Minutes of the Meeting of the
LEGISLATIVE COMMISSION'S
INFORMATION TECHNOLOGY SUBCOMMITTEE (NRS 218.682)
Legislative Building, Room 4100
Carson City, Nevada
February 6, 2002

The first meeting in 2002 of the Legislative Commission's Information Technology Subcommittee (ITS) (NRS 218.682) convened at 1:10 p.m. on Wednesday, February 6, 2002, in Room 4100 of the Legislative Building, Carson City, Nevada, with a simultaneous video conference to the Grant Sawyer Sate Office Building (GSSOB), Room 4406, Las Vegas, Nevada.

SUBCOMMITTEE MEMBERS PRESENT IN CARSON CITY:

Assemblyman Bob Beers
Assemblyman Lynn Hettrick
Senator Dean A. Rhoads
Senator Michael A. Schneider

SUBCOMMITTEE MEMBERS PRESENT IN LAS VEGAS:
Assemblyman Bob Price, Chair
Assemblyman Harry Mortenson
Assemblywoman Debbie Smith
Assemblywoman Sharron Angle

SUBCOMMITTEE MEMBERS ABSENT:
Senator Bob Coffin - Excused

LEGISLATIVE COUNSEL BUREAU (LCB) STAFF PRESENT:
Eric Dugger, Information Systems
Steven Lang, Title, Legal Division
Kimberly A. Morgan, Chief Deputy Legislative Counsel, Legal Division
Allan Smith, Manager, Information Systems
Steven J. Watson, Chief Deputy Director, Administrative Division
Sylvia A. Wiese, Executive Assistant, Administrative Division

OTHERS PRESENT:
Mark Blomstrom, Nevada Department of Information Technology

A copy of the meeting notice and agenda is attached as Exhibit A.

I. Opening Remarks by the Chair and Introductions – Assemblyman Bob Price, Chair.

Assemblyman Bob Price called the meeting to order. Thanked everyone for attending and said he was looking forward to the work this committee.

*II. Approval of the Minutes of the August 10, 2000, Meeting.

SENATOR RHOADS MOVED TO APPROVE THE MINUTES OF THE AUGUST 10, 2000, MEETING OF THE LEGISLATIVE COMMISSION'S INFORMATION TECHNOLOGY SUBCOMMITTEE. MOTION SECONDED BY SENATOR SCHNEIDER AND CARRIED UNANIMOUSLY.

*III. Review of Appropriations – Allan M. Smith, Manager, Information Systems.

A. Discussion of Appropriations and
B. Appropriation Modifications.

Mr. Allan M. Smith, Manager, Information Systems, referred to the exhibits in the packet.

Item 1, User Software Upgrades, Mr. Smith said that one of the things that has changed in this area is that Microsoft changed its licensing program primarily for its larger customers. We are tied in with the Executive Branch on Microsoft General License and one of the things they have set up is what amounts to an annual maintenance program. What this means is you pay a basic fee based on the number of copies of their applications that you have running. In terms of our cost, there are going to be some increases that we will have that will be sufficient to overrun this amount, however, since a lot of those licenses are related to session use we are going to try and do a mix and eventually get it paid off that way.

Item 2, BASN & Local Government, Mr. Smith said most of this money is reserved for session consulting costs. During the legislative session they bring in additional people to help them to weed through the data and make some of the different gyrations that they have to go through in order to keep the money committees running smoothly.

Item 3, Accounting System Upgrade, has been completed and we are running on the new version. We did purchase a new server for them as well.

Item 4, Network hardware and software upgrades, we are in the process of moving our servers to the Windows 2000 Operating System. We have a mix going right now, and we'll be completing that before next session. We have upgraded some of our server hardware and have plans for additional servers to set the Audit and Research Division data and give them control to some extent. The Interim Finance Committee has approved a new warehouse to be built in part of the space where the Capitol Apartments were. In order to provide network services to that building, which will house the General Services staff, we will be looking into putting in a wireless bridge, extending our wireless system over to that point. This will eliminate the need to run wire under the ground, which would be extremely expensive. It would also give us an opportunity to possibly extend that service further.

Assemblyman Beers asked if Mr. Smith said by extending the land wireless to the new location where the Capitol Apartments were would that extend coverage to the Plaza Hotel?

Mr. Smith replied that it would give us the possibility of extending the wireless to there. It would not by default do that. If you understand how wireless networking cards work, we can broadcast a strong signal with that antenna, the problem is the cards that are in the laptops aren't strong enough to send back to that distance, they only have a 300-400 foot range.

Item 5, Implement Virtual Private Network (VPN), we have been working on this technology and have run into a few issues that we are trying to work through. Our plan is to have this in place as soon as we can, hopefully before the beginning of summer.

Item 6, Public access kiosk project, the kiosks may or may not get done this time but if we do get into that project we are looking at putting one in the Las Vegas office and another one on the second or third floor of this building.

Item 7, Upgrade Research Library Database, is on hold right now. We have implemented some new software which is in the first phase which provides a much better search capability. They are going to look into whether or not they can use that.

Item 8, Upgrade to internet and Intranet, this is general software upgrades to keep pace with what is out there and some of the special development software that they use, as well as upgrading our web server.

Item 9, Front Desk upgrade, this is mostly software upgrades. There will be some training and incidental contract work. As some of the committee is aware, last session, when the legislature passed the LCB budget, the budget for the Information Systems Unit, was modified so that we could add another programmer. Our new programmer's name is Fred North, and he came to us with quite a bit of development experience and has already been involved in a lot of projects and has completed a couple very successfully. We are really looking forward to having him more involved and eventually being the one lead programmer on the Front Desk system.

Item 10, Upgrade Web Search, we have purchased this software. It's really the follow-up program to Folio Views, which is used for the Nevada Law CD. That company has changed and some of the original developers formed a new company eventually buying back the rights to Folio Views. Their new product is called Next 3 and we have about completed the first phase of this project and provides web access to updates to the CD. The first part of that is mostly dealing with the Nevada Reports and the Advance Opinion information, eventually we'll be adding more to that. Phase Two will essentially be putting the whole of the legal library on the subscriber side of our network mostly for those who are still CD users being able to switch back and forth without too much having to deal with both. Phase Three will be to make the public side also available with this search. It is a very robust technology and has been very well received and at some point in time we hope to be able to give you a demonstration.

Item 11, Phone system upgrade, we have been going along with a few items on that, most of it is incidental. One of the things on the detail listing that we are not going to do is the voice recognition software.

Item 12, Legal Division Projects, these are just ongoing upgrades and some new software that they have developed and that makes up the majority of this.

Senator Rhoads asked Mr. Smith to explain how the Virtual Private Network is actually going to work?

Mr. Smith said the way it works is that we have a server that will accept the client coming in. On each of the users, the laptops, would be using this software and we would have to place a client program. The client program consists of the program that does the interchange between that laptop and our server and network through the internet. It also has built into it a personal firewall which adds additional protection. One of the things about VPN is that because you're going across the internet a lot of additional steps need to be taken in order to assure the security and the privacy of that connection.

Mr. Smith explained you would have a local connection, whether you're using a DSL connection or a connection to another private internet service provider like AOL, Great Basin, etc. and you would dial into that service. You would again initiate the program to make the connection. The program then would go through. It would actually initialize the connection, there would be some authorization that would go on, you probably would have a login prompt and then completing that you would be into the network and would run your Outlook just as you normally would.

Mr. Smith said they did not put in this appropriation and upgrade to the PLC. In other words the Roll Call Vote System and camera movement. These are all controlled by a single device. The upgrade to this was quoted at around $100,000. This needs to happen before next session. We're probably looking at trying to draw some of that out of this appropriation. What he is looking to the committee for is approval to judicially spend this money in that direction. Thus taking away from other items that might have planned to do.

Mr. Price said they would consider this later.

Senator Schneider asked what would it cost to do all of Carson City so that you could use your laptop no matter where you live in Carson City and also with that, do a lot of the state employees have that access? Would they be able to take work home with them at night with their computers if they have wireless networking?

Mr. Smith replied we have several staff that have laptops and they are provided with wireless connections and do take them home for work projects. They do as you do when they are in town, they dial in. There are some issues with respect to making it available throughout the city, one is the cost of broadcast that far and also you must have the capability to get to us. We could probably put in an antenna that could. Right now the one we are looking at for across the street has something like a seven-mile radius, the problem is that your laptop doesn't have a comparable capability and so being able to set it up so it works both ways would probably be cost prohibitive. The other side of that is many of you come into town during session; you rent accommodations, some of those do have DSL access. DSL works faster but not as fast as the 11 megabyte wireless but certainly with speeds well in excess of what you're dialing would and it certainly would be a suitable way to do that. With that and the Virtual Private Networking you actually have a much better and probably a much more cost effective connection through a service to our network.

ASSEMBLYMAN BEERS MADE A MOTION TO ALLOW LCB THE FLEXIBILITY TO UPGRADE THE VIDEO CONTROL DEVICE USING THEIR JUDGMENT. MOTION SECONDED BY SENATOR SCHNEIDER AND CARRIED UNANIMOUSLY.

*IV. Proposed Policy for Changes to the Website – Lorne J. Malkiewich, Director.

Mr. Smith said Lorne Malkiewich was ill and unable to attend meeting but requested that he give the presentation on this item.

Mr. Smith said our Web Master, Andy Harvey, is receiving a lot of requests for changes to the website and they come in from several different sources and not necessarily the sources who have perceived ownership of the space that they want to change. This precipitated the need for formalizing that process. The first step was to draft a policy, which has been done, and then allow the division chiefs and this committee some time to consider it and provide some input and then to come up with a final version.

What we would like to do is use this at this time as an operative version until we finalize the policy which would give us some guidelines. What Mr. Malkiewich has asked is if you could provide some input and if you have some thoughts on the changing of the website, how it might be handled and if it's different from what we have here or if you have something new we have left out.

The Committee had no comment and took no action.

V. Discussion on Laptops for 2003 Session – Allan M. Smith, Manager, Information Systems.

Mr. Smith said normally we don't make a decision at this time on a specific laptop that we're going to use for the next biennium. IS will

recommend and have the committee consider retaining the laptops that they have now for the next biennium. With budgetary concerns and the fact that these seem to have been proved out to be a fairly good equipment. We feel some minimal upgrades will make them enough better that they would be usable for the next two years. The upgrades that we are looking at and going to recommend would be to increase the memory from 128 megs to 256 megs , upgrade the communication card (the built in card only has a modem on it) to a dual purpose communication card which has the 56K and network interface card so you who would like to be able to plug into your ADSL or DSL with your laptop would not have to buy an extra PCMCIA card. The cost associated with that would be roughly $280-300 per laptop as opposed to $2,500-2,800 for new laptops. He said he would like to remind the Committee that the desktop the power cords installed for last session would likely be obsolete if we were to purchase new laptops and would have to be replaced as well.

Assemblyman Beers said the upgrades sound like they would leave all the data and Outlook contacts that we had set up last session and whatever filing system have set up for their own organizational use in tact?

Mr. Smith answered that is correct. In fact, what they would be doing is bringing in each laptop to put in any necessary upgrades with respect to software, those legislators who are on Senate Finance or Assembly Ways & Means would want the new budget information put on when the time came, and any other modifications with respect to hardware. You would retain your contacts list, any software you may have added, any letters, communications, e-mails, etc. and would not have to be transferred.

VI. Discussion on Computer Security – Allan M. Smith, Manager, Information Systems.

Mr. Smith thanked Eric Dugger who is his network manager and also part of his security team, for doing most of the work on this presentation. Both he and Mr. Dugger participate in the IT Security Subcommittee which is part of the Nevada Information Technology Oversight Committee (NITOC). Mr. Smith said that in the last the subcommittee they've been participating in was broken into three groups. During that time we developed policies for the State of Nevada with respect to security and computer security. It also gave us time to think about our network and what we are doing here. As he was thinking about it, since we are the legislature maybe we should be the ones to lead the way and set the example.

The presentation was put to together to get the committee started in terms of understanding what it is we're going through. We will be talking about the security vulnerabilities that a network faces, possible outcomes and consequences of those not being handled properly, precautions that can be taken and the technologies that are available and then the plan Information Systems has put together for security for the legislative network.

The biggest vulnerability is the internet. Our connection to the network and probably the most non-secure communication pipeline that is out there. Because of the network, the internet, you have the possibility of hacking, viruses coming in and sniffing. Sniffing is where someone can come up to your firewall and actually look and see what is transpiring. What is passing back and forth. Through that they can actually get information and other things you don't want them to have. The biggest problem with dial-up services is that there may be non-secure computers attached at the other end. These computers may not have virus protection in place or maybe they just don't have the current definitions, and they may have been hacked and contain a Trojan which could be passed on.

Assemblyman Beers asked if Mr. Smith was suggesting that if he (Mr. Beers) has a cable modem at his home in Las Vegas or a DSL line up and he has hooked up his laptop to it, then dials out to a non LCB dial-up service, his personal ISP, while we're in session, so his laptop is both on your network and his ISP, does he represent an above average security risk?

Mr. Smith answered there are some risks, the fact that we do our best that everyone's virus definitions are up to date. We're more concerned about home computers. There are some issues with respect to outside ISPs where people can get through them into your PC and look at things and put things on there, such as cookies etc. If you have a personal firewall installed that prevents a lot of that.

Mr. Smith continued with his presentation on the next item of e-mail. He said e-mail obviously carries with it the potential for viruses, it also has the potential of releasing confidential information and when you send e-mail it is like sending a postcard, anything you send in plain text has the capability of being read by someone out on the internet. This should be and is a concern.

Connections to the State backbone. He said he knows that the state is doing everything they can to make it secure, it is a broad based network, it covers a lot of territory, a lot of state agencies, divisions and departments. It's nearly impossible for them to really have the kind of control they need to have. That is why NITOC and the IT Security Subcommittee has gotten together and is trying to do something about that. At this point in time we need to consider that as a vulnerability.

Social Engineering, most of us have a trusting nature, but what that really means is that on your computer do you share your password with someone else. If a phone call comes in and someone identifies themselves as Allan Smith and says I need your password are you sure that it is Allan Smith who is calling or do you say, "Okay, here it is." Those are the kinds of things that can occur and obviously we need to be prepared, we need to work at this.

Wireless Network, we consider an open network, the reason we do is that we operate on a fixed encryption scheme, that means there is just a single 128 byte encryption code attached to all the transmissions on the wireless network thus giving it the possibility of being hacked. Someone could, because it is in the air, it is available. There are technologies coming out which are changing that but for the time being this is the case.

Finally, Local Users, for example if you have a disgruntled employee or someone who has access to stuff that they shouldn't, you are subject to physical damage and the other thing, is we get back to non-secure practices such as writing down passwords and sticking it where it is easy to find.

Some of the possible outcomes are interruption of service. Normally this come through the internet in terms of hacking, in terms of viruses, as you may remember, we had problems with viruses that hit us during session. There also could be denial of service which means the websites, web servers or firewalls are tied up so badly that nothing can get through. There is no access to the internet because of this.

Loss of data is deleted or moved files, it also means destroyed storage devices and media.

Data integrity means that things can be modified. Our website could be modified. Someone could come in and change the text of bills, not changing the text of the bill that you are reading or what the public sees in print, but it certainly can be an embarrassment and is something that we need to be concerned about.

Disclosure of confidential information is another aspect of the concerns about data. Can someone get in and actually get to data that is secure and should not be accessed. Our Legal Division has about 80% of their work that is confidential whether it is bill drafts or opinion letters. Those items are not to be accessible by anyone except the attorneys and their clients.

Political impact is how it can affect you. If an e-mail you sent to a constituent or another legislator got in the wrong hands it could be damaging. If something happened to our website or e-mail then that damages our image. These are the kinds of things we want to avoid.

We have put in a firewall as a safety precaution. The firewall is not the be all or end all to prevent things but it does a good job of preventing most unauthorized entry into our network.
Any virus software and e-mail filtering; we do have Norton Anti-Virus software in place on our e-mail server. We also have a filtering program that does a lot of pre-filtering. This is primarily to eliminate any possibility of viruses coming through our firewall into the system or going out.

System and network monitoring, currently we do this on a regular basis. We monitor the logs of what is going on. We look at who is trying to get into our firewall, who is knocking at our door. We are looking at software that will improve the effectiveness of this as well as the efficiency.

Physical Security in terms of our network we have locks on the doors into the computer room. There are more things we can do on physical security and we're looking at those as well. It also involves the end user locking their doors, turning off their computers, making sure that access to the equipment is not an easy thing for anyone.

Encryption is one of the things that we can add that we don't currently have and that essentially is a way for you to send e-mail that is not in plain text format, it is in an encrypted form. There are different ways that this can be done. There are some very basic ways and then there are some ways that end up costing money because you're using an outside key service.

Patching. Over the last year we have applied several system patches to our web server, our e-mail software, a number of pieces of software that we run, the operating systems, most of these patches, including Internet Explorer, that we apply have really been geared towards improving and removing security loopholes. That is something we are very vigilant about, you cannot let down your guard. He said he has a good staff, who work hard and are very concerned about making sure that our system remains available, that we do not have to deal with the kinds of issues mentioned before.

Education is where we have not been strong. We intend to get stronger. Today is the beginning of our education process. We thought we would put this before the committee, give them an opportunity to hear what we have to say and also this will be something we will be putting forward to the Divisions Chiefs. We hope the education will change people's awareness and also their attitudes towards their individual responsibilities with respect to security.

Other technologies we are looking are Network Intrusion Detection software. It is probably one of the primary things. This will replace the network monitoring we're doing manually. This provides for automatic monitoring. There are a number of parameters that you can

set that allow you to look for specific things, allow you to send alarms to specific people and the nature of those alarms.

A Radius Server is an extra piece of equipment with software running that provides an additional layer of authorization for the network. This is one of the pieces we'll be putting into place that will further protect our wireless network. It is also a piece of technology that we will be looking at for other directions we're moving in.

Virtual Private Networking (VPN), which we've discussed before, is something that we are moving ahead with, although albeit a little slow at this time, but we are moving into the direction of having it done before summer.

When I spoke about encryption, Private Key Infrastructures (PKI) is a technology that is being used in a lot of areas. The main thing with the PKI is that it usually requires an external service for which you have a charge per user. That charge runs about $40 apiece. Is it worth it? Is there other technology? Yes there are. This type of structure also allows you to do electronic signature authentication.

Finally we get into the world of the future and that is Biometrics which is the use of fingerprints, retinal scans, and other unique physical characteristics for authorization into a network or computer system. There are actually some computer manufacturers that are putting these on their computers as part of their process as an add-on.

In implementation of the Information Systems' Plan we formed a security team. The security team we have is made of himself, Eric Dugger and Suzie Christensen, Senior Web Technician. They are both MCSE certified and have a great deal of experience in the technical areas that we need to make this whole thing work.

Next is to introduce security awareness and we're coming before you and will be going before our Division Chiefs as well as the Secretary of the Senate and the Chief Clerk of the Assembly with this same information.

We're going to perform an internal audit. We want to do our best to take care of all the security weaknesses that we can discover on our own. We feel that there are a lot of areas where we can improve what we're doing and with the tools we already have and are familiar with.

We're going to craft and implement practical network security policies. What we're really looking at is something that not only will be for the end user but also for the network. We want to be sure that we are doing the right thing in Information Systems. We also want to be sure that our end users are aware of what practices are acceptable and what kinds of environments they should be able to work in.

We want to build security awareness through education of end users. This is going to be an educational process, we're probably going to be putting together materials and whether or not to get into formal classroom situation.

Once we have gone through these steps, including our own internal audit, we're going to look at using a professional security consulting service to increase our knowledge of the vulnerabilities. This means that we would possibly have an evaluation by an outside company and we might have an "ethical hack" come in from the outside and figure out our weaknesses. What we hope to learn is what we don't know and from that determine what further steps we can take to strengthen or correct those areas. The next step would be is to actually take advantage of what they have provided and put that into practice.

And then, perform periodic security reviews. You can't just stop at setting it up and saying everything is going to run fine. Technologies change, hackers get smarter and our system and software changes. We need to be ever alert, we need to be continually making sure we keep a secure network.

Mr. Beers asked what percentage increase Mr. Smith attributes to Microsoft licensing?
Mr. Smith responded that we have roughly $138,000 in the software upgrade item on the appropriations and are looking at almost that much from the standpoint that there are two parts to the Microsoft licensing. One is that there is a catch-up fee and called an "upgrade advantage." This gives us the opportunity to take any licenses that we have that are not considered current by Microsoft, putting those licenses on that "upgrade advantage" allows us to come into the next phase which they call "Software Assurance" without having to pay penalties of having to buy a whole new piece of software. It is pretty expensive and about a third of what we are spending. The rest of that is the actual annual license fee, we really pay a biennial fee and is going to cost us about $100,000-110,000 for licenses for Microsoft Office, the SQL server, Exchange, etc.

Mr. Beers requested Mr. Smith to put together a document expressing this information in a percentage format with a before and after picture with the new licensing.

*VII. Consideration of Future Meeting Dates and Topics – Assemblyman Bob Price, Chair.

Mr. Price asked Mr. Smith what would be a safe time giving IS plenty of time to take care of business that we need prior to session?

Mr. Smith replied that some of the things that we need to be considering over the next few months would be the changes to the website policy. The other is that we will be bringing to this subcommittee security policies that we have drafted and will hopefully be ready by the fall. He said if we are going to buy new laptops we would have to have a decision by early September (he revised this after the meeting concluded to May).

The committee tentatively set up a meeting for Thursday, September 19, 2002.

VIII. Public Testimony.

Mr. Mark Blomstrom, Deputy Director, Department of Information Technology (DOIT), said he would like to compliment Mr. Smith for a very comprehensive presentation on security issues.

Mr. Blomstrom said a couple of things were raised and they have been working with LCB on the security angle from the standpoint of an intrusion detection system. We are looking at combining our efforts in terms of one type of system which would be helpful for both the legislative and executive branches in terms of having a system which is compatible.

Microsoft licensing was mentioned and he said while they can determine today a percentage of increase based on where we are at, speaking now for DOIT, we can also look at what it would cost under Microsoft's proposed licensing costs. The jury is still out in the sense that we are pushing Microsoft as an organization, and it's very difficult to push that giant very far, however, Terry Savage, Director of DOIT, has been appointed by the National Associations of State CIOs as a spokesperson for NASCIO in talking to Microsoft at this point and he is just starting to communicate with them. The reason that is significant is because this is the first effort that we know of on the part of states as a group in forming what might be described as a buying cooperative to apply pressure on Microsoft to back off the high price increases that are coming.

He said he'd like to mention they have worked with LCB staff on a cable system around the Capitol Complex. At this point, we spoke with Charter Communications, who is the cable operator for the Carson City area, and they are now delivering cable content. Parts of that channels off the Charter Communications system will be picked off and be rebroadcast along with the current video from multiple rooms here in the Legislative Building. DOIT will rebroadcast through the greater Capitol area here in Carson City and selected channels will be placed over our communication system and pumped down to Las Vegas for viewing there. That would be in addition to what LCB is sending down in compressed video.

There being no further comments, the meeting was adjourned at 2:39 p.m.

Respectfully submitted by,
Sylvia Wiese

_____
Assemblyman Bob Price, Chair