Standing Committee on Public Accounts

Hansard Verbatim Report

No. 9 – December 18, 2000

Legislative Assembly of Saskatchewan

Twenty-fourth Legislature

STANDING COMMITTEE ON PUBLIC ACCOUNTS
2000

Ken Krawetz, Chair
Canora-Pelly

Pat Lorje, Vice-Chair
Saskatoon Southeast

Rod Gantefoer
Melfort-Tisdale

Debbie Higgins
Moose Jaw Wakamow

Carolyn Jones
Saskatoon Meewasin

Carl Kwiatkowski
Carrot River Valley

Lyle Stewart
Thunder Creek

Kim Trew
Regina Coronation Park

Milton Wakefield
Lloydminster

Mark Wartman
Regina Qu'Appelle Valley

Published under the authority of The Honourable Ron Osika, Speaker

The committee met at 1:30 p.m.

The Chair: — We'll call the meeting to order.

Just a couple of points. We had to make some changes to the, I guess, discussed timelines that we talked about last meeting. And just to inform you we worked on some of the things that we might want to start on today and tomorrow.

Myself and the Vice-Chair, discussed certain chapters that we felt we would be able to begin with in the next two days, and then ending with the volume 1 from 2000 fall report, which is a broader document which we would not finish tomorrow when we begin it, and then that would allow us to end at an appropriate time.

We had talked about beginning at 11 a.m. this morning, but because of the inability of certain members from the Finance department to be ready for this week, we had to take out a chapter.

We felt we might be able to introduce the chapter on pensions. But when that was withdrawn from the proposed agenda, we didn't bump anything up to be able to start earlier because officials had been contacted already and it was just going to create too large of a problem. So rather than create a problem, we just felt that beginning at 1:30 would allow each and every one of you to travel in this morning, if you so decided.

Maybe we'll have to ensure that notices of meetings . . . I don't know whether the Clerk's office sends them directly to each constituency office, but I know in the case of Mr. Wakefield, the memo never went to his office, and he was prepared for this morning. Ms. Jones, you're the same.

If we get changes that occur to the agenda or to the times that we propose, we'll have to make sure that either I, as Chair, contact the members — each and every one of you — or maybe through the Vice-Chair that we ensure that everybody knows that there is a change to an agenda, if that happens in the future. And I apologize for that bit of an error that occurred. But we did make those changes I guess early part of last week.

The first half hour, as I indicated, was more of an adoption of the agenda and some discussions about the format that the committee works under. And I understand from previous PAC (Public Accounts Committee) committees that there is an outline of the committee's procedure that is read into the record so that we have an idea of how we will produce reports.

But before we get into that, is there any discussion of the agenda that you see before you? Regarding the timeline of today, 1:30 to 5, is there any problems with trying to go to 5? And then tomorrow beginning in the morning at 9 till noon, and then 1:30 to 5 as well. Mr. Wartman?

Mr. Wartman: — A question just with regard to a break. Will it be right at 3 o'clock? I'm asking because of a possibility of a conference call that I need to pick for a minute.

The Chair: — Today's break?

Mr. Wartman: — Yes.

The Chair: — Or tomorrow? Today's break is at 2:30.

Mr. Wartman: — Will that work out okay, Greg, according to our earlier conversation?

Mr. Putz: — Myron wanted to know before 3. So that will give me time to call him.

Mr. Wartman: — Before 3?

Mr. Putz: — Before 3.

Mr. Wartman: — All right. Thanks.

Mr. Trew: — I'm most anxious for 5 o'clock not to slide. I have another, former engagement.

The Chair: — Oh, no. We can be firm on that.

Mr. Trew: — Okay. That will work.

The Chair: — Both days?

Mr. Trew: — No. Today is the day that's a problem.

Ms. Lorje: — And if possible I'd like to see us be out of here before 5 o'clock just because I have to . . . I have another meeting I have to attend out of the city. But if we have to sit here . . .

The Chair: — Is this a supper engagement besides the brunch? Okay.

Ms. Lorje: — It is.

The Chair: — We'll try to ensure that we're on the short side of 5 rather than the long side of 5.

Ms. Jones: — Tomorrow as well because we need to be travelling in the dark. Short side of 5.

The Chair: — Okay. Any other questions about the agenda?

Ms. Lorje: — I'll just raise this now. I don't want it to extend the discussion but, Ken, you and I had agreed that we would put Board of Internal Economy on tomorrow. And I have been reviewing what the committee has done in the past and Mr. Gantefoer would be aware of this when it last came to this committee. I believe that there was agreement at that time that one legislative committee would not act as an oversight for another legislative committee.

And so I'm wondering if we even need to consider this. I think that what we really need is to make sure that the Board of Internal Economy considers this particular chapter rather than have it on our agenda. So I think that that can probably decrease our agenda for tomorrow if we all agree that it would be inappropriate for this legislative committee to be acting as an overseer of another legislative committee.

Mr. Gantefoer: — Thank you, Mr. Chair. Yes I think that that may well be the case and that that will be our decision but we still have to put it on the agenda in terms of an item that's been referred to this committee by way of a Provincial Auditor's report which we're obligated to deal with.

It's our decision as to what we deem is the most appropriate way of dealing with any of these issues so we have to bring them forward. I think there may be other items on the agenda that may indeed take less time so we should be just flexible about the time.

The Chair: — That was the reason, Ms. Lorje, for me putting it on the agenda was that regardless of what you as a committee decide to do with that item, we still have to move it somewhere, deal with it in some way but we want to have it in the record that this particular chapter has been dealt with.

And also with regards to the times, as I indicated in my letter to Ms. Lorje, these are flexible in nature. I have, you know, just looking at the number of recommendations and the chapters, just sort of guesstimated as to what the times might be and I hope that everyone is aware that the next two days will flow according to your needs and your wishes and we'll take it from there. So any further question?

Mr. Wendel: — Just on the agenda committee. Last week we tabled volume 3 of our fall report and I've asked the people that are presenting today and tomorrow to update the items that are here and bring in the volume 3 items. It'll make more efficient use of your time, as they're essentially the same things that are in the old reports. So for the planning 2000 which is dealing with year 2000, the fall report volume 3 has a summary of what's happened, what the results were, and it just brings it forward.

And the Board of Internal Economy, it sounds as you're not going to deal with it so I guess it won't be an issue. So it's essentially the year 2000 item. I've asked them to bring forward the chapter from volume 3.

The Chair: — Okay.

Mr. Wendel: — Sorry, the second question is do you want new binders for January with volume 3 built into them so that as you begin to work through the departments, as you begin to call them, you can deal with the most current stuff and the old stuff at the same time so it's efficient?

The Chair: — By new binders, Mr. Wendel, did you indicate just addendums that we would place at the various times, places?

Mr. Wendel: — We could do that or if it's a lot of changes, we'll give you new ones and you can turn in the old ones. Whatever you wish.

Mr. Wartman: — Yes, that's a very important point around the possibility of new information for binders, we need larger rings.

The Chair: — I think the consensus is that everyone would like to have the most up-to-date material to deal with. So either by way of additions to this existing binder or by replacement of, I think for our next meeting, if it's in January, we would appreciate the updated material using volume 3.

Mr. Wendel: — We'll make that available to you in January.

The Chair: — Okay could we have a motion to adopt the agenda, the proposed agenda, for the next couple of days? Mr. Kwiatkowski? Mr. Wartman? We don't need a seconder. All in favour? Opposed? Seeing none, carried.

Okay now as far as the report that this committee will eventually put forward to the Legislative Assembly, I guess this page identifies the committee's procedure for dealing with recommendations of the Provincial Auditor. And I'd like to share this with you.

As the Committee reviews and makes decisions about the various recommendations made by the Provincial Auditor's Office, the Chair and the Vice-Chair should work to ensure that the committee decisions are as clearly understood as possible. This is important for the members because they need to be aware in no uncertain terms of what they are agreeing to, and for the Committee Clerk who must include the decisions in the committee's own report. The following are some options for the committee to consider at the conclusion of its consideration of a recommendation made by the Provincial Auditor. The Chair and Vice-Chair have, whenever possible, attempted to guide the committee along these lines.

1. In the case where the committee agrees with the auditor's recommendation and through questioning departmental officials finds the department has or will comply, the committee should, for its report, agree to concur with the auditor's recommendation and note compliance or that the department intends to comply.

2. In the case where the committee agrees with the auditor's recommendation but finds that the department is unwilling to comply, for whatever reason, the committee should, for its report agree to adopt the auditor's recommendation for inclusion in its own report.

3. In the case where the committee disagrees with the auditor's recommendation, it should note this for its report and provide the reasons why it disagrees with the Provincial Auditor.

4. In the case where the committee would rather make an independent recommendation, it should do so by the adoption of a motion so that all members are clearly aware of what will be reported to the Assembly.

Final two bullets:

It has been the committee's practice to adopt matters for its report by simple agreement. If there is dispute about what the committee should adopt for inclusion in its report then the Chair should ask that a motion be moved so that the matter can be debated and resolved by majority decision.

And the second bullet:

For the purposes of clarity, when the committee decides to

deviate from a particular Auditor's recommendation and make its own independent recommendation, the Chair should ask that it be put in the form of a motion so that all members can be clear of the wording.

Any questions or discussions on those guidelines? Previous, as I've indicated, I believe previous PAC committees have followed that and it seems to have worked well.

Seeing no discussion, are there any other questions about any of the material from previous meetings, specifically the last meeting that anybody wants to bring up at this moment? We're able to start with the officials I think very quickly on the next item.

Okay, seeing none, then let's move into chapter no. 17, Preparing for Year 2000. Mr. Wendel.

Mr. Wendel: — Yes, Mr. Chair. I'll have Phil Creaser join me up here and Phil has a presentation to make to the committee. Can you see past me or shall I move over there somewhere. How about over there.

Mr. Creaser: — Okay, thank you, Mr. Chair, members. First, before I start . . .

The Chair: — Excuse me, just one moment.

Mr. Paton: — Mr. Chair, I'm aware that the officials are in the building that I think are speaking to this chapter. If you want we could have them maybe attend the presentation as well.

The Chair: — If we could ask Mr. Creaser to just hold on for one second. We are a little early . . . it's good to be early. So we'll just ensure that the officials are present as well.

The committee recessed for a period of time.

The Chair: — Good afternoon, gentlemen. We have officials with us this afternoon from both the Economic and Co-operative Development branch, as well as Saskatchewan Health, and if we might begin with some introductions.

Mr. Whelan: — We've got three names here from Economic and Co-operative Development; they're not all here yet but that's all right, I think. I'm Tim Whelan, with Economic and Co-operative Development. I was . . . I ran the Y2K (Year 2000) coordination office.

Mr. Hersche: — I'm Bob Hersche. I'm executive director of the information technology office in Economic Development.

Mr. Gardner: — Neil Gardner. I'm the executive director of the corporate information and technology branch in Health.

Mr. Wilkie: — I'm Jack Wilkie, Saskatchewan Health. I was the Year 2000 project manager for Health.

The Chair: — Thank you very much. Welcome gentlemen. These officials will also be our officials if they would stay for the second chapter, which is on the information technology security as well. Right. Good. Just to ensure that that's there.

Prior to getting into discussion about this chapter, I would like to read to each of our witnesses the testimony of witnesses appearing before the committee, regulations. And it indicates this:

Witnesses should be aware that when appearing before a legislative committee, your testimony is entitled to have the protection of parliamentary privilege. The evidence you provide to this committee cannot be used against you as the subject of a civil action.

In addition, I wish to advise you that you are protected by section 13 of the Canadian Charter of Rights and Freedoms, which provides that:

> A witness who testifies in any proceedings has the right not to have any incriminating evidence so given used to incriminate that witness in any other proceedings, except in a prosecution for perjury or for the giving of contradictory evidence.

A witness must answer all questions put by the committee. Where a member of the committee requests written information of your department, I ask that 15 copies be submitted to the committee Clerk, who will then distribute the document and record it as a tabled document.

You are reminded to please address all comments through the Chair. Thank you.

Mr. Creaser: — Thank you, Mr. Chair, and fellow members of the Public Accounts Committee. Thanks, Terry, for putting the brakes on me there.

I'm glad to see that now we have some of the officials here today to talk about . . . as we're talking about the conclusion of our Y2K work, seeing as how we're 300 and some days into the new year. These are some of the people that did a lot of the hard work this year to — or the last two or three years — to prepare for the Year 2000, and I would like to thank them myself for their hard work.

I wanted to do just a quick summary of what we've talked about. Over the last three years, three and a half years, we've tabled about six reports on Y2K (Year 2000). Now we've discussed the first three with PAC in the fall of '98 and I think we were one of the few provinces in Canada that actually had Y2K discussed with the Public Accounts Committee.

We're hoping to get your agreement on the final three chapters today and put a . . . close the book on Y2K I guess for, hopefully, unless 2001 happens to rear its ugly head and something happens, but I don't think so right now.

In the presentation, most of my remarks will be concentrated on the fall of 1999 report. The chapter in the fall of '99 concentrated on the work of four groups in the government. First of all we had the Saskatchewan Emergency Planning Group that prepared the emergency plan for Saskatchewan and worked with the municipalities to ensure that they were ready for any kind of an emergency.

And they've just worked with the Emergency Measures Canada

to adjust their plan for the Year 2000 to ensure that they were in place on December 31 in case there is . . . was some kind of a Y2K emergency, and thank goodness there wasn't. And they even went to the work of having a war room prepared to handle an emergency situation.

The second group was the information technology office, Tim's group here. They did, over the course of the years that I have worked with them, they did a number of surveys and also had an independent assessment done of the work of the number of the departments preparing for the Year 2000.

And they also had set up a group to monitor the departments and agencies — I think there was about 36 of them — to ensure that they were working to get their Year 2000 work complete, get their plans in place and get their systems remediated. And I think, as of the time we had finished our work, they were about 97 per cent complete; 97 per cent of their work was complete and their contingency plans were around 93 per cent.

The work of the independent assessor basically agreed with the recommendations that we've made in the past and helped provide comfort that the work that was being done was sufficient.

The third group that we worked with in coming up with our . . . doing our work in Y2K in the fall was Crown Investments Corporation. The Crown Investments Corporation worked with the Crowns, the CIC (Crown Investments Corporation of Saskatchewan) Crowns, to ensure that, and did quarterly surveys of their progress and wrote quarterly reports that then were, I believe, tabled with the Crown Corporations . . . CIC board, I'm sorry. And so they were able to discuss them.

We also, during the course of 1999, we met with SPC (Saskatchewan Power Corporation), SaskPower, SaskTel, and Energy to discuss their Year 2000 work and how they had gone about remediating some of their issues. I think the final report on the . . . that we looked at for CIC said that the three-quarters of the Crowns were done and that the last quarter were nearly done.

The final group that we evaluated in our final report was with the Health districts. I think at one point there was quite a bit of a concern about was Health going to be ready and were the districts going to be ready.

They had set up a project management office chaired by Jack Wilkie, and their job was to monitor and make recommendations on remedial action for the districts to help them get through the Y2K crisis. They looked at biomedical equipment, information systems, facilities and the supply chain, the medical supplies. They worked with Regina and Saskatoon Health Districts on biomedical equipment and they used consultants to help them with the other three areas.

And at the time we were finishing they were just in the process of finalizing contingency plans. And they were in the process of receiving their independent assessments from each district and I think they were partway through that. And this was in October of 1999.

Based on the work that we did and the contacts we had with organizations at that time, we basically said that we felt that the progress was solid, that all the sectors in the government had taken reasonable steps to prepare for Y2K going in. And the only recommendation we made on the report was a continuation of one we had in the spring report, was that we felt it would be good for all the sectors to do a review of the lessons learned from Y2K and to take advantage of those lessons in their own work.

The recommendations that we had in the spring report of 1999, we were asking that reasonable steps be taken to ensure third parties and partners were ready, there was a complete contingency plan and all contingency plans were complete and the lessons learned were recorded. And in the fall of '99 we reiterated the lessons learned. We felt at that point that we're getting pretty close to the end of the year. The other recommendations were somewhat redundant by the time the report came out as well.

Finally, just to follow up on our last recommendation. In the fall of this year we talked to the Department of Health, CIC and to the information technology office about what had they done about the lessons learned; if they had prepared any reports or done any studies on what they felt they had achieved with the lessons learned from Year 2000. And all three of them are able to provide me with a report that they had done. And I think, correct me if I'm wrong, if they're all public documents, but I believe they are.

In our report we also identified some of the challenges for the future. As far as lessons learned, just a few of them that seem to be fairly common in most of the reports. First of all, accountability works. It seemed that the process that was taken with having these three organizations just monitoring the work of the various agencies and the agencies being accountable for their own work seemed to be . . . it was a different process and was done in many jurisdictions where they actually had . . . The Y2K work was being coordinated and being managed by central agencies and it seemed that the role that they took here seemed to work fairly well and obviously the work got done.

Secondly, on the communication works, there was talk throughout about some of the firsts in getting groups together; the departments, the Crown corporations, and actually even the municipalities. City of Regina organized some workshops that I attended that had the Crown corporations and most of the departments there.

The utilities worked together quite a bit. They actually helped coordinate their plans, the three major utilities — SaskPower, SaskEnergy, and SaskTel — because they all were dependent on each other and they seem to be able to do a pretty good job of coordinating their plans and the communication between the organizations seem to be fairly strong.

Next, contingency planning was something that is kind of near and dear to the auditor's heart. And we were concerned about contingency planning throughout the year 2000 work but we found that it was very well done in the Crown sector in particular. In the other sectors, the plans were finalized and completed on time and so we were . . . seemed to heighten the awareness of the importance of contingency plans.

And finally we can't go without saying that the strong senior management commitment to the Y2K work helped ensure that the work was done and was done on time because there was only one deadline.

Finally just a couple of comments and challenges. I think there was a lot of work done for Y2K. One of the things that seemed to be prominent in that was a lot of the planning work that was done. It certainly stressed the strong planning for Y2K could be carried forward into the strong IT (information technology) planning for the future. And I know with the PMART (performance management and accountability review team) initiative there's more work being done now in the Treasury Board sector at least to try to coordinate the IT strategic planning at a more consolidated level or aggregated level.

And it's an opportunity to use the updated technology as governments moving into the world of e-government and e-commerce and also a need to — and the work that's going on and we'll be talking about that in a few minutes — the need to improve security so it's adequate again to move into the e-government realm.

The government agencies, Crown corporations did a lot of work on their inventories and systems and practices and I hope that they maintain these lists, keep track of it, and maintain these inventories for the long term. And in a few cases where the contingency planning could still be improved that there is a continual effort by agencies that are still working on their contingency plans to finish them and get them approved by senior management.

That's all I have to say, Mr. Chair. That's my comments and again, thanks to the officials for their hard work.

The Chair: — Good. Thank you very much, Mr. Creaser. Any questions or comments to be directed towards Mr. Creaser from any of the members? Maybe there will be after the next presentation.

I'd like to welcome, I believe, two additional members. If introductions could take place at this time before we have the presentations from the government officials.

Mr. Spannier: — Larry Spannier, deputy minister of Economic and Co-operative Development.

The Chair: — Welcome, Larry.

Mr. Shaw: — Hi. Chairman, my apologies for being late. I had an incorrect start time on my calendar so I'm going to blame it to technology. My name is Mike Shaw. I'm the senior vice-president of Crown Investments Corporation.

The Chair: — Welcome, Mike. It was a security breach.

Mr. Shaw: — Lack of contingency planning.

The Chair: — Okay. I'd ask the officials for your presentation or comments and I'm not sure who wants to begin.

Mr. Hersche: — We don't have a presentation per se. Essentially we're open to questions.

The Chair: — Great. Good, okay. We'll then begin with questions of either the report or the chapter as identified by Mr. Creaser or of any of the departmental officials that we have before us.

Mr. Gantefoer: — I thank you, Mr. Chair, and welcome to all of you. I guess on December 31 last year everyone in the world sort of watched with some trepidation as to what was going to happen. And it struck me, as we watched the coverage on the media as New Year's started in Australia or somewhere and moved around the world, that I didn't notice the lights going out anywhere. I don't recall that we had reports of any major shortfalls of the system anywhere in the world, and I guess that's a tribute to good planning everywhere.

The question is is that I doubt very much if there was the same level of planning that occurred everywhere in the world, and I guess I have sort of a Gordon Sinclair type of question. How much did it cost us?

Mr. Spannier: — On the executive government side, it cost $15 million of which was . . . all of that was absorbed within the department's normal operating budgets. On the Crown side, SaskTel was $25 million, and a lot of that was to . . . a good portion of that was to upgrade existing technology and so on, as well as $17 million were spent between SaskEnergy and SaskPower.

And then in addition to that, as you are aware, there was $50 million given to the Department of Health. A $50 million fund was established to assist the district health boards with their Y2K readiness.

Mr. Gantefoer: — Many of those investments though, were or have longer term beneficial effects for the department's affected. Is that not correct?

Mr. Spannier: — Yes.

Mr. Gantefoer: — Have you been able to identify or isolate in any way what the actual planning and effort was . . . what did that cost I mean to have the special office operating and things of that nature which would be more specific to the actual cost of preparing for Y2K rather than in the longer term investments? It would be much less than this hundred odd million.

Mr. Spannier: — Yes, right on. As you are aware, the Y2K problem or issue was coordinated by the information technology office. Their budget is around a half a million dollars so that's all that was basically allocated for administration purposes.

Mr. Gantefoer: — What's happened to that office?

Mr. Spannier: — Actually the office continues to exist. This is one of the issues that in addition to their other duties they took on, and what the office focuses on now is the whole coordinates information technology right across government now. That's sort of a centralized office. We're moving forward on the whole e-government initiative and government on line and that type of thing.

Mr. Gantefoer: — I'll leave the e-government. I think that's

coming up in the next section on technology and security and some of those issues, so thank you, Mr. Chair.

The Chair: — Thank you, Mr. Gantefoer. Any further comments or questions from any of the members?

Mr. Wakefield: — Sorry, I was formulating a question in my mind here. All the coordination that went on here during this exercise, like it has some long-term benefits in terms of doing the audit inventories, efficiencies, all those things.

As we're moving ahead — and maybe this will be coming up under what we call e-government — was there a recognition at all that information technology could be more coordinated rather than each particular department or Crowns or whatever having their own functioning IT? Is there a redundancy that was recognized?

Mr. Hersche: — As Mr. Spannier talked about before, the information technology office, there was . . . has been expanded, and it has looked at that role in terms of coordination. And because of Y2K there was recognition of the kinds of plans, that there was more potential for duplication. Some of the kinds of things that the ITO office is doing now is essentially doing that kind of larger plan for the government, working with the systems management council of all of the departments, bringing together those kinds of projects.

So much of the organization that came about because of Y2K, we are extending those kinds of structures, if you will, into ongoing operations, and hopefully again to make sure that we don't duplicate efforts and that we do . . . are able to focus as much as possible.

Ms. Lorje: — Well I was always of the personal opinion that Y2K was nothing but a giant scam on the part of certain people in the computer industry to maximize their job prospects. And observing the near public hysteria that occurred in some parts of the world and, as Mr. Gantefoer has correctly pointed out, the absolutely total lack of public disasters that happened on January 1, I'm simply confirmed in my opinion.

The other thing I noticed was that as each date approached and all the doomsayers were not able to present us with the sky falling in, they changed their tune and there was yet another thing that we had to be aware of — the September 29 bug, the February 28 bug, the January 1 bug. And I'm sure that I'm missing a whole lot of them.

I still think it was a scam. I would like to know, is the computer industry predicting a new one for us now?

Mr. Spannier: — Not that we're aware of.

Mr. Hersche: — No. In terms of those kinds of disasters or things, there's no large disaster looming that anyone's aware of. We have some concerns. As you know, periodically there are viruses that come in the systems that do affect things. We deal with those.

Ms. Lorje: — I think the opposition party is very much aware of that.

Mr. Hersche: — So we are looking at, we are looking at ways to make sure that our systems are secure and function and are protected from those kinds of viruses. But in terms of that, anything that kind of scope, no, we're not aware.

Ms. Lorje: — Well even though I do think the whole Y2K thing was a scam, I do think that a lot of valuable work was accomplished by many public agencies. I think there was a need to upgrade certain technologies. There was a need to have better coordination.

Some systems had been put in sort of jury-rigged or they grew like Topsy. So I think that there was some beneficial work that happened. But I just hope that we are never once again presented with this need to put our public . . . to divert public resources away from day-to-day operations of things into planning for a crisis that I think was created by an industry.

The Chair: — Mr. Whelan, did you have a comment?

Mr. Whelan: — Yes, a couple . . . I think the points you've said are very valuable. I found working on this, and I'm sure Jack would agree, that it was an issue of failure of communication and that the more one spent with the issue, the higher one's level of confidence rose.

My own level of confidence was satisfied about 15 months before the Y2K deadline at a meeting of officials in Ottawa where someone representing the electrical industry in North America — what's it called, NERC, North American Electrical Reliability Council, or something like that — basically said a large scale failure of electrical system was impossible and that the entire system had been built like that since the last one in the early '60s.

So people that were close to the issues, level of confidence was up here, but the public's information wasn't getting through. It was much easier for the media to write a headline saying the world is going to come to an end; the sky is falling. And they separated it. It wasn't until almost until the end of 1999 where public's concerns began to be mashed and there was less hysteria.

The other thing that's worth noting about this is that Canada as a whole, as a result of the very large effort put out by the federal government, has got a good understanding of the infrastructure of this country for the first time since the end of World War II.

And they're moving forward with that and the federal government is likely to establish a federal infrastructure program to keep the infrastructure initially of the federal government safe in perpetuity and eventually maybe into the public or the private sector as well, something that would have gone forth and have been approved by the federal cabinet if it had not of been for the federal election. And I'm told that it's going to be back on the order paper in February. But it's a direct outgrowth of the work that was done for Y2K.

Ms. Lorje: — Speaking again rather cynically, I'd be satisfied if the federal government would simply fund a national highways program so that we could do something about Highway 16 and Highway 1.

Mr. Wartman: — Just a curiosity. I noted there's been significant upgrading in the technologies that we had both in the medical area and just in terms of the computers that were being used in both our government departmental area and in the Crowns.

And my curiosity is around what happened to the technologies, health technologies that were updated? And what happened to the computers that were formally in place that were replaced? Were those put into the system once they were checked out? Are they being used by schools in need or what happened to that equipment?

Mr. Hersche: — In terms of the computers and the replacement of computers, we normally have a system to . . . and they would all be the same. They would essentially go through SPMC (Saskatchewan Property Management Corporation). Many of them from SPMC will be refurbished; some that are not refurbished go on public auction, those that can be refurbished do go into the school system. Now I'll turn that over to Health.

Mr. Gardner: — On the Health side we literally had to check thousands and thousands of pieces of equipment. On the medical device side there was actually in the end about 150 that had to be either replaced or upgraded. We tried to upgrade wherever we could, and these are things like defibrillators, heart monitors, very critical kinds of devices. There were some that simply could not be upgraded and, you know, were not reusable for patient safety concerns.

Mr. Wartman: — Following the year 2000, December 31, were those machines subsequently tested to see whether or not they were functional?

Mr. Wilkie: — The machines that have been replaced?

Mr. Wartman: — Yes, for example, a defibrillator or some of the machines that would put solution . . .

Mr. Wilkie: — Anything that wasn't removed from service that wasn't deemed to be unserviceable would have been tested, and there's an ongoing testing environment within environment, within sort of the biomedical engineering methodologies that are used so that they would have been tested on an ongoing basis.

Mr. Wartman: — Thank you.

The Chair: — Thank you. Any further questions? I would refer you to chapter 17 of the documents that are in your binder. It's volume 2 of the '99 report and Mr. Wendel has also circulated chapter 15 of the fall report, the 2000 fall report, volume 3, in which there are no new recommendations in chapter 15.

But in the previous chapter, chapter 17 of volume 2, there is one recommendation on page 338, and that recommendation is that:

> We continue to recommend that the Y2K Office, CIC, and the Department of Health record the lessons learned from the Year 2000 work so that they can be used in future government projects.

Any comments, any questions, any further comments from the auditor's office.

Mr. Gantefoer? Questions first of all?

Ms. Jones: — No question. I did have a comment. I was comparing the volume 3 and you clarified that for me, that there were no further new recommendations coming out of that and so we're dealing with the recommendation on 338, which is chapter 17, as I understand it.

Having read through it earlier, it, chapter 17 was quite tentative, I thought, in its approval of what had happened thus far. And looking at the new addendum in chapter 15, it is fairly complimentary saying that the government ought to be commended for its hard work and diligence. And so I'm pleased to see that we've made some progress in somebody's eyes at least.

I don't think that we should have any difficulty concurring with the auditor's recommendation. I think that it is quite self-evident that the work that went on was a valuable exercise, that there were lessons learned; and I think that there is nothing identified in non-compliance so I think we simply need to concur and note that compliance has been done. And I would move that.

The Chair: — Okay, we have resolution that we agree with and that compliance has been noted. Any further discussion? All in favour? Opposed? Carried.

Any further comments on planning for 2000 chapter 17 or 15? No other recommendations, as I've noted, but are there any other comments before we . . . Ms. Lorje?

Ms. Lorje: — Do we have to formally note that we've also reviewed chapter 15 of the 2000 fall report?

The Chair: — It will be noted. Thank you for that.

Okay we're . . . at 3 o'clock is the next item which is the information technology security one and with officials here, I'm just wondering if we couldn't recess right at the moment and maybe reconvene a bit sooner if the officials . . . (inaudible interjection) . . . You want to do that first?

We'll do the introductions and then we can recess exactly at 2:30 to allow the previous discussion to take place. Sure, let's begin. If we could have the . . . Reference of course is to chapter 11 of the '99 spring report and chapter 18 of the fall report. And please note that there is no additional chapter from the volume 3 report so it is the documents that are contained within your, within your binder.

If you're looking for it, it's immediately, it's the red tab immediately next to the orange tab, which is the one that we dealt with on preparing for 2000.

Ms. Jones: — It was chapter 11 that . . . I saw 18 — I didn't realize that 11 was tucked in behind it.

The Chair: — You have both. Okay, Mr. Wendel.

Mr. Wendel: — Mr. Chair, I have Victor Schwab with me

today and he'll be giving you the presentation on this. He's advised me his presentation is about 20 to 25 minutes. So is that . . .

The Chair: — I think then we will not begin it because I don't think it's proper to recess it in the middle. So let's recess at the moment, and if we could start at 10 to 3 please rather than at 3 o'clock and that way we don't have to have our officials waiting out in the hallways. Mr. Wartman, question?

Mr. Wartman: — Can I check first with Mr. Putz? The information was as long as we spoke before 3 or as close to 3 as possible.

Mr. Putz: — That's correct. For the other members of the committee, we have a Tobacco Committee issue going on and the committee members were asked to respond to the Chair of the Tobacco Committee before 3 o'clock so I think this will work out fine.

The committee recessed for a period of time.

The Chair: — And as we were about to begin with a presentation from Mr. Schwab on the information technology security section, I'll turn it over to Victor, please.

Mr. Schwab: — Thank you, Mr. Chair. I'd like to say thank you for the opportunity to review with you our chapters on information technology security. And with yours to follow along, I've also provided a printed copy of the slides that I'll be using.

Just to give you an overview of what I plan to talk about today. First of all, there's been several chapters in our reports dealing with IT security. I will review the work that we've done up to now.

Information technology security. I'd like to highlight the importance of IT security and its importance to government. The chapters that we will be dealing with today are chapter 11 of the 1999 spring report and chapter 18 of the 1999 fall report. I will review some of the recommendations in those two chapters. And finally, I would like to just summarize the key messages of the two chapters. I will get the government officials to provide an update as well.

Just to give you a little bit of background. Our IT security work began with an informational chapter in our 1995 fall report, chapter 5. In 1996 and 1997 we surveyed government departments and Crown corporations and other agencies. Those results were contained in our 1996 spring report and 1997 spring report. These chapters made several recommendations to improve IT security. At that time this committee discussed our recommendations and recommended that the government address our concerns.

The chapters that we are specifically dealing with today are a follow-up to those chapters. Chapter 11 of the 1999 spring report deals with government-wide recommendations that were made. And chapter 18 of the 1999 fall report deals with agencies' specific recommendations.

Information technology security. We define information technology security in terms of having three components — confidentiality, integrity, and availability.

Confidentiality is keeping confidential information from being disclosed. In other words, it is ensuring confidential information is only available to those that have a need to know. For example, passwords can be used to restrict access to certain information.

Integrity is ensuring no errors or unauthorized changes are made to the information. Passwords can also be used to segregate who can give information and who can change information.

Finally, availability is ensuring information is available when needed. Two common ways of ensuring availability is having back-up copies of programs and information, and creating contingency plans to be implemented in the event of a disaster.

Adequate IT security requires policies and procedures. These policies and procedures must be cost-effective in that the cost of implementing the policy or procedure should be outweighed by the benefit.

They should be documented. If they are not documented, employees may not be aware of them. Also, you cannot hold employees responsible to follow them. They must also be distributed. Employees need to know the rules over the IT systems they use. They also need periodic reminders of those policies to ensure they are followed. And finally, they must be monitored for compliance. You need to ensure policies and procedures that are set, are in fact being followed.

Security is only as strong as its weakest link. For example, you could protect your IT equipment by having strong password controls and bolting the equipment down, but if the doors are not locked, someone could come in and vandalize the equipment, or they could bypass security on the server.

Policies also need to be based on a threat and risk analysis. A threat and risk analysis looks at the risks and the likelihood of occurrence and the cost of mitigating those risks. The cost should be less than the perceived benefit of the measure of protection.

For example, if you determine that there is a risk of having your desktop computer stolen, you're not going to spend money on a fulltime security guard to prevent that. The costs of the guard would outweigh the asset you're protecting. There are other controls that can be implemented that are just as effective, and less costly.

If you're looking for more information on security, the technical security branch of the RCMP (Royal Canadian Mounted Police) has a lot of information on information technology, security and security standards.

Now to look at the importance of IT security in government. It continues to increase. There is increased connectivity. More and more agencies are connecting their computers together over longer distances. For example, over half of the district health boards are connected such that they can e-mail . . . send e-mail to each other. There is increased use of Internet and intranets.

E-commerce. The government is beginning to look at this as a means of making it easier for public to acquire certain goods and services.

External access to networks. As a changing way of business is done, more agencies are allowing their staff to access information electronically while they are away from the office.

More mission critical systems. There is increased reliance by government on IT systems to do their work.

In 1998-1999, government agencies reported that they spent over $250 million on IT. This amount is expected to continue to increase. There are numerous government IT initiatives . . . IT initiatives taking place in government today.

Encryption software. A pilot project has been developed to provide better security over the transmission of electronic information.

High-speed connections. Negotiations have been taking place to provide increased capacity for wide area networks and the Internet for a majority of Saskatchewan communities. With this, departments with offices in smaller communities will be able to provide their employees with better access to their head office systems. As well schools will be able to obtain higher speed Internet connections.

Internet use. More and more agencies are finding the Internet a useful tool to provide information to others and to obtain information from others. For example, every report that our office made public since 1997 is available on our web site. As well, if we need to refer to a report from the office of the Auditor General of Canada, it is available on their web site.

System upgrades. As an example, a few departments have recently implemented new financial systems in order to improve the quality and timing of information they require to manage their business.

And finally, payment gateway. SPMC and Queen's Printer is undergoing a pilot project whereby an individual can obtain publications electronically and pay with a credit card.

Some of the risks of not having adequate IT security are: you may not meet your organizational goals; you may incur financial losses; it may lead you to make poor decisions because of insufficient or inaccurate information. All of the above may lead to the loss of public confidence in systems.

Now they talk about the chapters. Chapter 11 of the 1999 spring report. This chapter provides an update on the status of the government-wide recommendation. In this chapter, we note that there have been several developments regarding IT security in government. An information technology office has been formed — ITO.

One of the roles of the ITO is to coordinate IT policy across government. The Public Service Commission has also developed an IT acceptable use policy which outlines acceptable uses for the government's IT systems including the use of computers, e-mail, and the Internet.

Also several departments are working together with the ITO to develop a template for IT security policies. This is an important step towards a government-wide security policy. However, we still do not have a government-wide security policy and we continue to recommend that the government should establish a government-wide general security policy for its IT systems.

Chapter 18 of the 1999 fall report. This chapter compares the current results with the previous survey. There were 32 government agencies surveyed. They include larger departments, Treasury Board, Crowns, Crown corporations, health districts, and educational institutes. Exhibit 1 of that chapter lists those agencies. We asked that agencies respond to a variety of questions relating to IT security. The results show that IT security has strengthened but more improvement is required. As I mentioned, this chapter is a follow-up of our previous work, but the recommendations made in the previous chapter are still relevant. There has been progress on a number of them.

Normally we ask that you deal with each numbered recommendation. To make it easier, and since the committee has dealt with most of the recommendations, I'll present the five new recommendations and ask that you deal specifically with those. These five new recommendations expand on and clarify our previous recommendations.

Chapter 18 is divided into six key areas: responsibility for security, security policies and procedures, security awareness, protection of IT resources, confidentiality and integrity of IT resources, and availability of IT resources.

Responsibility for security. Senior management commitment to security is critical to the successful implementation of policies. There has been positive improvement in the number of agencies that assign responsibility for IT security independent from operations. Given the significant reliance on information technology in today's world, senior management should be assigned responsibility for IT security. This recognizes it as more of a priority.

There has been no change in the number of agencies reporting that their security administrator is independent from operations. The recommendations that we made in this section were that agencies should assign responsibility for IT security to a senior manager independent of IT operations and the security administrator should report directly to this senior manager.

Security policies and procedures. Written and approved policies ensure management needs for security are documented. There has been only minimal improvement in the area of security policies and procedures. The results show that 81 per cent of agencies report that they have some written policies and procedures. However, only 38 per cent of agencies report that their written policies and procedures are up to date, cover all major risks, cover all applications, and are approved by senior management.

As I mentioned earlier, policies and procedures need to be based on a risk analysis. Only 44 per cent of agencies report that they do this. The information technology office is presently working with agencies to help them put in place adequate written policies and procedures. The recommendations that we

made in this section are: agencies should establish security policies and procedures, and periodically monitor them to ensure they still meet their needs.

There is also a new recommendation in this area. Given that information technology is constantly changing, agencies need to ensure that their policies and procedures are kept up to date and are applicable to any new system they implement. Therefore we recommend that agencies continue to monitor their security policies and procedures and ensure they meet the needs of the agency and meet or exceed minimum standards.

Security awareness. Written policies aren't enough. You need to get the message out. At the time of the surveys, there had been little improvement in the area of security awareness. Normally, the majority of security breaches or incidents originate from within the organization. Employees not aware of the policies or the consequences of their actions account for a large portion of the security breaches.

Generally, security awareness is one of the best uses of money to improve security. For most organizations, it would not take much effort to set up sessions for employees to review the organization's security policies and procedures to make staff more aware. Staff need to be periodically reminded of their responsibilities for security. Recently there has been some improvement in this area. For example, the Department of Finance and the Department of Justice have held extensive security awareness training sessions for their staff.

The recommendations that we made are that agencies should inform their employees of security requirements and have them agree in writing that they will follow these policies.

Another new recommendation is that we found that although access is revoked when employees are no longer at their job, it is not documented. Without the policy being documented, employees may not be aware of what has to be done and who is responsible to ensure it is done. Therefore we recommend that agencies ensure they have written policies and procedures for revoking employee access to information when their employment ends.

There has been slight improvement regarding protection of IT resources. There has been no improvement in the area of physical security. I would have expected this area to show at least some improvement. Physical security is safeguarding your IT assets, including computer software and related equipment, from outside threats, employees, and third parties. Good physical security makes passwords more effective. This survey was a self-assessment and 40 per cent of agencies felt their physical security could be improved. One of the recommendations that we made is that agencies should periodically report to senior management on the effectiveness of their security policies.

And as well, a new recommendation. We recommend that agencies determine their physical security needs and assess the adequacy of their security measures. A timely example of where there has been improvement in this area is the new security requirements for this building.

Another new recommendation. If agencies do not specify security and confidentiality requirements in contracts, they're at risk of the contractor disclosing information. Therefore we recommend that agencies ensure their service contracts include requirements for security and confidentiality.

Confidentiality, integrity, and integrity of IT resources. There needs to be a system to classify information. This will help set good IT security policies by knowing what level of protection is required for each class of information. There has been significant improvement in this area of ensuring the confidentiality and integrity of IT resources. Almost all of the agencies report that they have set password standards for their IT systems.

The recommendations that we made in this section are agencies should ensure their password rules meet an acceptable standard. Agencies should identify their confidential data and define who can access the data, and employees should monitor and control access for their support employees.

And the final section — availability of IT resources. Agencies appear to have good back-up procedures. Recovery procedures have improved but still could use more improvement. Sixty per cent of agencies have some sort of recovery plan, but only 50 per cent are approved by management. And that 60 per cent is at the time of writing that chapter.

The recommendation that we made are the agencies should improve their contingency plans by testing and improving the plans, basing them on a threat and risk analysis, and specifying the acceptable recovery time.

One new recommendation out of this area. The survey results showed that the 32 agencies reported they have over 500 of their systems that are mission critical. Some agencies included e-mail and word processing as mission critical systems. Without a critical analysis of which systems are critical to the success of the agency, inappropriate resources may be used to protect those systems.

Therefore we recommend that agencies specify which systems are critical to the mission of the agency.

Just to summarize. The graphs and the results of the surveys indicate there has been improvement. However, more improvement is required.

And just to summarize the key areas of improvement that's required. Senior management is not always made aware of the risks to their IT systems and data. Without this information it is difficult for them to make the appropriate decisions as to the level of protection required for those systems. Management will need to make the decision whether to accept the risk or mitigate it by implementing more controls.

Secondly, IT security officials need to be independent from operations of the IT systems. IT operation objectives are often in direct conflict with the IT security objectives. Employees need to be made aware of the security policies and procedures that they are required to follow. When an employee does not know his or her responsibilities, IT security suffers.

And finally, only 34 per cent of agencies say they have good

physical security. Physical security needs to be improved.

And I was also going to give an update of the statuses, what the status is today, but I'll leave that for the officials. Thank you.

The Chair: — Thank you, Victor. Are there any questions off . . . right at the moment for the presentation or anything for clarification? Any of the members? None. Officials?

Mr. Spannier: — Just a few comments, Mr. Chair, and committee members. First of all just for your information, Mr. Schwab mentioned a project underway with the Queen's Printer selling publications on-line and so on. I just wanted to advise the members that it's interesting, the first sale was to somebody in Paris, France. The second sale of a publication was to a law firm in Washington, D.C. and both of those were credit card transactions so we feel we have a secure system there.

However, in terms of some of the progress we've made since the fall of 1999, we do have a security charter that we have developed. Departments, agencies, and Crown corporations have in fact signed the security charter. Every department, agency, Crown has someone assigned responsibility for security. The IT office has organized educational events for these departments' representatives. Canada's top IT security company EWA-Canada has been brought in to advise departments on security. We also have brought in the RCMP to do a threat and risk assessment course. We have government-wide standards, as you're aware, but each individual department also has its standards.

We continue to work with the private sector. The Queen's Printer is an example whereby we're working with CUETS (Credit Union Electronic Transaction Services) to develop the payment gateway.

And that's about it. So overall I think, to sum up, I think that we have made some considerable progress since the fall of 1999 with the measures that I've outlined and I think, if need be — I don't know how you want to handle it, Mr. Chair — we could update you on terms of each of the auditor's recommendations. But I leave that up to you, Mr. Chair.

The Chair: — I think the question that is before us right now, as indicated by the auditor's office and the officials, we have a total of 21 recommendations that have come before you — one in chapter 11, and 20 in chapter 18. And as highlighted by Mr. Schwab, 16 of them are, have been dealt with by this committee or by a previous PAC committee in one form or another. And the question that is before you is do you wish to have an update on those 16 recommendations as to their status? Yes or no?

Ms. Lorje: — I don't think it's necessary.

The Chair: — Not necessary. Concurrence there?

Okay then let's move directly into the five new recommendations, and as indicated in your handout they are recommendations 5, 9, 10, 12, and 17 out of chapter 18. If we could turn to chapter 18, the fifth recommendation is on page no. 352, and it's already been read to you by Mr. Schwab. Discussion and questions.

Mr. Gantefoer: — Mr. Chair, a few general questions first because I think these five recommendations strike me as being fairly generic, commonsensical about, you know, in regard to any agency or organization that's using information technology at all.

One of the great risks of this profession is there always seems to be new acronyms or whatever coming into play. What's e-government?

Mr. Hersche: — E-government is essentially electronic government. It's delivery of services electronically, not necessarily as a substitute for face-to-face or other kinds of delivery, but as an adjunct to that and an increase in kind of service level.

Mr. Gantefoer: — Is there a strategic plan or a direction that government is heading through this combined informational technology office or any other place that is looking at moving services of government in one department or another at different levels into this electronic world?

And I heard you mention about the Queen's Printer or you know there's different projects that have been going on department to department. I think Justice is dealing with Land Titles and different things like this. Is there an overall plan to implement an electronic service delivery?

Mr. Hersche: — Yes. We have a strategic plan that we have developed for that. And prior to developing that strategic plan, we had a small pathfinder fund for the last two years, through the ITO (information technology office), developing a number of different projects to see what's best and how best to approach some of the kinds of transactions we want to do in electronic government as a result of that. And essentially what we wanted to do is see the costing and to look at various costing methodologies to see what the cost of electronic government would be in that move towards that.

On the basis of that, we have developed a strategic plan which we have taken before cabinet, and we now have before Treasury Board, essentially looking at . . . It will be their decision on the level of funding that they would like to put towards this, to say how fast we want to go towards e-government and to what degree we want to go towards e-government.

Mr. Gantefoer: — As part of the strategic plan, is there a pulling together of various initiatives by agencies or departments or Crowns to build a comprehensive plan?

And I refer to things like I think it's called CommunityNet, where SaskTel is talking about high-speed Internet in those communities that essentially support high schools. And I don't know if there's other criteria, but those kinds of initiatives, are they being pulled together to say okay, this now has impact on health through the SHIN (Saskatchewan Health Information Network) project? And there are communities that don't meet necessarily the criteria of a high school but have a health facility, so therefore that should be in a CommunityNet. What I'm getting at, is there some pulling together of various initiatives as part of this strategic plan?

Mr. Hersche: — And that's precisely what the ITO and our

function is.

For example, we are the lead with CommunityNet. What we have done with CommunityNet was we brought in our partners, the Department of Health, Department of Post-Secondary Education, K to 12, essentially who have gone to each of their — and CommunityNet is an example — of gone to every school division, gone to every health care district to look at their specific needs, what kinds of things are out there. So we have pulled that together.

CommunityNet is really the base. What we're building on in terms of the plan with the base is saying now that we can deliver high-speed Internet, we are dealing with those departments and other departments through the Systems Management Council to see what kinds of services we want to deliver to those communities or other kinds of government services.

As I mentioned in our previous session, as part of that we're also bringing together where the kinds of overlaps would be. Essentially, as an example, Larry mentioned the payment gateway. All we need to do in terms of establishing a payment gateway is we establish it once for government; we don't need every department to establish one of those. It decreases the cost and making sure that we have the higher standard of security in that respect, that we can do this kind of payment gateway through . . . we mentioned the Queen's Printer, but for hunting licences, for other kinds of services that are out there.

We're also, through our information, we have a steering committee of deputy ministers for information technology. And through that, that committee in bringing together the deputies, we make sure that all of the departments are . . . not only buy in to what we are doing, but are able to pool their kinds of priorities and see where we can make sure that we can eliminate any kind of overlap and create some synergies.

So we have a number of items that are going down the pipe in that way.

Mr. Gantefoer: — And I'm sure that, you know, the very obvious things like e-mail and things of that nature are just so obvious. Are there issues surrounding the storage and maintenance of essential data basis and things of this nature as part of this as well?

Mr. Hersche: — Yes they are, and as Mr. Spannier talked about we are doing those kinds of security projects across government. In addition, we have hired an information management specialist in the ITO to continue that kind of focus. Tim has been focusing on broader security, and this individual will be focusing more and more on the kinds of data standards that we need to cross government.

Mr. Gantefoer: — Will it also, like, tie in, and I think particularly in SHIN where you are talking about legislative requirements under privacy and confidentiality of individual records, and at the same time, where there is appropriate accessibility so issues of over-prescribing and multi-doctoring, shopping, if you like, to abuse the system, can also be dealt with. And I know it's always a balance between protecting privacy issues and also then having the tools to safeguard against system abuses. Does this office, informational technology office, work then with SHIN or how does the relationship work in establishing those system . . .

Mr. Hersche: — Extensively with SHIN and the Department of Health in putting this together as an example, the security needs under the health information privacy Act, or HIPA (The Health Information Protection Act), was a very great consideration when we were putting together CommunityNet. What kinds of needs do they require for . . . precisely for those privacy concerns that we have?

The differential between agencies, of course, is quite broad. I mean, personally in my office, I'm trying to give away as much information as I can and I want as many people to have all of that kind of information so my security requirements are slightly different than for example the Department of Health and personal health information. So security levels again will be quite different in different agencies depending on the kinds of information that they have and where they want to distribute them.

Mr. Gantefoer: — So work on . . . or is there sharing of information between the legislature per se in terms of looking how it might be more appropriate for members of the Assembly, at least the non-Luddite members of the Assembly, to access information electronically in a meaningful way.

Mr. Hersche: — I'm not quite sure how to answer that, I'll be honest.

Mr. Whelan: — How many non-Luddite members do we have?

Mr. Gantefoer: — We're not sure. We're trying to gather up their abacuses.

Mr. Whelan: — I was going to comment on what you said about storing databases and archiving databases, and the issue of archiving and storing electronic files is a really problematic issue. Up until recently, the standard for storing anything was, it was in paper. And you don't need any technology to be able to read a book. So archives everywhere are having . . . national archives . . . are having the issue of what format do I store electronic data in so that somebody can read it a hundred years from now.

If you just think for those recent computers the way the storage medium has evolved every two years there's something different. And it's a really big problem. They don't know how really to deal with that.

Another issue is that some kinds of electronic data changes so often if you decide that you want to archive web pages so there's a historical record of the Department of Health's web site. And it changes every day because some part of it has changed. Which version of it do you store? Or do you store 365 versions every year? These issues have not be adequately addressed.

As Bob has mentioned we have hired an expert information management has been with our office a couple of years . . . a couple of months at this point. There's also a national

committee on the subject which our boss Lynn Oliver, the CIO, (chief information officer) is the Chair of, because these issues have to be addressed nationally because every jurisdiction's facing these problems. And we're working with archives and librarians and those kinds of things across the country.

Thank you, Mr. Chair.

Mr. Wakefield: — Thank you, Mr. Chair. One of the purposes, of course, for all this IT information and the security of it is for access by people in the province. Is there an inventory as to the level of acceptance of, or the use of, this kind of technology by Saskatchewan people? And how does that compare to other provinces?

Mr. Hersche: — In Saskatchewan we have something on the order of about 50 per cent of our households have Internet either in their home or have access to the Internet through either a library or through some other community access kind of point.

We're not the leading-edge province in that. Alberta is leading us by about another 5 percentile, if I remember correctly. The lowest usage is in Quebec and that is probably a language problem versus a technology problem.

We've also done a number of surveys with the University of Regina, HRDC (Human Resources Development Canada) on acceptability and the need for electronic government or electronic services. In the most recent survey, which was in 1999, it was, and I may have my percentages off a couple of points here, but no surprise something on the order of 80 per cent of those people with Internet in their home expected to receive or be able to use government services in their day-to-day life.

But what was surprising to us was that in excess of 60 per cent of those people who did not have the Internet expected in the future that they should receive their services electronically and be able to do that.

It's also in many instances, one of the reasons we're looking at . . . (inaudible) . . . and driving some of the high-speed Internet out to more communities is that accessibility issue for those people who live in communities which may not have easy access to a government office or may not have easy access to other facilities that they can get, at the very minimum, that they could get the form that they need in their home so they don't have to drive into wherever the local government office is and get that form and fill out that form and then — you know, at home — bring it back and those kinds of things.

Essentially what we're looking at in all of those, and that may be an answer to some of the earlier questions in terms of e-government, is really . . . we're trying to look at a citizen service kind of format of the seven days a week, twenty-four hours a day kinds of service levels.

And the most recent workings that we've done in terms of recreating the web site that we have for the Government of Saskatchewan . . . The Government of Saskatchewan web site is no longer structured in a manner that is looking at how government is structured. It's more looking at helping people in terms of the areas that they may be interested in. Again a citizen service model as opposed to saying, gee, I really know that vital statistics is in Department of Health versus a different department.

They don't need to know that kind of . . . the citizen doesn't need to know that kind of information. We have a very powerful search engine on there that will direct them to the appropriate agency and direct them to the appropriate person to do that.

Mr. Wakefield: — I guess that was certainly leading to what I was getting at with my question. I anticipate that the usage of e-government and services by that method is going to be on the increase. Everything points to that direction.

So is there an urgency to make sure that all the security is in place? And, you know, we've talked about what has been done, what is recommended, the kinds of things that you've done to comply. What kind of urgency do you see needing to move this along?

Mr. Whelan: — I think Victor has pointed out that the process of doing security . . . One of the problems that I have in my job in promoting this initiative across government is that's it's a pretty boring subject. And it's a bit like getting inoculated and getting people excited about getting their inoculations.

So that notwithstanding, Victor points out that in order to figure out what kind of level of security you have, you have to analyze the system and see what's the chance of somebody breaking into it — what's our exposure here? — and then you build your . . . So you do that analysis, then you build your security response to that.

I think the answer to your question is that security be done at this point on a case-by-case basis. If, for example, a particular department was about to put a system on line — and there are some examples that's currently going on — they would look at the kind of information that's captured in that system, analyze the potential problem of it going astray or of someone getting into that, and then build the system, put those kinds of safeguards in place before it goes on line.

At this point we haven't put a lot of systems on line that involve confidential information simply because the awareness and expertise is just beginning to grow within the government on some of these issues.

Mr. Hersche: — In addition, I should say we mentioned earlier Health as an example. Health and SHIN I know have seen security as a high priority, as HIPA has asked them to do, and they have some very secure systems in place. And they are in place now to look at who can access this kind . . . the kind of information they have. And as this rolls out to other doctors' offices, pharmacies, etc., they have some very good secure systems that they have put in place for that.

Mr. Wakefield: — Mr. Chair, one more if I could.

The Chair: — Okay. We have two other speakers so we'll shorten you down.

Mr. Wakefield: — Just to follow quickly then. The security

standards that you're putting in place, I assume there's some kind of standards that are being developed nationwide actually. We're not going off in a different direction here, are we?

Mr. Hersche: — No. We are trying, and not only in the technology but in the standards, we are trying as much as possible to do international standards. Because we have to as we begin to do this, we've talked about . . . Again, I'll go back to Health and the Saskatchewan Health Information Network. As you know that there's lots of conversations about a Canadian health information network. All those kinds of things have to be able to interface over time.

And everyone . . . as the presentation, it is the weakest link. And so everyone has to have faith that you're using those kinds of international standards. And that's why as Larry had suggested, we are using some of the top agencies — the EWA (Electronics Warfare Associates, Inc.) and the RCMP — of threat risk assessment, those kinds of standards. Again, they're national standards. We don't want to be unique in that way.

Ms. Lorje: — Mr. Gantefoer's questions and Mr. Wakefield's questions I think touch on the peculiar dilemma that we have in terms of individual rights and responsibilities versus collective rights and responsibilities. And then we have also overlaid on that the Canadian dilemma of the nature of this confederation and whether or not the provincial laws dovetail with the federal laws, and so forth.

So I think this is an important area. And the example that Mr. Gantefoer used about prescription drug medication is a very compelling and topical example right now.

I would like to know what the responsibility or the mandate of the federal Privacy Commissioner is, and how that might affect what we're doing here in Saskatchewan. And whether or not in areas other than clearly Aboriginal areas — which is an example that has been in the popular media in the last week or so — whether rulings from the office of the federal Privacy Commissioner could affect work that is being done by the ITO in Saskatchewan.

Mr. Hersche: — Okay. The new Privacy Act, C-6, at the present time the federal does not cover those items within provincial jurisdiction — i.e., does not cover health, does not cover those kinds of things. But it has a provision in it that does state that if we do not have comparable — comparable in terms of levels of standards — legislation or policies in place, that C-6 will apply to those areas.

Ms. Lorje: — So they're going to be wagging our dog?

Mr. Hersche: — That is why we have not necessarily at this point . . . I shouldn't say we. My understanding is the Department of Justice has not quite decided at this point where they will come from to that, and whether they will take and challenge C-6. The province of Alberta is also thinking of challenging C-6.

Now in another case, because you used the health example, because we have HIPA, my understanding is that that is of a sufficient level if you will of security, that the federal government or the federal Privacy Commission would not take that . . . would not have any authority in that area because we do have legislation in that area.

Ms. Lorje: — So therefore the federal Privacy Commissioner could not issue an edict that would have the effect of nullifying all the work that we're proposing to do with SHIN?

Mr. Hersche: — No.

Ms. Lorje: — And so . . . and in other areas that I can't even imagine, at this point we are anticipating the problems and we're developing the approach and the legislative solutions.

Mr. Hersche: — We are looking at it with the Department of Justice. There are some areas in business . . . there are some areas that we have, we do believe that there would be some problems or potential problems in very, very small businesses or very small organizations.

As an example, theoretically the women's bingo consortium in Swift Current or whomever, may not be handling their information about who does what and who buys what in a specific way. We don't believe necessarily that we want the federal Privacy Commissioner in that, you know, to go down to those kinds of levels and to interfere in those areas.

So we are working, the ITO and other agencies are working with the Department of Justice to put together a position and we are working on those areas.

Ms. Lorje: — It might be helpful in future reports — either from your office or from the Provincial Auditor — to have some comments about what is happening in terms of federal initiatives and how we are either responding to them or have gone past them, because clearly we're not an island in this. And I think that those kinds of national implications are important to draw to the attention of the legislators.

Ms. Jones: — Thank you. Are we kind of bouncing around throughout this or are we still on no. 5?

The Chair: — I would suspect that no, we're not totally on no. 5. I think we're all over.

Mr. Wakefield: — You're referring to my question?

The Chair: — General comments before we get into the specifics of the resolution, because there is no resolution before you.

Ms. Jones: — Okay. Well in general, I'd like a little further clarification and explanation of the use of the term physical security. And I believe that I heard, when we were listening to the slide presentation for instance, this building. I think I heard that. And again that's something that's somewhat out of the purview of this committee.

Reading through page 355 and see recommendations dealing with service contracts, I'm not too sure exactly what that means. Are we talking security companies? Are we talking locks on doors? So if anyone has any enlightenment for me I'd appreciate having it, because physical security seems to me to be something other than accessing a security block to accessing

computer programs.

So if anyone has a little enlightenment . . .

The Chair: — I think we could ask Mr. Schwab or Mr. Whelan to comment on those.

Mr. Schwab: — Okay I can start. Just to give a comparison of physical security. Another type of security is logical security whereas the system doesn't allow you to look at any information until you enter a password. Physical security are things like locking the doors so that nobody can access the computers, that type of thing.

As I mentioned with this building, they're stepping up security even just getting into the building. That has an effect on the security over the information technology systems because there's less people being able to access or get near those computers.

Ms. Jones: — But if I can follow through on that line . . . and we're talking about agencies. I assume we're also talking about Crown corporations, we're talking about hospital wards, we're talking about pharmacists, the possibility of a pharmacist system tracking prescription drugs. It seems to me an enormous mandate for this committee to receive information and make recommendations, or for the auditor to make recommendations on all of the possible physical security that might be necessary if we were to pass . . . you know, when you talk about agencies. Unless there's something more simple than I'm envisioning, I find this to be quite an onerous task.

Mr. Schwab: — For the recommendation on physical security, the recommendation is relating to physical security over the IT equipment, not necessarily physical security in general.

Ms. Jones: — But there's no difference if you're talking about SHIN. I mean, you're talking about hospitals and everywhere, like physical security of that system. If the information on the system is somehow a public information system, but it's in a facility such as a hospital, I mean, that makes it a lot more difficult to envision what we're going to do about the physical security in the hospital.

Mr. Whelan: — If I may?

Ms. Jones: — Please do.

Mr. Whelan: — As Larry has suggested we have developed an outline, a template of a security policy on all the government organizations and the Crown corporations that are participating. And even the city of Regina is sort of voluntarily auditing the process because they heard it was going on.

It's an outline of what should be in a security policy and it has a section on physical security. Asks questions like what are your process for challenging visitors? Do people have to wear tags? Do they have to have key access? And in essence, it tries to be comprehensive.

And it goes back to what Victor was talking about, about the idea of analysing your risks. Where are your weak spots? Where are the places where people can either come in physically and make mischief with your systems by trashing a filing cabinet or get in electronically and destroying a database? Figuring out where those holes are, analysing the likelihood of that happening, and then building your security appropriately. You don't want to . . . as Victor was pointing out, you don't want to have to have the server where all your critical information is in a room and it's got a . . . it's possible for anybody to hack into it electronically. But when you walk into the building, there's no locks on the door and there's a sticky note on the monitor that's got the password to get into the system — that would give you a false sense of security in that case.

Ms. Jones: — So would you be more interested in the physical security of the server as opposed to the user then?

Mr. Whelan: — Yes. Well, it gets pretty complicated . . .

Ms. Jones: — Yes, it does.

Mr. Whelan: — . . . as you pointed out.

Ms. Jones: — And I'm one of those Luddites so.

Mr. Whelan: — No. And these are difficult issues for people to deal with, because we're moving into a realm where people understand about locked doors and those kinds of things. We're dealing with a place where someone doesn't have to be on the same continent and they can still, conceivably, get at the important information that, you know, information that's important to citizens of Saskatchewan that we don't want . . . that we have a custodian responsibility for.

But the security . . . (inaudible) . . . we put in place commits deputy ministers like Larry and his counterparts to put the resources to it to get the job done, and we're sort of all coming along together on that process.

Mr. Hersche: — If I may add just one other thing to that. I think one thing you were identifying is the variety and, you know, that we . . . so much, so different in every circumstances. That's why what we're doing in many instances is developing the template. And the organization itself, in many instances, has to look at their specific requirements, and their specific requirements will vary slightly within these principles. But their specific requirements will be different, as you mentioned, whether they're in a hospital, whether they're in our offices, in our government offices or someplace . . . or in the Legislative Building.

Each one of those will have . . . all we can outline for them is these are the potentials and these are the things that you should look at. They're going to have to look at their own specific instances, or specific requirements, to say that's the door I need to make sure is locked. That's the, you know, I . . . the kinds of security I need per . . . for each individual that works in this office. Those kinds of things.

And so you're quite right in it's a very generalized kind of thing. That when we're talking about it as a principle up here; then we get down to applying to each individual organization, it becomes quite different.

The Chair: — Okay, thank you.

Mr. Kwiatkowski: — I think my question is perhaps best addressed to the Provincial Auditor's office but we're talking about information technology security right across government. And inherent in that very fact — whenever you talk about developing security systems — you're also providing the tools, the mechanisms, the systems that could conceivably in turn be used to compromise the security of others.

Are there any concerns around that? Have you looked at any of that, and are there any assurances that, I guess, the technologies, the skills, and what have you that will be brought to bear in terms of putting security around government systems not be used to compromise the security of others?

Mr. Schwab: — I'm not sure I've answered that. But I don't . . . I don't think there is a risk there. What we need to do is make sure that the individuals in the organizations have the proper knowledge and skills and abilities to be able to access the risks and the threats that surround their IT systems. And from there, then they develop the adequate policies and procedures. I'm not sure if . . . I don't think there would be a concern that that will be used against them.

Mr. Hersche: — Pardon me, and I'm just, I . . . if I'm interpreting your question correctly, in terms of developing the kinds of services and the databases that we are developing and in terms of access, we have adopted in the Government of Saskatchewan and all through all the departments the Canadian consumers' association standards for how we use data. And that we do use data in a manner which is — so if I word this properly — in a manner in which it was intended to be used for.

So if you . . . as an example, the federal Privacy Act is based on these same kinds of standards. The Health Information Privacy Act is based on those same kinds of standards as well. And some of the security kinds of operations that we're looking at are based on those standards so that we don't begin to use that . . . I think what you're saying is that we don't begin to use that information in an inappropriate manner for matters which it was not intended to be used for when the individual gave that information or provided that.

Is that an answer to . . . again, I'm trying to read your question.

Mr. Kwiatkowski: — Well thank you, it's close. I guess, you know when you think about it, a country's offensive technology, it's a lot similar — or defensive technology — it's a lot similar to the technology that they use in an offensive kind of way. And I guess, the fear maybe that something . . . (inaudible) . . . gets large enough that it can be used in almost some sort of an Orwellian type of fashion and that was just . . .

Mr. Hersche: — That's precisely why we have adopted those kinds of standards of data usage. Some of the kinds of information that we are trying to — and this goes back to some earlier discussions that we had of where we're looking at duplication — for example, name and address. We have a million people in Saskatchewan. How many data bases do we need for the names and addresses of those people?

So we may look at creating, for example, a central data base of names and addresses that other departments can begin to use in their specific usages. But that's quite different than creating a central data base that Bob Hersche could look at in terms of health. Bob Hersche has no purpose in looking at specific health information. That's not part of my job; that's not part of my security kinds of things.

And we are setting up those kinds of access standards of what kinds of information precisely so we do not get into the HRDC thing that you probably read about with the federal government in creating this massive kind of data base. There will be connectivity, there will be linkages, but in doing that linkage we have to . . . we will have our data classified in terms of that kind of access as who has access to it.

Mr. Yates: — Yes, one question is for the Provincial Auditor, the officials. In the areas of electronic commerce and electronic information transfer and storage, I'm aware of national standards being set by the governments of Canada and the provinces in co-operation.

Is it fair to say then that Saskatchewan will either meet or exceed those national standards as they're being developed for Canada, including the issues of electronic storage, signatures, evidence — all the various areas of concern regarding security of information usage — in our ever, I guess, developing world of electronic information and usage?

Mr. Whelan: — Yes, I participated in a national committee on information technology security and there is a complete recognition amongst us that we're all in this thing together. And that it doesn't make sense, as another member said, to build a standard in one jurisdiction that's incompatible with another. And we're taking measures on a variety of fronts to make sure that doesn't happen.

One that is currently going on right now is on information classification. The idea being that you take your files, whether or not it might be how many fishing licences the Government of Saskatchewan sold in a year, and you decide well anybody can know that. So that's public information.

And then there are levels above that that are not for public consumption, and then there are very confidential levels. For example, information within the Department of Justice about the prosecution of a case which would be a very high level.

And if you have these kinds of standards and everybody agrees on the levels across the country, then when it is appropriate for data to be exchanged between jurisdictions, everybody is on the same page and are treating the data with the same kind of respect and care that is required. And that's a national effort that's going on and we should have results by the middle of next year. Currently only three jurisdictions in the country have any kind of data classification standards.

And it's interesting. It came along in a very timely way because for the security template that we're developing we require data standards, and it turns out every other country, every other jurisdiction in the country has realized exactly the same thing and it's happening at the same time.

Mr. Hersche: — . . . answer some of your questions as well in

terms of where Saskatchewan is on that. Our CIO is the lead on that national committee so she is the Chair of that, so we are . . .

Mr. Whelan: — That's the short answer.

Mr. Hersche: — Yes, sorry.

The Vice-Chair: — Any questions, Mr. Yates? No.

Mr. Wakefield: — Would you care to move the recommendations one by one?

The Vice-Chair: — Yes, we'll move them one by one.

Mr. Wakefield: — I would be prepared to recommend that we concur with new proposal no. 5.

The Vice-Chair: — On page 352. What's the committee's wish?

Mr. Gantefoer: — Concur and note progress.

The Vice-Chair: — The motion is to concur and note progress. All in favour? Thank you.

The Chair: — Let's move to recommendation no. 9 which is found on page 354. Moved by Mr. Kwiatkowski. We concur and note progress. Any discussion?

Mr. Wartman: — I'm just curious whether those are going to be written on paper or electronically?

Mr. Whelan: — Actually the plan is . . . electronically. Are they going to be web pages? That's the current plan.

Mr. Wartman: — Because if we're looking at the policies only being electronic, then you get into those issues that were raised earlier on storage of and changed ways of reading and understanding the information.

Mr. Whelan: — That's true. The advantages of having them as web pages is that if you've got a section that refers to another section, you click and you link to the other section. You can refer to external documents that may be important. You can easily post them on a web site for your staff to see them, and only have one copy you have to worry about because it will evolve over time and you'll know that's a master copy and there aren't generations of copies floating around.

Mr. Yates: — And you can produce a hard copy?

Mr. Whelan: — And you can produce a hard copy by hitting the print key.

The Chair: — Thank you. Any further questions, comments? All those in favour? Carried.

Recommendation no. 10 on page 355, and this was . . . We had some comments and questions about physical security and again recommending to the agencies. Any discussion?

Ms. Lorje: — Yes, I'm wondering if, just for the sake of clarification, we need to make sure that we're talking about the physical security needs with respect to IT . . . (inaudible interjection) . . . I know it is.

Mr. Schwab: — This chapter specifically relates to IT security, physical IT security.

Mr. Gantefoer: — When we make our report, it's under the chapter on information technology so that references it automatically.

Ms. Lorje: — Okay.

The Chair: — Any further comments? Committee's wish?

Mr. Gantefoer: — Concur and note progress.

The Chair: — Concur and note progress. Motion, Mr. Gantefoer?

Mr. Gantefoer: — We don't need motions if we agree.

The Chair: — Okay. Any discussion? All in favour? Okay, duly noted.

No. 12 — recommend agencies ensure their service contracts include requirements for security and confidentiality. Bullet no. 1 . . . (inaudible interjection) . . . I know. I need all the help I can get.

Any questions, comments? Concur and note progress. Question before you. All those in favour? Agreed.

And the final recommendation is recommendation no. 17 on page 358 — identification of critical systems. Any further comments? Questions of officials or the auditor? Do we concur and note progress? All those in favour? Carried.

That takes care of the five new recommendations, and it was agreed that the others have been dealt with in one form or another. Any further discussions on chapters 11 and 18, under information technology securities?

I want to thank the officials for being here today and dealing with the two issues that we've had before us relatively quickly. Thank you very much.

Well in light of the fact that our agenda has indicated that we'll be starting tomorrow morning at 9 a.m. but that we're now at just shortly after 4, we will require a motion that we adjourn since it is not according to the agreed agenda that we had before us.

Mr. Yates: — I move we adjourn.

Ms. Lorje: — I think we should have the Chair sit here until 5 and the rest of us can leave.

Ms. Jones: — Are there any smaller items that we could just quickly dispense with ahead of time or do we need officials for everything?

The Chair: — Well, there is one section that we've talked about already and that's the Board of Internal Economy which

we did not, we will not, we have not scheduled any officials . . . (inaudible interjection) . . . You have someone here for that?

Mr. Wendel's indicating that he has someone here for the first item right now that was scheduled for tomorrow morning — the Standing Committee on Public Accounts. Do you want to deal with that one now? No.

Well, could I ask you this so we can plan tomorrow's agendas maybe a little more precisely. Do you expect that the three items that we have for the morning, that we'll deal with them in such a fashion that we would require the officials that are scheduled for 1:30 to be here prior to the noon hour?

Mr. Gantefoer: — What officials do we have for 1:30 in there from the auditor's office?

Mr. Wendel: — I just want to make sure I have those people here; they're different people. It'll be different people.

Mr. Gantefoer: — There's nobody else other than the auditor's office going to be here?

The Chair: — For which section, Mr. Gantefoer?

Mr. Gantefoer: — For the 2000 fall report. There's no department officials, or . . .

The Chair: — Is there? There will be department officials, Mr. Paton is indicating? So do you want those officials to be sort of on a standby for 11:00 a.m. if the three items that you have before you . . . if you feel you're going to deal with them in a fairly . . .

Mr. Gantefoer: — Can we move up the 3:30 item to early if that's . . . if we have the time. Because the 3:30 item is more of an internal discussion, is it not? With some recommendation perhaps from the auditor's office.

The Chair: — That's without . . . yes that's without officials.

Mr. Gantefoer: — There'll be officials there, so if we're moving forward in the morning we can move the 3:30 item up to 11 o'clock or something.

The Chair: — The other question would be, Mr. Paton, is whether or not officials like Mr. Boothe and others . . . will they be available before noon tomorrow?

Mr. Gantefoer: — Why move them around if we can just move some agenda item up.

Mr. Paton: — Mr. Chairman, I would anticipate that leaving it at 1:30 for Mr. Boothe would be preferable.

The Chair: — Okay. So we'll leave the agenda as is, and if we finish our three items that are proposed for the morning agenda sooner, then as Mr. Gantefoer has indicated, we can maybe move the last item since it's an internal matter and we don't need officials for that.

I would now entertain the resolution for adjournment, Mr. Yates, as you moved. All in favour? Carried.

The committee adjourned at 4:09 p.m.