food, clothing, shelter, you know, help business, and the struggle we have is that, you know, now that hierarchy of need, particularly for the poor, is food, clothing, shelter and some

sort of mobile device, and many of the poor have better mobile sophistication than my own workers do quite frankly.

Jerry Mechling: Mm-hmm.

Mike Willden: And so I guess my question is sort of, you know, I think we get it and we're moving that way. We have, you know, online projects, the self-service stuff, you know, there are keystroking applications. I don't have to pay somebody to keystroke an application. You know, we have lots of disease surveillance and we can get information -- push information back. But there really is still -- I guess maybe it goes to your other thing, that sort of change management thing. How do you get society as a whole to understand, you know, it's sort of like, you know, technology is only for the rich and not for the poor, and so we struggle with that. I mean, when we say we're going to go do this online and people say, well, how do they have the ability to do that, you know? We're not going to pay them their SNAP benefits and their TANF benefits and pay for their healthcare if they can afford a mobile device.

Jerry Mechling: Mm-hmm.

Mike Willden: So how do you -- what's your thoughts on how you work through that?

Jerry Mechling: Carefully is one answer. Because it is true that happiness is results divided by expectations, and there's a lot of expectations that are saying -- that doesn't mean my expectation as to what the poor -- how they live, how they should live, and whether we should do this, and maybe you're making a big mistake here. I think knowing that it is new we need to, again, try to make the business case, not the technology case. We're not doing this because we love the new tools or the new toys. We're doing this because we see that fundamentally the delivery of health services is going to require us for many groups in society, including the poor, to be able to reconfigure what we offer and how we offer it.

I think it's going to be very clear that my generation is going to have a lot more in-home healthcare to keep you out of the specific facility that provides you with the, you know, 24-hour care in a specialized location, the nursing home kind of stuff. It's going to have to recede to family and neighborhood-based folks who can, with the technology, help people live in the place they'd rather live for a long time. I would see that as an earlier -- not earlier necessarily, but a move that a lot of people understand is going to have to take place, and may well support those steps that are clearly aligned with that kind of transition.

But I think it is very interesting how much of our society now does go to healthcare and with the demographics how much more will. The pressure to say we can't do it the way we used to do it is going to be there and open up these possibilities. So if you're working on those kind of things, I think that's where you ought to be working.

Paul Diflo: For the record, Paul Diflo. Dr. Mechling, I enjoyed your information very good. Let me start out by saying I represent the private sector here at this table.

Jerry Mechling: Yes.

Paul Diflo: And I find that it's easier to get certain things done with business units because in the private sector we're typically motivated by the same thing, whether that's a stock price or bonuses. We may not agree who gets the profit or how to get there, but we're pretty much motivated by the same thing. So recently we recognized that we needed a mobility strategy and a distribution strategy. And while IT could push some things, we really needed to get a group of business units together to define the strategy that would move the company towards their goals. So I think that the five things that you stated, at least the top four, are relatively easy to recognize. It's that fifth category about, you know, the processes, and the people that make it challenging, and I'm wondering if you're seeing other governments that might put together a representation, a committee of different government departments to say, okay, as a state we need to have a mobility strategy, or a distribution strategy to help kind of move that along. My daughter's in public school. I talked to her teacher last week and she needs help in math. He said, you know, I'm really not supposed to tell you this, but you ought to go online and look at Khan Academy.

Jerry Mechling: Sure.

Paul Diflo: And it's great, you know, it's really good stuff. But what's going to motivate a group of state teachers to tell their union, you know what, I think we ought to promote this, I think we ought to bring this into the schools? And I know that's a lot of information. I'm just…

Jerry Mechling: No. I think that is hard. That is among the greatest frustrations that I think maybe all of us will have is -- I started this with saying that there is a new normal. There's a new set of challenges. I think most of us see that. And then I move to those governments that are taking action in what the leading edge is doing. What I didn't spend a lot of time on is that the average government now is still hunkered down, let somebody else go first, we're not sure what we're going to do, and so you do see some planning about technology, but the technology plans I see in government are almost always the IT strategic plan. It's not the budget for this jurisdiction and how it can evolve and be there. It's not very much the customer service strategic plan, or the performance management strategic plan, or the economic development strategic planning. I did see that in Singapore, my example. For year after year they pulled the people together to say where as a group are we going, and they had to get the teachers as part of this, and it wasn't always a consensus. You know, they had -- and there will be a lot of debate. I am hopeful that enough people seeing the reality that we're coping with can be educated to be supportive of an intelligent strategy that tries to address these issues in that way.

One of the things I would point to, I would argue that over the last decade Virginia did some very interesting things with technology as a state when Governor Warner was there. That New York City has done some very interesting things with technology with Mayor Bloomberg there. Well, you take a look and say it wasn't their CIO that convinced Warner and Bloomberg that technology might be a major catalyst for institutional success here. They had a lot of personal history. But you're now seeing, you know, Governor Snyder in Michigan, a Gateway person. I think there is an evolving set of leadership that will come to both public and private institutions that recognizes that this is the information age, and we need to respond to it more successfully, that will pull together, hopefully, the kind of groups that have to come together, including the stakeholders that think that they're losers in this transition, and their best hope is to just fight it off as long as they possibly can.

There will be some that will inevitably be that way, but I think a lot more -- I was interested in the State of Ohio where I grew up coming in to bring a shared services program in that required union support to relax the job descriptions and allow people to be shifted around, and there was a lot of effort suggesting that there's going to be a lot of training given, people will be allowed to take these new jobs, but they won't be guaranteed of those new jobs by their seniority, but that the work that we're doing here is not only important enough and the financial pressures are we're going to cut these jobs if you don't help us do this anyway, so there is a threat here that's real. But also, all the people getting this training, the career pattern now is you're going to have to have two or three different jobs in probably different institutions and that as a public sector worker, we're going to help your longer terms possibilities, not by just clinging to this particular job, but by making you a credible candidate for lots of different jobs. It didn't work for everybody, but it was pretty credible and followed through on, and I think was pretty successful as a shared services consolidation success story in Ohio.

Kevin Farrell: Kevin Farrell, for the record. I spent the week last weekend in San Francisco with 90,000 other people at Dream Force, which is Sales Force's annual conference. I'm very interested in what you've seen governments do with the cloud, perhaps at the application level or platform level even. Even in the Expo I really didn't see that much targeting government.

Jerry Mechling: Right.

Kevin Farrell: And then a second area under your point about the degrading credibility of government. The other major theme of Dream Force was all around business is social, and social business, social media tools are an essential new way of interacting with customers and partners, and if you see any of that taking hold as a mechanism for interacting with citizens and being more responsive and providing real time information to get some of that credibility back.

Jerry Mechling: Let me try to respond to both. On the cloud and government and the government's slowness is going there, I think that's all true. I think the cloud is coming and I think government naturally is going to be slow, partly because government is very worried that

the security concerns that we are more responsible for and privacy concerns that we are more responsible for and so we want to be sure we don't make a mistake, and there's more effort in the government to have government clouds, that is institutions that share our legal requirements and our cultural need to make privacy and security as prime concerns. So there is that testing and that slowness in that kind of response that you do see and, therefore, a lot of the early cloud work in government is very vanilla stuff. Email, you know, do we need 23 different email? No, we can go to -- and there are competitions there. So on the cloud stuff, I see that.

I also see a number of states -- I'll go back to Michigan. Michigan is now saying there are a number of smaller municipalities in the state that used to try to offer geographic information systems, licensing systems, financial management systems all on their own, and they're under such pressure now that they can't be cost effective. We at the state level are large enough to offer a state cloud-based series of applications that we can partner with the smaller jurisdictions, and so I see that as an emerging niche. I'm not sure how far it's going to go, but I do see it.

On your second element on will social be important, let me cycle back to my examples in the open government and in the self-service, the policing example of a neighborhood watch on digital steroids is really a social engagement effort, which I do see as a very important thing in the government. Another Harvard professor, Yochai Benkler at the law school, has made the big meta observation that we do, as individuals, we tend to do things for three broad reasons. Once we invented money, we found that was pretty interesting, and do a lot of market-based stuff, and once we noted that societies can have bullies and can people who don't follow the rules, and we do need governments and authority structures. And so a lot of what we do we do because an authority tells us to. But fundamentally we do a lot of what we do because we find those interactions reinforcing even if there's no money changing hands, a lot of our social interactions, et cetera. And the ability of the internet to open up lots of essentially social interactions that people get engaged in but produce major things like Apache, like Linux, like the open-source software world, and to take that into other social problem solving, be it crime solving is the example that I gave, be it the support that communities can give to educate people who need an education, continuing education, as well as childhood education.

I think we are going to see social, and the technology opening up the door to that, as increasingly important, but don't think it's going to happen very -- really quickly because government inherently is reasonably slow in its decision-making process, and it is a third of our entire social structure. So it takes a while for these things to take hold. Those are the things I would respond to. We're very interested in those details.

Joe Marcella: Just a couple of comments to wrap it up. Again, almost noted for stating the obvious, but a couple things I heard, one, is that there's a drive to an understanding the constituency, and we've talked about that before. The other thing that I just heard, and I'm going to summarize this into something sort of a little bit glib, but it's -- what you've just said was balance the drag of legacy with the pole of leading edge. And in a governmental organization,

it's not easy to be here at the higher end of technology until you've addressed this piece to pull it along, and that takes time.

Jerry Mechling: Mm-hmm.

Joe Marcella: Also, what I've heard is that not everybody is going to follow our idiosyncratic rules, and if you don't mind I'll cite an example. We placed kiosks all over the place at the city. Truth is, is that folks are not going to travel to the city to use a kiosk.

Jerry Mechling: Mm-hmm.

Joe Marcella: They only deal in cash, and it doesn't take cash. And the only reason they're there is because somebody gave them a ticket and they want a throat to choke. So in some instances, there's a purpose for government at the lower end, or at the end where you're dealing face to face and understanding who your citizens are, and understanding what kind of services you can deliver, and that adoption takes time.

Jerry Mechling: Mm-hmm.

Joe Marcella: Thank you. Any more discussion from the Board. Cory?

Cory Casazza: Just great comments and I appreciate listening to him.

Jerry Mechling: Thank you very much. Again, my final point would be to say I obviously believe that this stuff is important, and so I'm delighted that there are groups like your group working on these issues. I wish you all the best.

Joe Marcella: Thank you. Joe Marcella, for the record. Now that I have a quorum, could I go back and vote on the approval of the minutes? So can I have a motion to accept the minutes?

Cory Casazza: Cory Casazza. I make a motion that we approve the minutes as submitted.

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

Group: Aye.

Joe Marcella: Thank you. Okay. I actually had a vote for something and that's out of the way.

* 8. CYBER SECURITY OVERVIEW - The Current and Future Threat -Mary Siero, Information Technology Consultant, Innovative IT

Joe Marcella: Mary, thank you for waiting so patiently. If you don't mind, I'm going to introduce you. You have one heck of a history and a reputation, so if you don't mind. Mary Siero, I'm sorry, Siero, is an executive-level information technologies consultant with over 30 years' experience in engineering and technology in such industries as gaming and hospitality, healthcare, that one's specifically for you, Mike, consumer products, manufacturing and education. Over her career, Mary has developed and managed IT security, risk compliance, operational environments for multiple organizations, and has worked for Fortune 100 companies as well as for-profit and not-for-profit healthcare organizations. I'm going to skip down here a little bit. Among her notable accomplishments, February 2011 she was a recipient of the Chief Information Security Officer CISO of the Year Award. Congratulations, Mary. That was last year, so -- past recipient of the (inaudible)?

Unidentified Female Voice: (Inaudible).

Joe Marcella: (Inaudible), I'm sorry, Angel of Strength Corporate Achievement Award for Hispanic Women, co-inventor of the Hallmark patent for Long-Distance Greetings, team leader for Cadillac Division of General Motors' gold-plated ornamental team. Okay. Recipient as part of the Fisher Guide, and I'm sorry, the glasses are wrong, Division Team for Society of Plastic Engineers award for the most innovative use of plastics. Now, are there plastic surgeons involved in that at all? So I've asked Mary to talk about cyber security, past, current and the nagging future. Mary, if you would. Thank you.

Mary Siero: Thank you, Mr. Chairman and members of the Board. I'm honored for this opportunity to share with you some information related to cybercrime and cyber security. Cybercrime started long before the internet. More than a century ago, in the lecture hall of the royal institution in London, a wireless demonstration by famed radio pioneer Guglielmo Marconi was hacked during a public demonstration. Marconi had boasted that he had developed a secure way to transmit Morse code wirelessly using a technology he patented in which a wireless transmitter was tuned to broadcast on a precise wavelength. This tuning, Marconi claimed, meant confidential channels would be set up. From over 300 miles away he would send a message to a waiting audience. Before Marconi's message arrived, the distinctive tapping of a Morse code message sounded out. A message not from Marconi as planned, but from a public detractor interested in wireless technology by the name of Nevil Maskelyne. Mr. Maskelyne was frustrated by Marconi's many broad patents and wanted to embarrass him by demonstrating the lack of security in his patented technology. This hack into Marconi's very public demonstration was perhaps the beginning of hacktivism back in 1903.

Fast forward 90 years to the internet, and with it alarming growth rates for a new type of crime, cybercrime. As defined by the GAO, cybercrime refers to criminal activities that specifically target a computer or a network for damage or infiltration, and also refers to the use of computers as tools to conduct criminal activity. In the 1990s, cybercrime started out as cyber mischief, and cybercriminals were motivated by ego. Their attitude was, why did I do it? To prove that I

could. They attacked systems indiscriminately in an era that characterized by fast-spreading malware in the form of worms and viruses like (inaudible) and Blaster.

The next wave of cybercrime brought out those who were motivated by profit and more intense cyber-attacks began to take form. The favorite weapon of this era was the botnet. A botnet is a collection of internet-connected computers whose security defenses have been breached and control is given to a malicious third party. It wasn't enough to attack your computer, cybercriminals now wanted to take over your computer and use it to expand their attacks to other computers. To give a sense of the reach of botnets, we look to the well-known backdoor Trojan horse known as Storm Worm. Storm Worm is one of the more advanced forms of malware used in botnets and it infects via an email attachment. It was discovered on January 17, 2007, and five short days later on January 22, 2007, it accounted for eight percent of the malware infections globally.

Cybercrime hit the big time when hackers organized themselves into cybercriminal enterprises where they could take advantage of specialization and use organized business processes to grow and prosper. Online marketplaces for tools needed to conduct attacks began to appear and continue to be available to this day. Today you can purchase online software to exploit system vulnerabilities and malware kits that come complete with technical support. Malware distribution is facilitated through online services, botnets are available on a rental basis, and you can take advantage of a pay-per-install model and move into point-and-click cybercrime whether for profit or for a cause. The cybercriminal enterprise facilitated the ability to target victims, and it was the advent of these enterprises that hackers began to target victims, and it was the advent of these enterprises that hackers began to target specific victims.

Today, all of those types of cybercrimes still exist along with the new present-day threat from nation states. The arrival of cyber espionage, that is intellectual property theft, theft of U.S. trade secrets, and threats to our nation's critical infrastructure which are most commonly credited to nation states, lead us into new and previously unchartered territory. Last week on September 20, Warwick Ashford reported in computerweekly.com that the counter-terror unit, a security firm, Dell Secure Works has identified two separate cyber espionage campaigns that target energy firms throughout the globe. These campaigns are thought to be the work of the China Beijing Province Network. Eleven days ago on September 13 in his opening statement before the House Intelligence Committee, Chairman Mike Rogers noted that the U.S. has seen a 17-fold increase in cyber-attacks from 2009 to 2011. For close to a year, the House Intelligence Committee has been investigating the position our country should take regarding whether or not we allow the Chinese-owned telecommunication companies Huawei and ZTE to expand their footprint in the United States. At issue is the potential increase in risk to our government and to American companies for vulnerabilities that may be introduced into an infrastructure controlled by organizations which are based in China.

In 2010 the first-known cyber espionage attack on an industrial control system was launched against the Natanz fuel enrichment plant in Iran which produces low enriched uranium. Natanz, a secret facility until 2003, is a well-fortified plant sitting 8 meters underground and made out of concrete walls that are 2.5 meters thick. Despite the impregnable traditional security at that location, the Stuxnet worm found its way in. Most believe it came in on a USB flash drive or some other form of removable media. James R. Elsty (sp?), a security consultant, describes the Stuxnet work as quote, "A weaponized piece of malware that was developed with a specific intent," end quote. The intent being a design to attack specific frequency converters manufactured by Siemens for the Iranian plant. Due to the sophistication and complexity of the worm, many believed at the time it was developed that Stuxnet was written by a nation state. On June 1, 2012, in his New York Times article, David Sanger reported that Stuxnet was developed jointly by the United States and Israel under a program started by President Bush in 2006 and accelerated by President Obama shortly after he took office. This program code named Olympic Games was intended to cripple the nuclear infrastructure of Iran.

The attack on the Iranian nuclear enrichment plant is a real-life example in which a cyber-attack caused physical damage as Stuxnet systematically destroyed 11 to 30 percent of the centrifuges at the Natanz facility before it was detected. Because the industrial control system was not connected to a data network, damage was limited, but that hardly matters. This attack represented an astonishing leap forward in modern warfare, and highlighted a new security concern, the danger of an attack initiated in cyberspace causing physical damage to industrial equipment and crippling operations. The implications of such an attack should give us pause.

Kim Zetter reported in Wired magazine in January of this year that a researcher from Cambridge University found over 10,000 industrial control systems, including critical infrastructure such as water and sewage, all connected to the public internet. Damage to these systems could extend far beyond an individual facility and create a public safety concern. Equally troubling is the realization that the next generation of cyber weaponry has arrived with reports of Flame. Bigger than Stuxnet and more complicated, Flame appears to be used for intelligence gathering and spying. Since 2011, there has been an increase in cybercriminals committing crimes for a cause. Anonymous and (inaudible) have demonstrated to the world that cybercriminal groups that are passionate can wreak havoc on businesses or governments with whom they want to embarrass or prove a point. In cyber cause attacks, attacks originate from hactivists or nation states and the weapon of choice for executing these attacks is distributed denial of service. In August 2011, according to the Associated Press, Anonymous took credit for hacking into 70 sheriff's office websites and posting the information they obtained publically in an attempt to quote "demonstrate the inherently corrupt nature of law enforcement using their own words and disrupt and sabotage their ability to communicate and terrorize communities," unquote.

There is no way to obtain a true figure as to the extent or dollar value of cybercrime because most of it goes unreported. Unreported to avoid reputational losses, or unreported because companies and organizations don't even know that they have been breached or to what extent

they have been breached. However, we are able to survey the security landscape, thanks to the annual published reports of companies that report data about breaches they have investigated in business and in industry. These reports reveal trends and new developments and serve as harbingers of new threats to security. Cybercrime does not discriminate. The Symantec 2012 report shows that of the corporate victims, 50 percent are business with over 2500 employees. Eighteen percent are small businesses with less than 250 employees. Breaches span every industry and type of business from major corporations like Sony to security firms like RSA and even to a corner newsstand in Chicago. Typically breaches in private industry target credit card or other financial data, intellectual property and industry trade secrets.

The 2012 Verizon data breach investigation report reveals that in 75 percent of their investigations, it took only minutes from the time of the attack to the time in which the data was compromised. In 38 percent of the cases they investigated, data was exfiltrated from the organization within minutes, yet it took more than half of the companies months to discover the breach. The 2012 Norton Cybercrime Report provides some more sobering facts. Norton reports that there is a victim of cybercrime every 18 seconds, 556 million victims each year, and over two-thirds of all online adults will be a victim of cybercrime in their lifetime. The reported cost of this crime in the United States is $110 billion, which is more than the illegal drug trade and more than we spent annually on fast food.

With respect to government sponsored attacks, impervious research points to a heavy reliance on advanced, hard-to-detect attacks. With respect to attacks on government agencies, Rapid Seven reports that from January 2009 through May of 2012, government agencies suffered a total of 268 breaches consisting of a loss of more than 94 million personally identifiable information or PII records. The most common type of incident involves a combination of unintended disclosure and loss or theft of portable devices. 139 of these types of incidents were identified, and they totaled over 91 million records exposed. These statistics include one of the largest governmental data breaches in history. In October of 2009, a defective hard drive was sent to a government vendor for repair and recycling. That hard drive contained unencrypted PII records, including social security numbers of 76 million U.S. veterans. During the three-and-a-half year time frame included in Rapid Seven's research, they identified 14 separate incidents of hackers obtaining PII data from veterans at both the state and local levels.

Symantec's research reports that 25 percent of all targeted email attacks in 2011 were in government or public sectors. Other research shows that hacker attacks on governmental agencies use a combination of malware and phishing to collect public records and convert them into PII. In one specific example made public in May of this year in Utah, there was hack in May of this year in Utah where close to 800,000 residents health and Medicaid records were exfiltrated from a poorly secured server managed by the state's consolidated Department of Technology Services. Utah's CIO Steve Fletcher resigned over the incident.

In order to combat this massive assault on our governments and our economy, we need to better understand the enemy and how they operate so that we can build our fortresses of prevention in advance of when we will need them. The Duke of Wellington, Arthur Wellesley reminded us that when he said quote "The whole art of war consists of guessing at what is on the other side of the hill," end quote. The other side of the hill is revealed to us through the published reports from leading security vendors. Research from Imperva and others describe the increasing use of automation on the part of cybercriminals when they conduct attacks. These tools are popular due to the fact that they are publically available online, they have the ability to expand the attack base with little effort, they attack at a high rate of speed, and clever criminals can even use them to evade security defenses that look for patterns in attacks by programming in delays and other features that will circumvent detection software and processes.

Also from Imperva's research, we have learned the anatomy of at least one attack conducted by Anonymous in 2011. According to Imperva, like other hackers, Anonymous will use commercially available tools like (inaudible) and Acunetix to conduct a low-cost rapid attack. Unlike most other hackers, they have the resources to customize attack software if necessary. This is especially important if mobile devices are part of the attack plan. While we have not yet seen the first publicized breech where a mobile device has been used to pivot into an organization's data network, in private conversations, forensic security investigators will tell you that are currently investigating cases where they believe that to be the case. Until now, the biggest mobile cybercrime we have seen where a device has not been lost or stolen is toll fraud through the sending of text messages with malicious links to premium services.

In addition to the increased use of automated attacks by cybercriminals, two other trends are emerging that pose increased security risks for all computer users. Malware is being written to bypass traditional signature-based security detection mechanisms making it some of the most advanced malware we have seen. Malware writers have discovered ways to make rapid changes to their malware, employing a long list of file names and reproducing malware and morphing in an automated fashion. Also, since email has been a favorite attack tool, particularly for government and public sector attacks, cybercriminals are now employing disposable domains for use in spear phishing emails. This allows the email to fly under the radar of black lists or other detection techniques and is a low-cost, high-value addition to their arsenal.

Breaches happen due to a breakdown in people, process, or technology or any combination of the three. Too often, security fundamentals are not being widely implemented, and those that are, are not being maintained and advanced to keep pace with the cybercriminals. Verizon reports that 97 percent of the breaches they investigated were avoidable through either simple or intermediate level controls. Seventy-nine percent of the victims were targets of opportunity illustrating a people, process or technology failure. To further prove this point, Symantec recorded in 2011 the most widely-used attack PC vulnerability was four years old. Twenty-five percent of all websites had at least one critical vulnerability. Ninety-five new vulnerabilities were identified every week. One out of every 239 emails contained a virus. A unique variant of

a new malware was released into the internet every 13 seconds. And 10,000 malicious URLs were introduced into the internet each day.

We are reminded of our ostrich-like behavior in a statement by former Utah CIO Steve Fletcher when he said, quote, "Until you have a breach, nobody really wants to step up and pay extra money for security," end quote. Mr. Fletcher noted in the four months prior to the Utah breach, cyber-attacks on their system spiked 600 percent. Budgeting for cyber security initiatives proves to be a hard sell for most organizations. There tends to be an it-won't-happen-here type of mentality, either because an organization feels they have nothing a cybercriminal wants, they don't really understand it, or they have been assured of their security defenses by a well-meaning staff. Many organizations wait for compliance initiatives to drive their cyber security programs because that is the only way they know how to sell it to upper management. As experts agree, compliance will never equal security, but security will always equal compliance.

Even if legislative or regulatory compliance mandates could result in demanding adequate security, at the federal level, proposed cyber security legislation is mired in politics, and at the state level, a part-time legislature such as we have here in Nevada could not hope to keep pace. Government and public sector organizations tend to have long budget cycles, sometimes as much as 18 months or more. The amount of advancement the cybercriminal enterprise could make in an 18-month timeframe is staggering. By the time your budget comes through, it may be totally inadequate to deal with the problems of the day. It is important for this Board to transcend bureaucracy and find a way to help lead our state agencies to quickly implement meaningful cyber security processes and technologies that will not only protect the residents of this great State of Nevada, but will also protect our economy. The emphasis is on quickly. We cannot wait for long budget cycles or part-time legislatures to implement what we know needs to be done. It is already too late.

Fortunately, cyber security guidance is readily available. The federal government has invested heavily in the development of cyber security standards and recommendations through the NIST program. The State of Nevada, under Mr. Christensen's leadership, has demonstrated that we are doing a lot of things right in the area of cyber security. In 2010, he led the team that won the Department of Homeland Security's annual Cyber Security Challenge competition. Mr. Ipsen is a tireless advocate for good practices in the area of cyber security, and is a nationally recognized expert in the area as he was honored as one of the top ten most powerful voices in security in 2011. The State of Nevada is fortunate to have Mr. Ipsen as our CISO leading the way for a more secure Nevada, and he didn't pay me to say that. I just thought I'd add that.

It is important for the state to accelerate timelines wherever possible and remove jurisdictional boundaries that delay efforts to build a strong cyber security program. Conducting risk assessments in every department not under consolidated control is a critical step to take so that the right resources and prioritized activities can be undertaken. In this way, state employees can be assured to work on things that matter. Management processes that prevent our state systems

from being targets of opportunity include consistent and timely patch management processes, strong password manages processes, hardened remote access management processes and perhaps most important, continuous, timely, effective security awareness training programs for all employees.

We can no longer rely on traditional firewalls and antivirus software. Cybercriminals have automated their attacks and introduced a level of intelligence to them that must be matched by us in an automated continuous intelligent monitoring and prevention solution. The vision for Nevada's cyber security future includes automated defenses, continuous education and strong operational processes to manage and maintain the most important security fundamentals to create a safe and secure Nevada. General Omar Bradley is quoted as saying in war there is no prize for the runner up. Thank you for your time. Any questions?

Joe Marcella: Please, from the Board. Joe Marcella, for the record. I do have a couple of comments, which is typical. First of all, what I heard from you, Mary, was that it's not whether we're going to be breached, we will.

Mary Siero: That's correct.

Joe Marcella: So it's not if, it's but when. The other thing that I heard is that they're not magic formula. it's not preventative, it's not detective, it's a matter of good policies. That comes with -- and all I was going to do is ask you for that standard list of what makes -- what's the foundation that's necessary for those best practices and good policies, and I'll start it off with standardization and other things. And then the approach to start to move in that direction. Typically what fires up someone's attention and gets folks moving in the right direction whether it costs -- whether there's a budget for it or not, is a catastrophic breach. So just some of standard approaches to making sure that we're headed in the right direction, if you will.

Mary Siero: Absolutely. I've read the recommendations from this Board and from a security perspective there seem to be kind of three elements. One was to identify a framework with which to use for the cyber security program, and that is absolutely a good thing to do. The second is to conduct a risk assessment to find out where you're -- what you want to do is you want to find out where you're highest priority risks are, because you do have a limited budget, and it makes more sense to target your money in those areas where your risk is the highest. And then the third arm of that was to establish a governance program for cyber security. So I think you're on the right direction. The only thing I would say is do it faster.

Joe Marcella: Joe Marcella, for the record. Paul, this was your committee and you chaired it. Any comments?

Paul Diflo: For the record, Paul Diflo. I'd be interested in your take on governance process. You know, again representing the private sector, with our governance committee, we targeted the

VPs from all the key business units and let the business really make the decisions and be aware of the risk. It was our job in IT security to present the risk, articulate the risk, position recommendations and then let the business, and in some cases, once a year, the Board of Directors make the decision on what level of risk we're willing to accept as a company, and then what to shore up. So in looking at the government at the State of Nevada, what would be a good makeup for this governance board, and how high would it go? Would it go to the Governor?

Mary Siero: I don't know that it would necessarily go to the Governor. I think that the Board has to be made up of people who have the respect of others in the field and people who have the ability to cross agency boundaries. So people who -- and business people, I think you're spot on. It's true that the information security department, their role is really to advise of the risk and to identify good solid practices, but it's really a business risk, not an IT risk. So from a process perspective, I think your committee or your governance board needs to have those people who will get people's attention, because it doesn't matter if everyone -- if you define the right things to do if the person can't make it happen across agency boundaries. Then it doesn't matter what you've done. It's only going to help maybe a certain agency or another. So I think you need to find people who have the credibility and who have the reputation to help make things happen across agencies, whoever they may be.

Paul Diflo: Okay. Thank you.

Mary Siero: I definitely think that you need some top down support, you know, from the Governor, but I don't know that he needs to be on the governance board itself.

Paul Diflo: Right. Right.

Joe Marcella: This is actually a policy statement, or question. You mentioned top down and the Governor has to be in front of it. The question that comes to mind is that state is a lead agency in my mind and, therefore, in my mind there should be some level of management direction as if not standardization across the enterprise, and I would call the enterprise the state, and that means that all counties and cities underneath the guidance and the direction of the state should actually be following some of that process and some of those rules and some of those standards. Is that true? And this is just an assumption. And is that done in any state across the United States that could be held up as an example?

Mary Siero: You know, I haven't seen any states where they've actually done that. I do agree with that approach. And to further go on and kind of toot Mr. Ipsen's horn, you know, he's got the right people that can do that, that can really provide the standards for the state, that can really provide the guidance that they need, because they know what they're doing. The only state that may have done that is, again, the State of Michigan. The State of Michigan, their Governor, as I recall, is a former executive of Gateway Computers. So he is somebody who understands technology, and that's probably why Michigan is a little bit out in front of that.

Paul Diflo: One brief clarifying question. You mentioned a federal program called NIST?

Mary Siero: Yes. Mm-hmm.

Paul Diflo: (Inaudible) a little bit more?

Mary Siero: NIST is -- it stands for the National Institute of Standards, and there are hundreds of -- they actually have three different groupings. Some of it -- some of the reports are just special reports, others are actually controls that you can use, and then others are standards for equipment in terms of, you know, how it should be configured to create a secure operational environment. So there's a NIST standard which is special publication 800-53, revision 3, and I will tell you that it is somewhat mind numbing in terms of the number of controls that are included in it, but it's a great level of detail to use to really define your security program. I'd take it one step further and say that while that is really good and really detailed, it's very difficult for any organization to really do everything in NIST. There's over 500 controls that I believe are there.

So what I like to do, is I like to look at the SANS organization, S-A-N-S, and they have something called the SANS Top 20 Critical Controls. Now, I'd like to believe that means it's only 20 critical controls, but it's really not. Each of the critical controls is really an area to focus on, so they can help you really prioritize those 500 NIST-type controls into areas where you'll get the most bang for your buck. Further, I know that in Australia they've come up with four things, that if you do these four things right, you'll have sort of an 80-20 role with regard to security. So does that help?

Paul Diflo: Thank you. Yeah. Thank you.

Joe Marcella: Joe Marcella, for the record, and Laura Fucci's gonna kill me for this, but, Laura, you're in front of several cyber security committees. Actually you chair a few. There's also three grants or actually one grant split three ways between some jurisdictions. I think it would be interesting for the Board to hear what's going on in the State of Nevada today, and some of the initiatives that are bottom up and top down and then the funding and the direction. Do you mind?

Laura Fucci: No. I can take a few minutes and talk about that. You know, funding, as Mary -- and thank you, Mary. Your talk was very well put, very informative. I think we can all resonate with some of the statistics that was said. So my appreciation, Mary, to your words there. The funding is always a challenge. I think the funding in government is -- and I agree with some of the comments that we drive -- coming from the private sector and moving into the public sector, I see a real split that we drive towards compliance rather than security in the public sector space.

A few years ago Chris and I formed an ad hoc committee, if you will, and it's comprised of CIOs and Chief Security Officers of government agencies throughout the state focused on cyber security, and that's the Nevada Cyber Security Committee. And our objective was to identify -- and many people that are on this Board participate on that committee. Our objective has been to identify what our priorities, or (inaudible) priorities in the cyber security space, so we got together and we all did kind of a brainstorming session around cyber security and identified our priorities -- identified our issues, prioritized them all, and then we went over -- we sought grant funding through the Homeland Security grant fund -- or grant program, which is chaired -- there's a Nevada Commission of Homeland Security chaired by the Governor for that.

We were able to obtain funding for three cyber security projects. One of them is a disaster recovery project that's actually funded through the UASI. There's a USAI for Southern Nevada. Then we obtained funding for continuous monitoring. Let me back up. The Disaster Recovery Planning Project is being executed by Clark County. The Continuous Monitoring Project is a project that is being executed by the State of Nevada, and it's a statewide project. And then the third project has to do with credentialing and identity management type stuff, verifying credentials of individuals from the access systems. Also a statewide project and it's being executed by the city of Las Vegas. So we meet -- in fact, we're meeting tomorrow. We meet monthly, the project managers, for those projects to discuss how the projects are moving forward. And then Nevada Cyber Security Committee meets quarterly. So we continue to progress and try to find ways to ensure that government agencies throughout Nevada are increasing as part of their posture in the area of cyber security.

Another thing that's going on in Nevada is that Nevada was one of two states that was chosen this year for the CIAS program. It's a Department of Homeland Security grant-funded program which focuses on security awareness. It's an 18-month program that targets executive level individuals, the top management individuals within public sector and private sector. We've had the honor of Mary participating in some of that. And includes three different exercises over the 18 months, and so we've been doing those in Southern Nevada in the Clark/Las Vegas community, and it's also been occurring in Northern Nevada in the Washoe/Carson City community.

Cory could probably speak to how that's been going up north. In the south it's been very energizing. There's been a lot of interest and excitement in the room. This is not -- the audience is not the, you know, CIO or the security specialist. The audience includes council people and CEOs, you know, the people who aren't typically part of the conversation when you're talking about cyber security, and it's been very much an education and awareness session. People come into the room with I don't know why I have to be here today, and by lunchtime they really understand that they are part of the solution and that we all need to be engaged in increasing our stance with cyber security. We all need to understand what the problem is and how to be part of it.

You know, I think one of the things that was mentioned at our particular exercise is, you know, we have to get it right every day, and the hackers only have to get it right one time. So that's been very good. We've gone through one exercise so far, and we're preparing for our second exercise. I'm not sure if the north has done their second exercise yet. But what's kind of happening in Southern Nevada is that we're starting to spawn subcommittees that are cross-sector, public and private sector to carry forward this whole initiative after the CIAS program is completed. So I think that this will take legs, you know, and that we will ensure that cyber security continues to be in the forefront of our thoughts and missions as a community. So that's exciting to see. That's all I have if you have questions, yeah.

Joe Marcella: Joe Marcella, for the record. Cory, did you have any more additional comments?

Cory Casazza: Just a few comments on the progress up in the north on the CIAS is that we've completed two of three exercises, and I think we have our third one scheduled. We have invitations out. I think it's at the end of this month. It's been great for us. We've had participation by the city and the county and the state in the north, but mostly we've a lot of private sector participation, and it's been really good for us to be working with the private sector to just -- mostly to raise awareness, and I think it's something that's going to benefit the community a lot. A lot of discussion and topics and working together on if an event happens, how do we deal with it, and it's been very good. It's been refreshing to see the public and private sector working together and the amount of collaboration on something like this. But I think it's great for not only just our community, but for the whole state.

Joe Marcella: Any other discussion? I wanted to add something, and Cory -- it's either going to Cory or Laura that cites this. Mary, first of all, marvelous representation and presentation. The second thing is that you cited a whole lot of statistics, and for many of us, it falls -- it's almost more than you can understand, and then the understanding that when a security breach happens, it's typically under the radar. We don't see exactly what the impact is. And I prefer either Cory or Laura to explain -- we just came from a conference, and one of the organizations at the conference, which was a city, was compromised because of a thumb drive that was left outside. Laura, could I ask you to sort of describe the circumstances, very, very briefly, but it brings it home so that you can understand clearly how a simple act, social engineering, or leaving this thumb drive outside of an organization could devastate an organization to that level. Laura or, I'm sorry, Cory?

Laura Fucci: Yeah, I think the -- oh.

Joe Marcella: Either or. He's pointing to you, Laura.

Laura Fucci: I can't see you, Cory.

Cory Casazza: Sorry, Laura. I'm having trouble remembering all the details from it.

Laura Fucci: Okay. I'll see what I can get out of it, and you guys can step in. But basically, if I recall correctly, what happened in this jurisdiction is that somebody left a -- had left a thumb drive, like, on the floor of the entry hall into the public area. I think it was probably outside council chambers or something like that. An employee walked by, saw the thumb drive, picked it up, took it back to their desk to plug it in the computer if they could -- to see if they could figure, like, whose thumb drive it was so they could return it. When they plugged it into their computer, whatever was on the thumb drive, a worm of some sort infected their computer systems, opening up access to the financial data, and it ended up that this financial data started going to an account in Russia. So they were able to get the FBI -- they were able to identify what was happening pretty quickly and get the FBI involved and get the banks involved, and it was -- I want to say it was $2 million that was being siphoning off to this bank in Russia, or some account in Russia. And they were able to get all of it back, or stop it and get all of it back except for half a million dollars which the bank made whole. That was kind of what I got out of the discussion.

Joe Marcella: Actually, it was $20 million, and they got back…

Laura Fucci: Oh, $20 million.

Joe Marcella: …and they actually got back 15. So there is an exposure, and it's real, and it's a very simple thing to happen. Mary, again, that was a marvelous presentation, very good information. This ends up on the record. Would you like her presentation submitted? Would that be helpful?

Mary Siero: We talked about that before, and I think we're covered.

Joe Marcella: You're covered. Thank you very much. Thank you very much.

9. EITS - STRATEGIC & BUDGET DIRECTION OVERVIEW -David Gustafson - CIO, Enterprise IT Services

Joe Marcella: At this point, David, I would like you to come on up and since we've -- you've been flooded with unbelievable information, experts heretofore never seen, I believe that you're probably poised and ready to move into a strategic plan and budget process that heretofore has never been seen at the State of Nevada. If you'd report on the current status, it certainly would be appreciated. Thank you.

David Gustafson: Thank you, Mr. Chairman. I'd probably like to start off by saying thank you to the presentation -- the presenters today that this was a rock star lineup and now you have me to deal with, so I want everybody to know for the record.

Unidentified Male Voice: The group.

David Gustafson: That's right. Now you got the regular up here. So let me go ahead and pull up -- I wanted to start off with -- I want to start off with some budget stuff, and then I'll get into some of the strategic planning things I'm working on. This budgeting process for me, at least certainly since we've merged with the Department of Administration, for the record, David Gustafson, is unique because we are no longer a department. Now we are a division of a larger department. And so the process is a little bit different, and I need to give high praise to Director Mohlenkamp, who can't be with us today, about the transparency of the process. Normally what happens, this is probably what happens to the other Directors up here, you build your budget, you send it over to the budget office, magic happens, it comes out the other end as the Governor's recommended budget and you sort of find out what happened to you during this, you know, when it actually gets live. And then the legislature gets a hold of it and does more stuff to it, and then you actually find out what happened to you after that once it goes through what they call ledge approved budget.

This process that I'm going through now, as part of our agency request budget, has been nothing short of a miracle since I've been at the state government, I can tell you. We have been working really closely with the budget office to actually discuss each one of the requests that we're making and why we're making them, and so we can sort of build a picture as to our budget, as to what our direction is together with the budget office so that they understand that when they go off into the black box that they know that the things that are in there are actually real. And this isn't the first time this has ever happened to me, so big kudos to the Director on that one.

A lot of the things that we've been talking about here, and I see the recommendations, and I apologize, I was talking to Joe a little bit earlier, the Chairman, and the version that I had of the recommendations was a bit dated, and the one that I have had my assistant send me last week was actually the newer version which had a lot more information on it. But nonetheless, what I do want to say is that a lot of the recommendations we are moving forward on, and I'll pull out a few of those, you heard from Dr. Mechling that mobility is one of those. I have requested a full-time mobile programmer as part of our budget, knowing that one programmer in mobility for the state is clearly not going to be enough, but it is enough to at least get the ball started, show some great progress in that area, sort of lead by example, if you will.

I also want to say in the meanwhile, now the legislature doesn't go into session until February 5, 2013, that just last Friday, and I wasn't planning on telling you guys this, but I'll tell you, I was up at the Department of Agriculture and we are working with them to aggressively pursue mobile applications for them now as we speak so that they can do branding inspections, they can do online renewals of, you know, pesticides and fertilizer licensing and all this kind of stuff. Also that they can, you know, track -- I hope I'm not out of place by saying this, you know, a cow, if you will, from birth to death to track its progress and what (inaudible) where the shots

have been, what it's been grazing on, all this kind of great stuff. Information is really, really important in their world, as well as most other departments, and so we're focusing on these opportunities that we have.

I noticed that consolidation was the first recommendation, and well, I can't really influence that one. I think that we're at least at the state moving forward with DPS and other areas of opportunity which will certainly keep at least the Division of Enterprise IT busy for a while. So I think that at least we're moving in the right direction on the consolidation front. So before I get too much into the strategic plan, before I can't speak too much about what's actually in our budget although there's a lot of things that we talked about until the budget office gives me the okay to talk about it, but do you have any specific questions right away?

Paul Diflo: For the record, Paul Diflo. David, can you tell us what the percentage variance is from the previous budget that you're proposing?

David Gustafson: Okay, sure. We were instructed to hold flat budgets from the last biennium. The Director has authorized me to exceed that authority at his discretion of -- I hope I don't get in trouble here, of $6 million additional investment in IT for this go round. And so we're finalizing what those things should look like. There's a lot of support equipment, phones, critical infrastructure, security, continuous monitoring, there's a lot of stuff like that that's in there.

Paul Diflo: So if we do the gap analysis as we recommend any solutions that come out of the gap analysis, is that going to come out of your budget, or does that come out of a different budget?

David Gustafson: It will come out of my budget.

Paul Diflo: It comes out of yours.

David Gustafson: Mm-hmm.

Paul Diflo: Thanks.

Laura Fucci: David, this is Laura Fucci, for the record. You said $6 million, so do you know approximately what percent of the budget that is for you?

David Gustafson: My budget's about $30 million now.

Laura Fucci: Okay. Thank you.

David Gustafson: Mm-hmm.

Kevin Farrell: Kevin Farrell, for the record. This might be too specific to answer, but the core systems that need some attention, over the next 24 -- over this budget cycle, how much of any of that will you try and address?

David Gustafson: Okay. So I manage a lot of things under the sun here, so let's start with particular -- let's just pick telephones.

Kevin Farrell: I was thinking of the financials.

David Gustafson: Financial systems. As far as the software itself, we will be looking at doing an assessment of that. We're talking -- a new ERP is, according to my friends at Gartner, 20 to 50 million, depending upon, you know, what you want. So we won't be doing that, but what we will be doing is an assessment moving forward with the Controller's office to sort of look at what our requirements would be, sort of benchmark where we're at and where we need to be. But we're finding a lot of the short comings of the system here are really prohibiting the business units from actually making intelligent decisions because they just don't have the data. You know, we have a 30-year-old banking system, you know, as our ERP and it's just not very appropriate for this day and age.

Kevin Farrell: Thank you.

Cory Casazza: David, you kind of talked about your budget strategy and what's -- how it's coming through your office. What's the strategy going to be for budget for the deconsolidated shops? Are they going to be asked to be held at the current level? Are they going to be given some additional funding for infrastructure? And is there anything that's happening in the budget that's going to help consolidation as far as on the IT side?

David Gustafson: I do not know what the -- let me say this. I believe the agencies are held to a flat budget. So this opportunity that the Director is giving us is unique to us, not to others, as the best I understand it.

Cory Casazza: Then in the distributed agencies with distributed IT, is the budget identified in there, or is it kind of (inaudible) in with everything else and it's hard to tell what's tech funding and what's operations and what's capital? Is there a lot of discretionary funding in a lot of those budgets to fund tech on the deconsolidated departments?

David Gustafson: I believe they're largely integrated into all of their systems. Typically because the revenue comes from various sources. For example, we're looking at the Department of Public Safety, and they have 12 different revenue sources, whether it's core assessment at, you know, traffic stops, or fines, or licensing, or, you know, the yellow lights or whatever, or assessments. So there's so many revenue sources which is what makes it very difficult to sort of separate in that way. That's sort of one of the complexities of government is that there's so

many revenue sources. I mean, there's grant money, you know, Director Willden has many, many, many, many revenue sources and grant funds, and that's -- they're all integrated. So it's not that easy.

Cory Casazza: And just one last question, sorry.

David Gustafson: Why do I get all the questions? Go ahead.

Cory Casazza: Because you know all the answers.

David Gustafson: I do not.

Cory Casazza: How are vacant positions being handled in those decentralized departments? As they become vacant, are they allowed to refill them, or is there a move to -- in the agencies that are willing to consolidate, is there a move to let you hire those positions and move that funding and that position into your budget in the next -- I mean, will that be a push that's made through the legislature, or is it going to kind of remain status quo, and it's going to be a fight to get any consolidation efforts to happen going forward?

David Gustafson: Sure. Again, the government is more complicated than we would like it to be, but agencies, they are hiring their own staff, and it's just not as easy as saying, oh, David, now you go ahead and hire this guy to do whatever, this resource, because when the legislature approves those positions in your budget, they must stay there until the legislature moves them. So we don't have that sort of discretion, and the executive branch just kind of moves things around. Furthermore, because of some of the classifications -- well, most of the classifications, I am one of two who are actually unclassified in my entire division of 130 people, meaning everybody is stuck in a class series so they can only do those things that are in their class series at their pay scale, if you will. So it's a box that's very difficult to manage, and it doesn't tend to grow and shrink very easily. So the answer is they're in their budgets and we can't really help them unless the legislature approves it, and that's not easy.

Joe Marcella: David, there's another nagging problem. Joe Marcella, for the record. We've talked at several Board meetings about application life cycle which is really the modernization of some of the current applications. Two issues. One is, have the alternatives been identified? And the reason that I'm asking, because that needs to be done in my mind rapidly, because many of the skills inventory, the folks that maintain the older systems are probably as old as I am, maybe a little bit younger, but the boomers are leaving and they're uniquely qualified to maintain some of the older systems, and they are key to that transition to a more modernized system, because you can't there from where they are unless you've got them with you. Has that been considered, in other words, the timing of all of this?

David Gustafson: Let me say yes and no to that. I think it's safe to say that most of us recognize that the state government, the IT resources are an aging population and that we need to do more to recruit, train and grow the junior staff, if you will. Having said that, we also have physical constraints and bureaucratic constraints that aren't quite that easy as just saying, hey, hire some young guys or, you know, young gals out of college and get them to work and away we go. Knowing that we have such a fiscal constraint, that's not a very achievable goal. But I believe, at least from my perspective, I recognize that, and I'm certainly doing everything within my authority to fix that, but we are also stuck and facing, you know, potentially a 50 percent retirement in the next several years, especially if the economy turns around.

Mike Willden: Mr. Chair, I was going to add a little color commentary, and, again, I'm like David. I feel like the Board's sort of asking some questions about where we're going IT wise, and since I'm a 60 percent customer of this shop, it might be a couple comments, but I'm going to tiptoe around confidentiality issues also. But, you know, from my department's perspective, Human Services, we have lots of projects with David, and I think we hopefully will be fairly successful in the budget process. I think we have four of the eight TIRs, Technology Improvement Requests, and in the past that's usually a competition for the money sort of outside the cap. My department was able to fund those inside the cap this year, which is one of the first times we've ever really been able to do something like that. And probably this is a bit of foreign discussion for this Board, but you get a cap like David said. You have to live in the cap.

Well, in my department there's a thing called FMAP, the Federal Matching Assistance Percentage, and because Nevada's economy has been so poor over the last several years, the federal government pays for a higher proportion of our medical costs in our Medicaid program and other kinds of programs. So you get cap room. Now, we have been able to focus a lot of our excess cap room on information technology infrastructure projects, so we're pretty happy that, you know, we hopefully will get a turn in the barrel on some big technology improvement requests. And then what is public, I think we've talked a little bit about this, we've got several contracts out there, massive systems overhauls, we call them eligibility engine, quality control contractors around that. That's all around the healthcare reform. The Board of Examiners just approved what we call the BOS, Business Operations Solution, for the health insurance exchange, so we have vendors galore in town now, Xerox, and Deloitte, and PCG, and I don't -- they're all here I think right now, all working on contracts in cooperation with Enterprise IT.

We also have major federal funding for health information technology, health information exchange. There's the health insurance exchange, but we also have a major funding stream for the next couple years for some health information technology health information exchange. And so it's been a pretty robust year for us in the budgetary process. And again, it'll all be public October 15 or October 16, depending on when the press decides to publish the stories. But from my perspective as a big user and working with David and his staff, we've got a lot riding on the next couple years, and then that's not even to include a lot of the catch up on equipment. You know, we've just been frozen for so long, and what's the retention rule, or replacement rule, five

years you're supposed to get a new one? I think 80 percent of the Welfare Division is eight years old, and so we're going to be doing some big time catch up and working on some of those kinds of things. So we hope anyway. So lots of things in the cooker.

David Gustafson: For the record, David Gustafson. And I think it should be recognized from Director Willden that whether he knew it or not, he actually just purchased about a million dollars worth of UNIX infrastructure for use in the enterprise that we are going to be supplementing and becoming more efficient and saving money by collapsing countless UNIX environments into one, and (inaudible) what I call IBM contraption. So I won't tell you what it is, but he should be recognized for that. That is a major contribution to the enterprise.

Joe Marcella: Joe Marcella, for the record. So that means that you become my new contingency site up north.

David Gustafson: Potentially.

Joe Marcella: Any other discussion? David?

David Gustafson: Okay. Thank you, Mr. Chairman. So I'll go through a little bit about the strategic planning process. Last time I was here and I spoke a little bit about what I pulled out from other agencies, from other states, and I was distilling those down into some common ideas. And to be honest with you guys, I really wasn't very happy with what I was seeing, that I thought that what I saw as a strategic plan, if you will, was not reflective of what I was finding at least in the government space. It's great that states can whip out a 100 page document and say here it is, boom. Someone fills it -- they check the box and they move on and they pick it up five years later and, you know, they take a look at it and say, well, does this make sense, yes or no? And I would probably argue that maybe a few years ago we might have even fit into that same category. But technology is accelerating, and when you look at this, you've been hearing the presentations today, we don't have time for that anymore. And so we don't have time to say, well, gee, I want to build something five years from now. Five years from now we're going to be doing things we don't even know exist yet. The technology is really accelerating how we do this.

So what I've really tried to do is I've tried to distill the plan down into what I say is the current state, and I can sort of go through some of this in a little bit more detail, but sort of the current state, where we are today, the importance of IT, and then really get into what are those priorities that will enable us to build the next generation of system, more of the fundamentals. Not so much the, hi, I want to build a Cisco network five years from today, or I want to do something like that. Really more about productivity and efficiency and those kinds of goals. How do we do that on a higher level that has more value knowing that this plan should be a living and breathing document, not shelf ware for five years and then someone picks it back up again. I want all of my chiefs to look at this particular document and say, yes, I see now where we are going. We

are saving money. We're being more efficient. We're being more productive. We're (inaudible), you know, those kinds of things. And then they can build their plans appropriately.

So I really wanted to make sure that I didn't get too far into the weeds on purpose, so I want you guys to know that, that it is -- I'm looking at this more from a business perspective even though it is an IT strategic plan. I think that it's really important that the business people can pick it up and read it. My target audience when I sit down and look and I write these things are Cabinet level directors, legislators, other business people from other states that can look at this and say, I understand. I see where they're going with this. Because a lot of times you pick up these IT strategic plans and, you know, they're great for the IT people, but they're not so great for anybody else. So I wanted to make sure that I was building a business version of an IT strategic plan for right or for wrong.

So, Mr. Chairman, if you don't mind, for a few minutes I'll just kind of roll through here what -- sort of some of the -- a little bit level of detail down, if you will. I wanted to focus -- and this is on a draft by the way. What I'm going to do after this meeting, I'm looking for some peer review. Once I feel like it's sort of finalized and into a draft form, I'll send it out to all of the Board members and look for more feedback. I've also listed all of you in the plan at the end of it, so I think you might want to read it and see if you agree or not. Oh, no.

Joe Marcella: David, have you given us credit or you're citing that we gave you some direction?

David Gustafson: Both. We're all in this together. I just want you all to know that, right? Okay. So I think it's at least on the right track. I wanted something uniquely different, and the feedback I received so far is that it is more aligned with what other people's expectations would be. But I really focus on some key strategic areas. And one of those is the merger of Department of Public Safety's IT organization with Enterprise IT. This is a potential, if the legislature approves it, will be a successful merger going forward on the consolidation front. Ways to improve employee and systems productivity, measures to increase system and infrastructure efficiencies, methods to reduce expenses while increasing functionality and services, and governance and tools to increase the security of our critical data sets are just the five high-level strategic areas that I'm looking at here.

I also call out the current state of IT. I think it's important to know where you are before you need to determine where you want to be. It's always good to know what you want to be in the future, but first you need to know what you are today, and so I spend probably a page describing what we are today so that when people pick this up, they can understand, oh, okay, now I understand why they're making these decisions or where these decision trees are at and this sort of -- some of these opportunity costs that we could be looking at. I go in to essentially say that we are a largely decentralized IT organization, so Nevada has essentially three choices in front of us. We could decentralize more and everybody do their own thing. We could fully consolidate

and do some centralized super IT organization, if you will, or we can do a hybrid of both. But whatever we want to be when we grow up, we should at least know what that is so that we can then build a proper road map going forward.

It's difficult for everybody when we're trying to -- we're changing direction all the time, we're not sure what we want to be. As I say, when we grow up we're not sure what we want to be, and I think it's really important so that people understand that we're looking at really three distinct models for Nevada, and I think it's not up to IT to determine what those are. Sort of what the presenters were saying earlier. These are not IT initiatives, and I maintain a position that the business drives consolidation or anything related to IT because you don't consolidate IT because you just want to consolidate IT. You consolidate IT because you want to save money, you want to be more efficient, you want to have a smaller workforce or whatever you want to do, it's a business driving those things, not the IT organization.

So I implement, or actually call out some strategic goals. And I'll just go ahead and read you these. There's only four of them. And they've captured my thoughts as of this moment. Implement and leverage enterprise class technologies to provide a more robust and available IT environment for business applications. I think it's inherent for IT organizations to build a platform which the next generation of business applications will be built. Mobility is one of those, self-tuning databases, automating IT services, self-provisioning portals, those kinds of things. That's where a lot of the cloud technologies would come in. Improve information security of enterprise infrastructures and state data sets. Understanding the threats, I mean, everybody here has understood. I've presented on the threats that we face as a state every day, 2 million attacks on our network, 600,000 spam viruses, you know, those kinds of things. You guys have heard this story before, but we face pretty strong challenges with the states, our major data collectors, and there's a lot of reasons why people would want to have what we collect.

So when you look at what are those assets, how do we secure them, what's really important. You know, I'll say this. As an IT guy, I thought all kinds of stuff was important, and I come to realize lately that from talking to some decision makers that the things that I thought were important really weren't all that important to them, and the things that they thought were important, I clearly didn't think they were that important. So we need to understand what kind of data is important and make sure we have adequate security controls around that and build a process to ensure that it's audited and it's kept safe. So anyway, secure the data.

Improve the customer and employee experience. I want to give the opportunity for staff to stretch and grow, give an opportunity for someone to go through my organization all the way from the lowest paid position all the way to my position. I think it's really important in any organization not to have gaps where you can't bridge them. Right now we have some gaps in my organization where you can't go from, you know, the lowest level guy, mail room guy or whatever, to CIO. You can't do that because there's some gaps that in the classified system you just can't breach. You have to have, you know, a master's degree and 20 years of experience

from somewhere that just you pull it out of a hat in order to jump back out. So anyway, I want to make sure that I'm filling in all the gaps and give people the opportunity to stretch and grow and promote from within. I want to make sure that we have adequate training involved in our budgets in which I think we're working more on building up our training budgets again.

And I also want to make sure that agency missions and IT services are a provision on common platforms under clear IT vision strategy and statewide architectures resulting in an overall improved customer experience. Remembering that my customers are agencies, and so what I want to be able to do is bring those enterprise class technologies, those self-provisioning portals to my customers so that when my customers need a new server or a new database, they can just simply go to a portal, clicky clicky, put in my GL account, hit the create now button, they get a link that says here's your new server, thank you, have a great day. Everybody's happier. I'm happier. It's a lower cost for me to deliver the service. They're happier it's a faster turnaround, it's 24 hours, it's automated, it's magic. So I want to work on that.

Lastly I'll say simplify the IT ecosystem. I was reminded of this when an agency pulled out their network diagram for one of their major systems and probably I was the only guy in the room that could actually understand what was actually built because it was so complicated. And I realized that we as a state need to standardize on platforms, applications. We need to do more about leveraging those enterprise class technologies that we do have available to us. And so I am going to do more in this area to make sure that we're promoting those opportunities, that we're working together where we can. This is what I was pointing out from Director Willden earlier, using some federal money to build an enterprise-class UNIX environment that we can leverage for many other applications. So I want to make sure we're building enterprise-class technologies to ultimately simplify the IT ecosystem, as I call it, which results in a lower cost to deliver the services. So anyway, enough of the planning talk, unless you guys any questions.

Paul Diflo: For the record, Paul Diflo. So let me know if this is an appropriate question or not, but you've got your goals, the four goals that you've stated. One of them is improve enterprise security.

Gustafson: Mm-hmm.

Paul Diflo: So then you've got your proposed budget. How much money is allocated to improve enterprise security, and does it take into effect the gap analysis that's going to be done, and then any possible remediations that come out of that?

David Gustafson: I can't say exactly how much, but we are making a substantial investment in the top four SAMS controls. The patching, the monitoring, reducing credentials and the application of (inaudible) for 20,000 end points, which is a statewide initiative.

Paul Diflo: And then another security-related question. Do you align -- when you do your goals, do you work with the office of the CISO and say, hey, you know, one of my goals is to do this…

David Gustafson: Chris is probably watching.

Paul Diflo: …to do this gap analysis and we think you ought to be part of that gap analysis?

David Gustafson: Well, Chris reports to me, so we confer frequently often.

Paul Diflo: All right.

David Gustafson: More than he would like.

Paul Diflo: Okay. Thank you, David.

David Gustafson: The fact is, the security guys caught me for four hours in a car a couple weeks ago and I said, it's fine for me. I just get in the backseat and put my arms around the front chairs, and I say, guys let's talk about security, and they were like, oh, turn the music up. They didn't want to talk to me about it, but, no, we had a good time.

Joe Marcella: Joe Marcella, for the record. Any additional discussion? Then I have a quick question. It sounds like you're moving in the right direction. It also sounds like this Advisory Board actually gave you some of the language to start to move forward, and a lot of your own. A lot of listening to your constituents, the folks that are using your services, a little bit of ingenuity, and in fact a whole lot of ingenuity, and it's sounding and appearing to be that you're getting some momentum. Two things. One is I'm hearing that the budget is somewhat tentative. I'm also hearing that the document that you're preparing is conceptual at best. I'll get one step further. I'm thinking that the next meeting's going to be on the 3rd, the 10th or the 17th of December. Will you be ready with somewhat of a -- and I didn't hear a strategic plan, I'm hearing a business plan forward, more towards using the strategies to implement business solutions. Will you be more comfortable at that point as to solidifying the direction you're going, and also because of many of Paul's questions, being capable of tying some dollars to it? At least not necessarily the dollar amounts, but the distribution of what part gets how much and the priority forward.

David Gustafson: For the record, David Gustafson. Yes, I am. And thank you for the feedback. I think the recommendations from the Advisory Board have been instrumental in at least to helping me quantify and qualify those things that are important. I think I've gleaned quite a bit of information from that, and some of these things we were talking just this morning about an information security management system, for example, about moving forward on that. I think whatever this is, it's certainly a lot more than a concept. It is a draft. I think it'll be ready

for some prime time here very soon. I also have a whole section in here about planned projects and initiatives which I didn't bother mentioning, but it goes on for a whole page of things that we're doing -- that we're planning on doing that are going to facilitate and execute on those goals in those key strategic areas that we're working on, recognizing the fact that the legislature may or may not approve funding and that the direction could go in a different way, if you will, but at least as of this moment, this is where we're going.

Joe Marcella: We very much appreciate it. Thank you, David.

David Gustafson: You're welcome.

Joe Marcella: Any additional discussion?

10. DISCUSSION FROM MEMBERS

Joe Marcella: Okay. We'll move on to the next Agenda item. First of all, so we're -- there is no discussion.

11. PUBLIC COMMENTS

Joe Marcella: I wanted to move on to that this is a public meeting and I wanted to see if there's any public comment. Laura's coming back into the room. Is there anyone down south, Laura, that's absolutely chomping at the bit to make a statement?

Laura Fucci: No. The crowd is holding back down here.

Joe Marcella: Up north? Anyone here in the audience?

* 12. ADJOURNMENT

Joe Marcella: Seeing none, hearing none, let me move on to an adjournment. But before we go there, I want to have a quick discussion with the Board. I'm asking that the next meeting be in next quarter and be in December. I don't want to bump into the holidays, so I'm thinking Monday the 3rd, the 10th or the 17th. Could we have a quick conversation about that? And, Lenora, I would assume it's the availability of a room as well, but you don't have a…

Laura Fucci: Excuse me, can you repeat those, please?

Joe Marcella: No.

Laura Fucci: The dates.

Joe Marcella: Yes. The 3rd, the 10th and the 17th of December.

Laura Fucci: Thank you.

Lenora Mueller: Joe, I won't know until I talk to the broadcasting department here.

Joe Marcella: Okay. So you're meetings aren't online, so meeting rooms aren't online.

Lenora Mueller: Right.

Unidentified Male Voice: Usually we're locked out of here in December.

Joe Marcella: If we're locked out in December, then we'll just move it to January and we can start a new year.

Mike Willden: Mike Willden, for the record. There are other avenues. We have this technology in our office is we can (inaudible) if you want to use our offices or whatever that -- usually in the past, usually about the middle of November they lock this building down for major cleaning, rehabilitation, whatever, before the legislature rolls in the first week of February and agencies are locked out. Now, I don't know if that's going to be the plan the next time that you can't use the committee rooms, so you might want to find out about that.

Lenora Mueller: It's my understanding, Joe, and thank you for that, Director Willden, that it'll be hard to meet our statutory requirement here in this building during the budget session, and like Director Willden is saying, starting in December.

Joe Marcella: Then let's go ahead and target these dates. However, we can possibly use another facility as long as it…

Mike Willden: You're welcome to use ours. We certainly can have -- we just need to know in advance.

Joe Marcella: And as long as it's a published meeting as posted, we're okay, is that correct?

Lenora Mueller: That's correct.

Joe Marcella: Is everyone on the Board agreeable? Okay. So the meeting…

Laura Fucci: Excuse me.

Joe Marcella: Yes.

Laura Fucci: Excuse me, I'm sorry. For the south, you know, I have the video teleconferencing capability in my office. So if I'm probably the only one attending, that might be a good place for the south.

Joe Marcella: Yeah. You can do that in my office as well, so we'll find a way to work that out. Okay. So the dates then are the 3rd, the 10th and the 17th. I'll just wait for some feedback and then we'll decide and I'll canvas the Board. Okay. Can I have -- any further discussion? Can I have a motion for adjournment?

Unidentified Male Voice: Move to adjourn.

Joe Marcella: Second?

Unidentified Male Voice: I second.

Joe Marcella: All in favor?

Group: Aye.

Joe Marcella: Thank you, everyone.

Laura Fucci: Aye.

Notice of this meeting was posted in the following Carson City, Nevada locations:
Blasdel Building, 209 E. Musser St., Carson City, NV 89701
Legislative Building, 401 N. Carson St., Carson City, NV 89701
Nevada State Library and Archives, 100 Stewart Street, Carson City, NV 89701

Notice of this meeting was emailed for posting to the following Las Vegas, Nevada location:
Capitol Police, Grant Sawyer Office Building, 555 E. Washington Ave, Las Vegas, NV 89101
Hadi Sadjadi: hsadjadi@dps.state.nv.us

Notice of this meeting was posted on the internet via the it.nv.gov website:
http://it.nv.gov/Governance/dtls/ITAB/Information_Technology_Advisory_Board_(ITAB)/

We are pleased to make reasonable accommodations for members of the public who are disabled and would like to attend the meeting. If special arrangements for the meeting are required, please notify the Enterprise IT Services Division at least one working day before the meeting at (775) 684-5849 or you can fax your request to (775) 687-9097.