Standing Committee on Public Accounts

Hansard Verbatim Report

No. 20 – November 2, 2001

Legislative Assembly of Saskatchewan

Twenty-fourth Legislature

STANDING COMMITTEE ON PUBLIC ACCOUNTS
2001

Ken Krawetz, Chair
Canora-Pelly

Ron Harper
Regina Northeast, Vice-Chair

Rod Gantefoer
Melfort-Tisdale

Debbie Higgins
Moose Jaw Wakamow

Carolyn Jones
Saskatoon Meewasin

Judy Junor
Saskatoon Eastview

Carl Kwiatkowski
Carrot River Valley

Lyle Stewart
Thunder Creek

Milton Wakefield
Lloydminster

Mark Wartman
Regina Qu’Appelle Valley

Published under the authority of The Honourable P. Myron Kowalsky, Speaker

Public Hearing: Saskatchewan Property Management Corporation

The Chair: — Good morning, everybody. Okay, we're set to go this morning with an agenda that should take us near noon. First up this morning we have SPMC, Saskatchewan Property Management Corporation. And Fred, a couple of new people I guess. I'd ask you to introduce your officials from the auditor's office.

Mr. Wendel: — Good morning. With me today I have Rodd Jersak who attends all our meetings, Phil Creaser who leads our work in our computer audits and security audits, and Victor Schwab who also works in our computer audits and Victor . . .

The Chair: — Good morning, Fred and welcome to all of your officials. And welcome to officials from SPMC, and Mr. Law I'd ask you to introduce all of your officials as well.

Mr. Law: — Thank you, Mr. Chair. From SPMC, in addition to myself, sitting at my right is Phil Lambert who looks after from SPMC's perspective, directly the GEMS (government electronic mail system), the electronic e-mail system and is responsible for our telecom services.

On my left from the ITO (information technology office) office at Economic Development is Lynn Oliver. And in the back, from Lynn's shop also, sitting on the left is Tim Whelan. And also from SPMC I have Al Moffat, our vice-president of commercial services. That's the area in which Phil does his work. And also John Dumalski who is with our finance area. Thank you.

The Chair: — Thank you to you, John, and to all of your people.

We'll ask Phil to do a presentation first and then I understand that there'll be a presentation from SPMC which will require a little bit of a media change, so we'll have a small little interruption while we switch some computers. So go ahead, Phil.

Mr. Creaser: — Well thank you, Mr. Chair, members, officials. I'd like to thank you for the opportunity to talk to you about our chapter on the electronic mail system of the government.

If you'd like to follow along, I've got a set . . . we've handed out a set of slides for you to look at. I guess at the start I'd like to thank the officials at SPMC for their co-operation in our audit and in particular Al Moffat and Phil Lambert who are here today and Darcy Hislop who is directly responsible for managing the e-mail system in government.

We'll see how technically challenged I am here today. This is chapter 9 of our Fall Report Volume 3, page numbers. My presentation will cover a little bit about why we did the audit, a short overview of the e-mail system, our work, our objective with the work that we're doing, and the recommendations that follow that work.

I think that, why do we do this work? Well in our office we're fairly concerned with the . . . as government is moving more and more to the use of technology to do their work and the movement to electronic service delivery, we were . . . and need to evaluate the electronic infrastructure of government, we've been making those priorities in our work to try to make sure that we feel that they're safe, secure, and well managed.

With the mail system in particular, it's becoming a very important part of everybody's work. And I don't think anyone around this room would deny the fact that it would be pretty tough for them to live without the mail system any more. When we were doing the work, we found that the number of mail transactions had risen from something like 16,000 in the three years before to almost 750,000 transactions per month is the statistics we're seeing. So it's getting to be fairly large and an important part of government.

What is the mail system? Well we looked . . . we tried to describe it in our chapters as kind of on a parallel with the Canada Post, except it's maybe a bit more efficient, a little faster.

But the idea is that the mail system, it's a way of people communicating with each other. The mail system is designed to pass messages from one person in government or outside of government to another person.

I don't know if this slide turns out very well on your system but . . . on your slides, but I know my eyes are starting to go.

But what we found with the . . . To get an idea of where we're coming from with this, the government is the big box, the GEMS system sits within the small box. So I think the technical term is a store-and-forward system.

What happens with the mail system in Saskatchewan is if you're in organization A, you send a e-mail message to organization B; you initiate the message on your computer, it goes through your own system in your own office. It goes over to SPMC servers. They pick up the address just like the postal clerk picks up your postal code, finds out where it's supposed to go and ships it on down the line.

So when we were looking at this system we decided to concentrate our efforts on the work that SPMC was doing. So it looks like this centre box here.

So our objective was to ensure that SPMC had adequate controls over the operation of GEMS. They're part of the GEMS system. And we looked at it at September of last year.

At this point in time we haven't done any follow-up work to see if any of our recommendations have been . . . the status of the recommendations, but I'm sure we'll hear more about that in a minute.

We had six objectives when we did this audit. The first, we felt it was important that SPMC had measurable, quantifiable objectives and targets for the mail system, and they could work with other government agencies to ensure that it was meeting everybody's needs and they could measure their success better with that in place.

We also wanted to look to see if they had adequate policies and procedures to protect the security and integrity of the mail system.

We wanted to make sure there was adequate physical controls over the servers and the files that are sitting at SPMC. And it includes this . . . As I didn't mention before, they have their large address book there that includes everyone's e-mail address, so it's very important for everyone to know that that particular file is there because we all use it every day in our lives.

Logical controls are just the controls over password access to the mail system itself. And we wanted to make sure that those controls were strong.

We also wanted to make sure the mail system was up and running at all times. We had to plan if the mail system did go down for any reason, how they were going to get it back up and running or what would happen in the event of a disaster.

And finally we wanted to look at, is there controls to ensure that mail that's in transit, when it's moving from organization A to organization B, how is it adequately protected in case somebody intercepts that message?

We found that the controls over the GEMS system were adequate, but we did make three recommendations. And we also, as a result of our work, we actually made a fourth recommendation that was, that we felt was important, that came about as a result of our work.

Our first recommendation, we felt that SPMC should set specific performance measures for GEMS and report on whether it met those objectives. They should communicate those objectives and the performance measures to all GEMS users.

It's just part of the, our ongoing work in performance reporting and trying to encourage government organizations to set standards or set performance targets, communicate them, and let everybody know what they are. And I think it helps people understand what standards should be met, and measure if you are successful.

The second recommendation we made is that we felt that SPMC needed adequate policies and procedures to address the risks around the mail system, ensuring that all mail transactions are safe and secure and . . . We all hear about the virus issues that are out there and making sure that we've protected ourselves in those ways, but adequate policies.

Their reply to us on that work was that a lot of it is out of their hands; it's the government. Because every individual organization runs their own mail server and they look after their own mail, it's up to them to have adequate virus protection and adequate security on there.

So we suggested that they work together with the rest of the government organizations to see if there was standard policies that should be established to, and could be enforced, to make sure that people are confident that the mail system is secure and will reduce the risk of virus.

As aside, I think we were one of the first organizations in Canada to pick up the I-love-you virus and it was at SPMC very early whatever that morning was. So I mean they should be commended for that.

The third recommendation was around disaster recovery. We felt that SPMC should do a threat and risk analysis. From the positive side, they do do adequate backups of their systems, minor risks of downtime and that, that they would be protected. They'd be able to get their mail system up fairly quickly. But there were other risks that we felt they should measure and try to determine if they could get up if there was a major disaster, a major system failure or a fire.

The final recommendation was, as we were going through this we were looking at the flow of the e-mail from organization A to organization B, and we kept coming back to how they adequately safeguard these messages and are they complying with The Archives Act. And our work . . . As we talked to a number of organizations in government and asked them how they were archiving their e-mails and do they think they were complying with The Archives Act, and they all felt that they were adequately archiving their e-mail messages, but they weren't sure if they were in compliance with The Archives Act or what exactly they should be doing to be in compliance with The Archives Act.

And so we decided that we would make a recommendation that some work be done to determine what kind of messages should be archived, how they should be archived, and it's a complicated area and we appreciate that. And we just wanted to make it available to people to know that that is something that should be worked on and I believe they've been doing some work on that.

That's the end of my presentation. As I said, we haven't followed up yet on these recommendations. It's only been a year. We look forward to your comments or questions and also the comments from SPMC. Thank you very much.

The Chair: — Good. Thanks, Phil. And again we'll take a couple of minutes now for a presentation from SPMC, if you'd like to get set up.

Mr. Law: — Thank you. Mr. Chair, what we've done for the committee is that we have put together a very brief overview that we thought might help provide some context for the issues that have been raised by the Provincial Auditor's office. Our attempt in providing what will be a four-slide presentation here is to provide you with a little bit of an overview about what GEMS is.

This system was established by SPMC in 1993. It actually became operational in about 1995. Since it was started we've been responsible for funding the system for government as a whole. And when we started out I just wanted to make reference to the fact that at that time there were no policies or procedures or anything regarding how e-mail would be handled. So it's a relatively new environment in which we are providing a support service for government.

On this first slide, what we've attempted to do is to show you a little bit about . . . This is not far off from what Phil showed you in his slide. It’s a little bit of a different representation. The GEMS environment is shown in the middle and what we’ve got out there are some of the various users who are connected up through the government e-mail system.

There are 89 post offices, if you will, that are located around government. So for each government department . . . There would be a post office for the health districts. They would be represented by a single post office in this case. And very much along the lines of the analogy that Phil was using, we would take that mail and have it distributed through each one of those post offices and they in turn would look after having that communication forwarded on through their respective organizations.

So this just shows you some of the users. If you look at the specific references, there are a number of government departments. We also have on the list SAHO (Saskatchewan Association of Health Organizations) representing the health organizations as well as a number of the other users who are there.

This slide again, following up on what Phil talks about, makes reference to the growth that’s taken place in the number of e-mail messages that have taken place between the users on the system. As you can see the growth is really exponential.

In some respects it’s important to point out that in addition to the number of e-mail messages, what is not represented on this particular graph is the complexity of the information that is being transmitted. Back in 1995 when we started, the e-mail messages were relatively simply documents that for the most part could have been, you know, looked upon as being sort of single-page letters that you would send in the mail. What we have now is that most often people are sending documents with attachments that in some ways can be characterized in our analogy to parcels, you know, they’re much more involved, much more complicated information that is going across the system.

So in addition to what we’re showing there in terms of the growth on GEMS we also have a much more complex set of information that is travelling across the system.

On this third slide what we’ve done is we’ve simply tried to give you some indication of the number of GEMS users and how that has been growing since the system was implemented. This now includes in our current environment some 8,500 health district users as well as the ongoing core of government departments and agencies. We’ve approximately tripled the number of users since 1995 who are currently operating on the system.

Phil talked a little bit about the viruses that we’ve handled. And this gives you an indication of our capacity in terms of dealing with some of the viruses that have sort of attempted to infiltrate the government’s e-mail system. GEMS is now successfully handling up to 1,000 viruses per month. If you look at this in the context of the I-love-you or the nimda viruses, as you know a number of other government jurisdictions experienced some difficulties in these areas. The Government of Ontario and British Columbia, for example, were shut down between three days and two weeks. Largely as a result of some of the good work of some of the folks that are here with us today, we were fortunate in being down for about an hour and a half, early in the morning, and then able to get up and running.

I think part of the reason for our success in this area is that we have some of the latest virus protection tools employed in support of the system. We subscribe to a recognized industry and virus alert organizations group, I think the abbreviation is CanCERT. Phil can tell you what that means because I don’t know.

We also have a system for notification of our users on the system. If we were to happen to have a situation where our e-mail system went down, one of the questions is: how do you let people know what’s going on and how you’re managing it? In our case, we have a voice mail distribution that allows us to interact with folks off of the system and in an immediate fashion. So that in terms of letting people know what’s being done and how it’s being handled, and what their respective roles and responsibilities are, we have a separate system that provides that support.

So I provide that as a . . . simply as a brief background to the system. I’m certainly prepared to take any questions you might have on the system. Fortunately, I have some wonderful expertise around me. I know very little about these things myself, I just surround myself with people who do.

I’d like to, if I can, turn to the recommendations and our responses to them. Phil made reference to the fact that this work was done in September of 2000, and we would like to respond to these.

At the outset, Mr. Chair, through you to the committee, I wanted to just say that while SPMC is happy to be here, two of the four recommendations are really government . . . recommendations to the government. Two of them are specific to SPMC.

So on the second recommendation in particular, I’ll ask Lynn Oliver from the ITO to speak to that one. And between Lynn and I we’ll try and address recommendation no. 4, which is perhaps outside of our respective purviews in terms of the role of the provincial archives, but nevertheless we certainly have a working relationship with them, and we will provide comments on that.

With respect to the first recommendation from the Provincial Auditor regarding specific performance measures and the objectives that SPMC has attached to those performance measures, we have two principal performance measures. And I want to say at the outset that we do support the Provincial Auditor’s recommendation in this area.

Those two performance measures that we have focused on have to do with the time it takes to deliver an e-mail message, and also our response time regarding trouble calls that might originate from the help desk for GEMS support.

Our time to deliver an e-mail message ranges from 5 seconds to 15 minutes, depending on the type of e-mail and the size of the message that is being sent. But in practical day-to-day situations it takes less than 5 seconds for us to provide that transmission.

On the issue of time for help desk calls, we have established a target of providing that support in less than one hour. For minor trouble resolution and for situations where we're talking about organizations that are having problems that are external to ours, in practical day-to-day situations we're talking about 15 minutes as our normal response time for 90 per cent of the calls.

This is not . . . this is, I should say, separate and apart from the kinds of problems that people might experience within their own organizational realm. Sometimes people have difficulties and may contact their own administrators in their own areas to say, I'm having trouble sending something or completing something.

In our case what we're describing with respect to this help desk is the network itself. So it's the interaction between the different post offices and that hub that Phil showed you in the original diagram.

I think it's important to point out in this area as well that the majority of the trouble calls that we receive are not service-affecting, that is to say the service itself is continued despite the fact that we may have something that creates a problem.

Examples of the kinds of things that we're talking about in this area are situations where directory updates are not working. Directory updates occur every night on our system where the directory is in fact updated. The process for updates is each post office sends in their own directory listings to GEMS, and GEMS compiles the listing into a master directory listing and then sends that on to each post office.

Another example is where people are finding that they are unable to deliver mail. This can be anything from the line being down to something being locked up on an individual computer within GEMS or within the organization's post office.

So in addition to those kinds of issues which we would normally provide support to, we do proactively monitor the network so that most service-affecting situations are avoided. Like we do work in advance trying to anticipate it, so oftentimes we are able to address these problems before they affect service for the operators of the system.

In terms of reliability, in this area over the previous 12 months our reliability is at about 99.93 per cent availability. In other words the system is up and running 99.93 per cent of the time. And that's not . . . When we're down in that 0.07 per cent of the time, we're not talking about the system as a whole being down. We're talking potentially about a single department having a problem. So when we say that, the rest of the system is still operating. But we may have a circumstance where one of the organizations is affected and that's the number we've used here.

When the e-mail traffic is down, that is not lost; none of those e-mails are lost. We have a store-and-forward system as Phil pointed out. Consequently no message is deleted until the system knows that it makes it through to the other end. So if there's a problem, that message doesn't disappear somewhere into the atmosphere. It's kept there and it is retained and protected and is still able to go forward.

With respect to the second recommendation, specifically that the government should establish some minimum policies over shared systems and ensure that adequate policies are developed and implemented, that responsibility for shared government systems falls largely within the government's information technology office at Economic and Co-operative Development. And the ITO have in fact established a number of initiatives to address this. And I'm going to ask Lynn Oliver, the government's chief information officer, to respond to this recommendation.

Ms. Oliver: — Thank you, John. The information technology office has addressed the objectives expressed in that recommendation in a number of ways.

Our first initiative was the introduction of the Government of Saskatchewan security charter. The security charter is a commitment by the permanent head of each government department to a security assessment and development of a comprehensive security policy for their organization.

We believe good progress is being made on this front. Seventy civil servants from departments, agencies, and Crowns went through an education process on security policy development over the last year. The city of Regina and more recently Saskatoon have also joined in this process, and my staff are working with several departments to develop a generic security policy which can be used by any public agency and modified to fit their unique requirements. This generic security policy will be finished in the next few months. So I believe that's good progress.

The Provincial Auditor's recommendation focuses on shared systems. Until recently GEMS was the only shared system in the government's information technology infrastructure. However with the implementation of CommunityNet, government will have a common data network which will be the basis of future shared applications.

Historically departments have each built their own data networks, and CommunityNet will consolidate over 700 separate Internet accesses and over 100 circuits to form one government network. So we're developing a security policy that will apply to this new network because all of government's data traffic will be essentially mixed together and all executive government agencies will be required to follow the CommunityNet security policy.

Just as an aside, CommunityNet will provide high-speed Internet access to all schools and health care facilities in Saskatchewan, and the total cost of CommunityNet over the next six years is 71 million, which will be supported by pooling our existing telecommunications resources to support the project.

So for security purposes and the stability of our e-mail and other network applications, CommunityNet will separate the data traffic from the government, education, and health sectors into three virtual private networks. We've learned this from the Government of British Columbia where education and government networks were not separated, and that resulted in some security problems.

In addition to that, we'll be also developing firewalls which will further assist in SPMC's ability to screen for viruses and hacker attacks.

Mr. Law: — Thanks, Lynn. Turning to recommendation no. 3. This recommendation dealt with the development and testing of a complete disaster recovery plan for the government e-mail system.

Again, SPMC supports this recommendation from the Provincial Auditor. In fact, as a start I just wanted to point out that Phil's brought along something that I hope I won't have to refer to in detail, but this is a copy of our business resumption or business continuity plan. It's been in place for some time now.

It identifies sort of a network of individuals who have the authority and responsibility to enact the plan if and when that should be required. It includes a complete inventory of all the hardware and software associated with the GEMS system, types of system disasters, and appropriate actions that we would take in the event that such events took place.

Some capital costing has been done of the associated financial implications, as well as a variety of our own security policies and procedures, including our virus policy. Our equipment — the equipment that supports the system — is located in an environment, in a computer room environment, that provides the appropriate support and security for the physical assets. We have electronic key card access for that system, an uninterrupted power supply, UPS (uninterruptible power supply), which provides again a level of protection.

It is environmentally sound, it's air-conditioned and provides hot spares for redundancy. We have daily system backups in that area as well as off-site system backups.

The one area I should speak to that has not been completely addressed as far as a holistic disaster recovery plan, is the recommendation that deals with the threat and risk assessment components of the Provincial Auditor's recommendation. We have not completed that work; we do have plans to complete it within the next year.

And the reason for that — I may have Phil speak to this, he understands this much better than I do — but in the process of adopting the CommunityNet system, in effect we will be adopting some practices which if we were to try and apply them to the current system would, in effect, be redundant. So for us to do it would require us to do it all over again in an environment which will be substantially different. I don't know if you want to elaborate on that maybe, Phil.

Mr. Lambert: — Yes, the environment that the GEMS was involved in up until June of this year was more of a point-to-point environment. As John mentioned in the first slide, we are the central hub and each of the organizations connect to us on a point-to-point environment. That changes with CommunityNet where we look at a different type of infrastructure.

And so we thought that we would wait until we were migrated onto CommunityNet as well as the other departments and at that point, you know, go through a threat and risk assessment. The threat and risk methodology looks at all the different threats to the environment and the risk associated with those threats and what action do we take to mitigate those risks.

So we felt that we'd be wasting some of our time if we did that prior to moving over to this new environment.

Mr. Law: — Yes, there is a methodology that is apparently — according to Phil and some of the others who understand this, again, better than I do — the RCMP (Royal Canadian Mounted Police) has in fact adopted a methodology which we have recommended in the government security charter that Lynn referenced as the basis for what we will do when in fact we do the threat and risk assessment of the system.

Recommendation no. 4 concerning how well we're meeting the requirements of The Archives Act. This is one of those recommendations concerning what government needs to do. So if I make any mistakes in what I say here, Alan Moffat, who sits on the provincial Archives Board, from SPMC, will correct me.

But my understanding of how we're going to try and respond to this has been based on some ongoing discussions with the provincial Archives Board, where of course responsibility is currently vested for the issues associated with access, retention, and the eventual disposition of records, including electronic records.

What has been done so far is that there are some draft guidelines that have been developed by the provincial archives to deal specifically with when and how we would dispose of electronic messages and electronic information. These guidelines have been circulated throughout government through the Public Documents Committee. They have not formally been ratified at this time, but it's understood that one of the issues that we have to deal with is to understand exactly what constitutes public information.

Some of the communications on the e-mail system apparently does not fall into that category. But nevertheless a significant volume of that electronic information would certainly qualify as public records, and we will need to ensure in our work with the provincial archives that that is covered by the current disposal schedule.

We also should make mention of the information management framework that the archives has been working on with the ITO; Lynn may want to speak to this in more detail. My understanding is that they have in fact been doing some work in this area, Lynn.

Ms. Oliver: — Yes. The information management framework is an initiative that Saskatchewan took the lead on in co-operation with other governments across the country. This is, as you can appreciate, a relatively new area and an area that is complex. So we developed information management guidelines that will enhance awareness, improve understanding, and provide practical approaches to dealing with information as a key resource of an organization.

So the information management framework, while dealing in part with the areas of The Archives Act, is also a more holistic framework that deals with principles; key decision areas, key drivers, life cycle activities — which is of most importance to The Archives Act — sensitivity management, interoperability, governance, and accountability. So we're working with the archives branch to begin to roll this out across government and develop the appropriate archival policies and guidelines.

In addition to the guidelines that have been prepared by the archives branch, I also just wanted to mention that there is an information technology acceptable use policy that has been issued by the Public Service Commission, and it deals also with guidelines for e-mail as well. So that's another way of providing information and guidelines for the requirements around e-mail.

Mr. Law: — Mr. Chair, that concludes our response. If I can briefly summarize. We support all four of the recommendations made by the Provincial Auditor regarding what he would like to have us look at doing in support of the government e-mail system.

I think for the most part that we can say that in three of the four areas we're feeling relatively comfortable that we're in a relatively good position with regard to what has been requested in terms of either having things in place or being on our way to being where we should be.

With respect to the last recommendation, Lynn was a little bit modest when she made reference to the work that they've done nationally. It's in fact been recognized as, I think, the leading piece of work that's been done in this area in the country. And as such, although we have a ways to go in trying to understand how we will apply the expectations of The Archives Act, I think that work is well advanced on the basis of some of the things Lynn has done.

We'd be happy to take questions.

The Chair: — Thank you very much, John, and thank you to Lynn and Phil for your presentations this morning.

And now we'll open the floor to questions from members, to either the auditor's office or SPMC officials.

Mr. Wakefield: — Thank you, Mr. Chair. Just a couple of questions. It's a very extensive, very new and exciting field that you're in and you've covered a lot of territory.

One of the things that us older people are aware of is the relevancy of the development of this IT (information technology) stuff. And really it's the obsolescence that keeps coming along; how do you keep up with that?

Mr. Law: — Well I'll let Phil talk a little bit about some of the initiatives within the GEMS system because I think the first thing I would say about that is that we are affected in some ways by resource limitations in other things.

But this is happening on so many fronts; I think our system is just one element of it, particularly in the context of things that are happening on the Internet. And I think particularly when we think about . . . We talked a little bit about not having done a complete threat/risk analysis yet.

Looking at what's going to happen with CommunityNet and how that is going to be implemented across the province, we see that as being the real sort of next generation of what we will need to be in a position to support.

So as a general comment, I think that we're doing our best within the resources that have been available to us to keep the system up to speed. But as to how you maintain relevance — to your point, sir — that we're where we need to be, I think this is happening on a variety of fronts. I'll let Phil speak maybe perhaps to some of these things. Lynn may have some comments as well.

Mr. Lambert: — Yes. Certainly that is a challenge that we do have. When you think about it, 10 years ago we never even had e-mail on our desk and today we couldn't live without it.

I think how we keep abreast of technology is being plugged into the right individuals and organizations that are doing things. The latest one with the viruses, we are plugged in with the CanCERT organization and the RCMP are certainly involved in that. Those are the experts that are knowing what's happening in the whole area of viruses. But that's . . . how we do plan to keep ahead is just, you know, talking to the experts in these areas and gleaning the information from them and applying those . . . the technology within the province here.

Ms. Oliver: — Thank you. If I could just add two other points. I think one of the key areas is education and awareness. We learned from our security charter policy developments that it was very much a matter of increasing the level of understanding and knowledge in this area among our civil servants.

So we hired the electronic warfare agency who came to us from the East to share with us their expertise. And we led civil servants through a very well-planned educational process. We also brought in the RCMP who shared with us their threat and risk assessment methodology that we'll be following. So that was a very key factor in developing awareness and allowing us to keep up with the technology as it progresses.

We also have a national security subcommittee that my colleague Tim Whelan chairs, and that allows us access to other governments' expertise and a sharing of expertise across the nation.

Mr. Wakefield: — Then, Mr. Chair, just a follow-up on that particular point maybe. I know there's a lot of expertise that is available and that expertise base is expanding. When we're talking about the GEMS system and moving into its compatibility with the CommunityNet system, are there outsourcing or leveraging of other kinds of knowledge in the industry?

Mr. Law: — Just as a general comment, and this is the thought I had as I was listening to my colleagues answer your question, that is the approach that we take in this area and with a variety of the other services that we're responsible for. We do not very much of the doing any more. In many instances what we're trying to do is manage either contractual relationships or take advantage, as Phil said, of the experts who are working in different areas of specialization.

Within government, we have a systems management council which draws together a variety of the folks who work in this on a day-to-day basis in the respective government departments. It provides a forum for the discussion of what's current in the industry. So in addition to staying in touch with some of these perhaps more informed sources outside, the intention with respect to how we've operated and developed GEMS has been based largely on our ability to draw the expertise from outside.

So for example — and Phil, you may want to use an example here with respect to the virus protection — but we are largely managing . . . or providing a management service which engages those experts from outside. So it is in some respects largely a system that relies on a sharing of those responsibilities between ourselves and private sector servers.

Mr. Wakefield: — Thank you. As you pointed out, and correctly I'm sure, the basic e-mail system has expanded really from a communication system and information-sharing system. Each agency and each department, I assume, has its own IT structure. Is there any problems with compatibility and keeping everybody up to the same speed?

Mr. Law: — Do I have to answer that one, Lynn? The short answer is yes. We are . . . it is a challenge for us. In fact, there is some work, as we speak, that is going on right now to try and understand and seek better options for us to enhance compatibility between systems.

As it currently exists with respect to GEMS, we are able to for the most part communicate the different forms of electronic communication and information that are available from one system to another seamlessly. But there are challenges on a day-to-day basis, and there's certainly opportunities for improvement.

Ms. Oliver: — Yes, I think one of the most significant advancements in this area will be CommunityNet which will at long last provide us with one data infrastructure. Historically departments have developed their own data networks which didn't allow communication between and among departments. So what CommunityNet will do will provide us with that basic infrastructure that will allow us to apply that to more applications and shared applications, and better use tools like e-mail and information management tools to help government do its job better.

Mr. Lambert: — If I can add to that as well. When we first started with e-mail, there were 10 different systems back then. Today we only have 4 different systems. And back then the 10 different systems were very incompatible. We had to do a lot of work to get them to exchange e-mails between each other.

And much the same, back then, where we had two different standards in word processing, we had WordPerfect and Word, and you couldn't read one document from one application to the other. The technology has improved significantly since then and with only four systems, the job has become a lot easier than it was back then five years ago.

Mr. Gantefoer: — Thank you very much, Mr. Chair. I can't resist the opportunity to have all this technical expertise in the room to ask a few questions in terms of CommunityNet and some of the implications of it.

From what I understand from some of my technical friends, CommunityNet will be an improvement in terms of stability and speed over the current high-speed Internet in most instances. And I'll just go on with that. And if that's true, the other reality is, is in many communities CommunityNet will be in the community and high-speed will not because of the criteria of CommunityNet dealing with health institutions and educational institutions. May have CommunityNet in their communities but they will never have high-speed because of a lack of volume and things of that nature.

Is there any thought of making CommunityNet available to a broader clientele than the health and education and government network, if you like? And I'm thinking of communities where there might be a significant business in that community that would benefit immensely by having a high-speed connection to the electronic world. Is there any thought of . . . first of all, is it true that the technology is better and second of all, is there any thought of improving the, or opening up the access to CommunityNet?

Ms. Oliver: — What CommunityNet does will . . . it will dramatically increase the speeds available to all government offices, all schools and school divisions, and all health care facilities. And in many instances these will be dramatic increases in speed and dramatic increases in the stability of the service. So it is a very significant advancement in the technology for the public sector, while it serves the public sector and provides all of the participating organizations with higher speeds and better service for the same or less cost.

At the same time it has provided SaskTel with the anchor tenant, if you will. And what that allows them to do is increase the mass volume customer base to allow them to then begin extending high-speed access to businesses and individuals on a business case by business case basis.

We've already seen the evidence of the CommunityNet impact on their service levels. We went previously from only eight communities with high-speed access to a current number of 49 with high-speed access, and SaskTel will be adjusting its service levels to individuals and businesses as CommunityNet is rolled out over the next three years.

On a second front, we're working with the broadband task force that was initiated by Industry Canada of the federal government. This task force included representation from all of the provinces. What we're hoping to do is to leverage the CommunityNet investment and persuade the federal government to use the CommunityNet model to be able to expand high-speed access to across the province.

We believe that we could . . . with current levels of technology and federal investment in this expanded program, we believe that we could reach eventually 95 per cent of the Saskatchewan population. So that's an initiative that we're working on presently.

Mr. Gantefoer: — Thank you. In terms that you said that it's a dramatic increase, is that in comparison to like a dial-up access? And is there any increase of stability and speed as compared to the current high-speed offering?

Ms. Oliver: — Yes. In many instances schools and health care facilities are going from a 56K dial-up access to a dedicated 640 speed, and 10 meg in many instances is what we'll be providing. So it's a dramatic increase in speed for educational facilities and health care facilities. It will allow them to do much more of the applications that require greater bandwidth, for example the distance education applications — video conferencing, audio conferencing, that sort of thing.

And in the health care facilities as well, the ability to transfer X-rays, the ability to do video conference training. So the high-speed access will permit them to do those kinds of applications in a much more stable environment.

Mr. Gantefoer: — Thank you. The other area is, has there been any discussion about allowing MLA (Member of the Legislative Assembly) offices across the province to be considered to be part of the government network?

And the reason I ask that is there are communities where I'm sure where there are MLA offices which will not likely be included in the high-speed system any time soon. But the CommunityNet system might be there. It would strike me that especially all rural offices particularly would maybe be able to benefit from that accessibility.

Ms. Oliver: — That's certainly something we can take into consideration as CommunityNet rolls out.

Mr. Gantefoer: — Okay. The final thing is the next frontier it seems, at least discussed in the computer industry, is the wireless network in terms of, you know, the blackberries, the palms, and all the rest of it in the digital world.

Is the program of GEMS or SPMC envisaging this next bump in the technology, if you like, from a wired electronic network to a wireless one, including the potential of having offices wired in the networks wirelessly?

Mr. Lambert: — You're certainly correct and that is where the technology is going, into the wireless environment. It is still fairly new technology at this point and in the development stages. We are looking at even, as part of an access on CommunityNet a wireless component to that.

So as an example where that may be deployed is in the surrounding areas of Regina, there are a lot of folks that are outside the city of Regina and the only way of really reaching those folks would be maybe through a wireless solution. So we are doing some research in that as well as, you know, just being able to connect your laptop, your blackberry devices, wirelessly.

We are looking at that and at this point the technology isn't stable enough to provide a realistic solution; but we certainly are looking at new technologies as we go forward.

A Member: — Thank you, Mr. Chair.

The Chair: — Seeing no further questions we'll turn to the recommendations then that are found on pages 255 to 259. And we'll deal with no. 1 first on page 255. Recommendation no. 1 deals with the measures and objectives and if I heard Mr. Law correctly talking about SPMC's support of that type of initiative.

Is there any further questions or comments on recommendation no. 1? Seeing none, is anyone prepared for resolution? Mr. Harper.

Mr. Harper: — Mr. Chair, I move:

> That the Accounts Committee concurs with the auditor's recommendation.

The Chair: — Thank you. Concurrence with recommendation no. 1? Any discussion? All those in favour? Opposed? Carried.

Recommendation no. 2 on page 256 I think was identified as a recommendation to government, and we had a response from ITO addressing it through the security chapter and the kinds of things that Miss Oliver had spoken about. Any further questions or discussion? Anyone prepared for a resolution? Ms. Higgins.

Hon. Ms. Higgins: — I move:

> concurrence with resolution 2.

The Chair: — Moving concurrence with resolution no. 2. Any questions? All those in favour? Opposed? Carried.

Recommendation no. 3 on page 257 centring around a disaster plan and the possible use of that binder over there on the table if we ever have to reboot. SPMC indicating support. Any further questions or comments?

Mr. Gantefoer: — Concur and note compliance.

The Chair: — Concurring and noting compliance. Any questions? All those in favour? Opposed? Carried.

Recommendation no. 4 on page 259 dealing with The Archives Act and whether or not this is a broader coverage of all of the departments. We're moving in that direction, I think is what I heard, but still requiring probably a broader vision there. Any further questions or comments about recommendation no. 4?

Any resolution at this time? Ms. Higgins, you have a question. I could tell.

Hon. Ms. Higgins: — Actually I do. As a non-technical person, when we're dealing with archiving e-mails and electronically transmitted information, what kind of numbers are we talking that would be stored, and how are they stored?

I guess I . . . well what I think of is that . . . I mean over the years it was . . . well years ago, and not that many years ago, it was said that . . . I mean all this electronic technology, we would have so much less paper. It would be so much less cumbersome. And that hasn't really happened. It's just easier. So we proliferate this information.

I'm really boggled over this e-mail in the archives. So just a little more information would be nice.

Mr. Law: — Well the only . . . when you ask the question about how . . . what's the volume, the only reference point that I can give you is based on the slide I put up that showed you what the transaction levels are right now.

I can agree with your comment that in many instances I think what we've done is . . . we may in fact be doing a reasonable job in some areas already just by virtue of the fact that oftentimes people print off a lot of their electronic e-mails, put it into paper form. And in one form or another I think there is some of that being captured in the current system without us having to talk about the electronic stuff.

But clearly that's not the intention. I might have Lynn speak to this in more detail, but my understanding is that the work that has gone on with the provincial archives is attempting right now to deal with this very issue — that is, to understand precisely what constitutes a public document in terms of what's going back and forth on the e-mail system. Some of those transactions will be dealing with things like scheduling meetings and so on, which wouldn't necessarily be things that you would be concerned about retaining for the public record. Having said that, I think this is a work-in-progress.

What we might be able to do for you is to provide you with some of the information on the draft guidelines that have been developed so far. Those are currently in circulation and my understanding is that the intent is to try and gather some additional feedback and therefore input on the characterizations of what should be included and what should be excluded.

Ms. Oliver: — There's also, in addition to increased education and awareness of the digital documents that we have and the implications for archiving, there's also some new information technology tools that we hope to take advantage of. We're working with IBM currently and one of their experts in Toronto to look at some content development and management tools that would allow us to do a better job of organizing, sorting out, and particularly retrieving our digital information.

So I believe it needs to go on two fronts. We need to have a better understanding of the implications for archival information, along with examining and piloting and, in the longer term, implementing new technological tools that will help us retain better control in management of our digital information.

The Chair: — Thank you. And I think, as indicated in recommendation no. 4, it's saying that the government should evaluate the requirements and develop processes. And in listening to your comments, Mr. Law and also Ms. Oliver, I think that's what you're suggesting is underway right now.

Are you there yet for something that Ms. Higgins and I could understand? Well, maybe not quite yet and we'll look forward to that . . . Never. Thanks, Mr. Gantefoer.

Anyways, the recommendation is before you. Is there anyone prepared to move resolution?

Ms. Jones: — I would move:

> That PAC Committee concurs and note progress.

The Chair: — Concurrence and noting progress. Any discussion? All those in favour? Opposed? Carried.

Thank you very much, Mr. Law and all your officials, the gentlemen in the back as well. Thank you for being present and assisting us work through this chapter.

Recess until 10:30.

The committee recessed for a period of time.

The committee continued in camera.

The committee adjourned at 11:12.