House of Commons
CANADA

Standing Committee on Public Accounts

PACP • NUMBER 025 • 1st SESSION • 38th PARLIAMENT

EVIDENCE

Wednesday, March 23, 2005

Chair

Mr. John Williams

Standing Committee on Public Accounts

Wednesday, March 23, 2005

● (1535)

[*English*]

The Chair (Mr. John Williams (Edmonton—St. Albert, CPC)): Good afternoon, everybody.

The orders of the day are, televised, pursuant to Standing Order 108(3)(g), chapter 1 ofthe February 2005 Report of the Auditor-General of Canada, "Information Technology Security", referred to the committee on February 15, 2005.

The witnesses today are, from the Office of the Auditor General of Canada, Mr. Douglas Timmins, assistant auditor general; Mr. Richard Brisebois, principal; and Mr. Guy Dumas, director. From the Treasury Board of Canada Secretariat we have Mr. Pierre Boucher, senior director,architecture, standards, and engineering; Ms. Helen McDonald, chief information officer; and Mr. Simon Gauthier, deputy chief information officer.

Before we proceed, I have two items. I've been given notice of a point of order, and before I go with that, I have an announcement for all our public accounts committee members. Once a year the federal public accounts committee gets together with all the public accounts committees of the provinces. This year it will be from August 21 to 23, and on April 4 we'll be bringing forth a budget.

The location is going to be Niagara-on-the-Lake, Mr. Lastewka, which is your hometown, so we're looking forward to some hospitality from you when we're down there, perhaps.

Hon. Walt Lastewka (St. Catharines, Lib.): No problem.

The Chair: As I said, I'll bring forward a budget on April 4. If you could, put that in your calendar so the federal public accounts committee can have a presence and show the rest of the country how we do things here in Ottawa—and how well we do things here in Ottawa.

Anyway, I have a point of order from Mr. Kramp.

Mr. Daryl Kramp (Prince Edward—Hastings, CPC): Today I must raise an issue of grave importance. It is the matter of the committee's privileges relating to in camera proceedings of this committee on this past Monday, March 21, 2005. Of course, I was shocked to read in today's Montreal Gazette, on page A16:

> ...Liberal committee member Mark Holland said the committee is being asked to examine something that has already been cleared by the auditor general. He said that is why he pushed for the committee to hear from Dodge and Fraser as well as O'Leary, Cutler and Kinsella.
>
> "It's an attempt to use the committee to score some partisan points and to try to drag people who have connections to the prime minister in front of the committee to hopefully find a way to embarrass them in a partisan way."

Mr. Chairman, Mr. Sauvageau, the Bloc Québécois member of Parliament, is mentioned in the same article and is referred to as saying he was pleased the committee has agreed to investigate the question:

> "I think we will learn that it wasn't only in the Guite, (Alfonso) Gagliano, Chretien group that things were happening, but it seems there was also, within the finance department, similar behaviour."

Now, Mr. Sauvageau's comments did not directly refer to the proceedings of an in camera meeting of this committee and therefore are not part of my point of order.

A member divulging in camera proceedings has been dealt with by the House before; please see page 68, footnote 96, of Marleau and Montpetit. In 1987 the Speaker accepted as a prima facie case of privilege a matter involving John Parry, member for Kenora—Rainy River, who divulged the results of an in camera vote; see House of Commons Debates of April 29, 1987, pages 5299, 5329 to 5330, and others.

The same matter regarding Mr. Parry is also dealt with in footnote 362 on page 130 of Marleau and Montpetit, which stated that the committee reported the matter to the House. In footnote 363 on the same page, the report to the House concluded: "Your Committee feels it is their duty to place these matters before you at this time since privilege may be involved and to give the House an opportunity to reflect on these matters".

Mr. Chair, I would therefore move that in light of the comments made by the member for Ajax—Pickering, Mr. Mark Holland, in the Montreal Gazette on page A16 on March 23, 2005, where he referred to in camera proceedings of the Standing Committee on Public Accounts and is quoted as saying

> ... Liberal committee member Mark Holland said the committee is being asked to examine something that has already been cleared by the auditor general. He said that is why he pushed for the committee to hear from Dodge and Fraser as well as O'Leary, Cutler and Kinsella.
>
> "It's an attempt to use the committee to score some partisan points and to try to drag people who have connections to the prime minister in front of the committee to hopefully find a way to embarrass them in a partisan way."

I believe it is in order that a motion be presented that the privileges of this committee have been breached or that a contempt may have occurred, and I therefore ask that the committee report to the House, stating that the committee feels that there is a prima facie breach of privilege or contempt and that it is their duty to place these matters before the Speaker and to give the House an opportunity to reflect on these matters.

The Chair: Thank you very much, Mr. Kramp.

Mr. Holland has just joined us; he wasn't here for the reading.

Mr. Holland, Mr. Kramp has raised an issue regarding your comments in the Montreal Gazette—I believe it's today—where you were commenting on an in camera meeting we held on Monday. You were commenting and he has quoted you twice in his statement. He's therefore asked this committee to consider it a prima facie breach of the privileges or a case of contempt of the committee and to report the same to the House.

I was wondering if you have any comment on this, Mr. Holland.

Mr. Mark Holland (Ajax—Pickering, Lib.): Can you give me a moment to see the article?

The Chair: Do you have a copy of the article, Mr. Kramp?

Mr. Daryl Kramp: I might have a copy. Yes.

The Chair: There it is, Mr. Holland.

● (1540)

Mr. Mark Holland: The only thing I can say about the conversation that took place between me and Elizabeth Thompson is that she had relayed to me the names of people she had heard were witnesses. I made a comment in general terms about dealing with chapter 5 of the 2003 report. I didn't at any time state that I was pushing for or advocating any particular witnesses.

What I did say was that if we were going to deal with the matter, then it should be dealt with broadly and in a non-partisan way. I think the quote "It's an attempt to use the committee to score some partisan points and to try to drag people who have connections to the prime minister in front of the committee to hopefully find a way to embarrass them" was a reflection of those general comments and certainly didn't divulge conversations that took place within a closed setting.

The Chair: I think it's actually the previous paragraph that seems to be more of a problem: "He said that is why he pushed for the committee to hear from Dodge and Fraser, as well as O'Leary, Cutler and Kinsella."

Mr. Mark Holland: That's paraphrasing my comments. I didn't mention the names. I said I had pushed for us to hear from a broader range, more than a few specific individuals. I did not refer to names or particular details. I pushed for it in a general sense; it's been paraphrased and these names added.

The Chair: Mr. Fitzpatrick.

Mr. Brian Fitzpatrick (Prince Albert, CPC): My own view is that even a general discussion of the whole topic would get into the area of violation of the in camera principle. To me, "in camera" means everything that's on the table in this room; when it's in camera, we don't discuss it outside. Even bringing up the fact that discussions on chapter 5 took place is disclosing something that took place in camera in the committee. Certainly any suggestion of strategies employed in the meeting and of why people were pushing for certain witnesses and so on is a clear-cut violation of the principle.

The only question I'd have in my mind is whether it was just a mistake or whether it was deliberate. If it was deliberate, then I would get quite concerned about it. People can make mistakes and there can be a slip of the tongue, but to my mind, something that is calculated and deliberate gets into the area of contempt and violation of privileges of members.

The Chair: I should caution all members, by the way, that the point that has been raised by Mr. Kramp is about what was discussed at an in camera meeting. Therefore, if any members get into a discussion themselves at a public meeting about what happened at an in camera meeting, they can perhaps put themselves in jeopardy in the same way Mr. Kramp has complained about Mr. Holland doing. You must be extremely careful about referring to the in camera meeting. I would ask that you contain or restrict your remarks to what appeared in the media rather than to what happened at the meeting.

Mr. Holland, do you want to say something?

Mr. Mark Holland: Yes, I have a couple of comments.

First of all, I don't know how the reporter obtained the list of witnesses, but she had the list of witnesses at that point in time. I don't know if that was public or not. Perhaps that's an appropriate clarification.

When she contacted me, my comments, again, were on the general matter of dealing with chapter 5. Again, that is public. The fact that this committee will be dealing with that particular chapter has been noted in many different stories. It is a matter of pubic record. I was commenting on the appropriateness of this committee engaging in a discussion of that particular chapter. Again, that has been in both The Gazette and, I believe, La Presse—and elsewhere. It was well reported that we were walking into that particular item. I was commenting in generalities both about my concern about us entering into that chapter and, secondarily, about my feeling that if we were going to enter into it, we should be hearing from a number of different individuals.

Now that's been paraphrased with the addition of a list of witnesses. I don't know where that list of witnesses came from. As I said, when I was called, I was told who the witnesses were and who I was pushing for. I did not repeat what that reporter said, but I can tell you the reporter did give me not only the list of witnesses who were suggested at the meeting but also the list of witnesses I was advocating. I did not repeat those, but I did say in general terms that I felt if we were to engage in this matter, it should be broad and it shouldn't be just with those individuals who have partisan connections. That was then paraphrased to say I was pushing certain names.

● (1545)

The Chair: By the way, the clerk advises me that by virtue of the report of the steering committee to the main committee, the fact that we were going to deal with chapter 5 is in the public domain. The issue that appears to be of concern is that reports of the discussions of how we were going to proceed, which were at an in camera meeting, now appear in the media.

Mr. Kramp, please.

Mr. Daryl Kramp: I'm concerned for a couple of reasons.

I'm here to work with my colleagues on all sides of the House, and we're all human. We're all capable of making a mistake; I think that's well recognized. My point is that this was recognized in a previous meeting, where there were incidents that were dealt with within an in camera setting within our committee here. As a result of activities and comments on the part of committee members and our committee chair, the air was pretty clear. Were this the first occasion a matter like this had been brought before the committee, I think some general latitude and understanding could be there.

But I certainly do believe our discussions have to be in confidence. That's the purpose of an in camera meeting, to discuss and bring forward an issue or an item like this. I am greatly concerned by the fact that just after having left one meeting where we had incidents that were discussed, we now find ourselves in a similar set of circumstances. I do believe some action must be taken so we can put this behind us and carry forward in an atmosphere of collegiality and understanding and with a determination to do what is right, literally, on behalf of this committee and Parliament.

The Chair: Mr. Carr.

Mr. Gary Carr (Halton, Lib.): Thank you, Mr. Chair.

I just have a point of clarification. I don't know if I should know this, but would anybody have known the list of witnesses, or was that leaked as well? I don't know whether that was public knowledge, or are we also talking about a leak of the witnesses' names on this?

The Chair: We passed a motion stating we would have a hearing and that witnesses would be called. The clerk advises me that the motion is a public statement and that by virtue of that fact, the names of the people who were called became public. But who moved them, who proposed them, and the debate around how we came up with these names are not part of the public record. Only the fact that a motion was passed and that these people are to be called by virtue of that motion is part of the public record.

Mr. Fitzpatrick.

Mr. Brian Fitzpatrick: I have to have an issue satisfied in my mind as to the facts of the matter. But maybe even before that, I would say that if we take our debates that go on internally here outside these four walls and discuss them in the public domain with a reporter or anyone, that in itself undermines the whole purpose of in camera meetings, because the debate is supposed to be carried on in here. To get enticed into that sort of discussion with a reporter and carry on I think is wrong.

More importantly, I read the article as a direct quote from Mr. Holland to the reporter. The way it's reported, the reporter is attributing that information directly to Mr. Holland. Mr. Holland is saying no, that's not the case. I have to get one point clear in my mind here. Is Mr. Holland saying the reporter is misrepresenting what was said or is lying on that matter? I see it as a direct quote from the lips of Mr. Holland.

The Chair: Mr. Holland.

Mr. Mark Holland: I'll reiterate this to be clear. I didn't know where the list of witnesses came from, and I appreciate the clarification that the list of witnesses had been made public as part of the motion. When I was called and asked about the witnesses who were on the list, in the course of the conversation I did, absolutely, say I had pushed for more than just partisan names. The names she mentioned as being part of the discussion and debate were the two, Madam Fraser and Mr. Dodge. When I said I had pushed for others than just ones who were partisan in nature, she put down explicit names. That's not lying, but it's also not a quote.

● (1550)

The Chair: Mr. Holland, I should advise you, you are regurgitating what happened in camera, so we have this real problem. We're meeting in public and debating what happened in camera, and as I mentioned earlier, I would suggest that people refrain from discussing what happened at the meeting and address themselves to what is in public documents. That means, as I said, the names that are referred to in the motion and what appears in the paper. Nobody is going to get into trouble if they restrict their remarks to these things.

Mr. Mark Holland: As a point of clarification, I'd like to point out that what I did was twofold: one, to comment on what I thought was the appropriateness of us dealing with this particular chapter, which I think is a fair comment, as it's my opinion; and two, on the matter of the public witnesses, to say whether it was appropriate to just have partisan witnesses or to have a broad list of witnesses. That's my opinion; that's not regurgitating something that happened in committee. That's saying that in my opinion we have to have a list of witnesses that goes beyond just those who are partisan; that reflects the quote I gave. A statement of my opinion is not a regurgitation of something that happened in an in camera proceeding. There's a major difference there.

Ultimately, if you read it, there is nothing I revealed through the course of that interview stating anything, really, other than my opinion on how the matter should proceed. It's not about the content or the subject of an in camera proceeding.

The Chair: Mr. Lastewka.

Hon. Walt Lastewka: I just want to go further on what Mr. Carr mentioned.

That was a surprise to me, by the way; I didn't know that when there's a motion made in camera and it has names attached to it, they also become public. I think that's a lesson learned. We have some new members of Parliament, and I think we have a good lesson learned here.

I take Mr. Kramp's comments very seriously, but I think we should leave it at that. We should carry on with the agenda but take it as a good lesson learned for all of us.

The Chair: Mr. Fitzpatrick.

Mr. Brian Fitzpatrick: I just want to reiterate the point about taking debates outside of in camera meetings. To me, confidentiality means confidentiality. If you're making reference publicly to somebody else in the meeting having an allegedly partisan list of witnesses, you're taking information outside the walls of this meeting.

The Chair: Just address your remarks to the chair, please.

Mr. Brian Fitzpatrick: That's the point I want to drive home. The debates and discussions are as important as any particulars that go on in these meetings. It's not just taking specifics, Mr. Chair, out to the public. If you're going to take the debates and the arguments that go on in the committee outside the four walls, you're violating the principle on that ground as well.

The Chair: I don't particularly enjoy having to deal with these kinds of issues.

Mr. Kramp did deliver his statement to me beforehand, and I had a chance to talk this over with our clerk. We can't bend the rules or decide what rules are for us; we have to live by a common set of rules. That is why Parliament has evolved. That's why we have Marleau and Montpetit, with its thousand pages of precedents as to what is and isn't acceptable in this place. There is a motion here Mr. Kramp has put forward, and in Marleau and Montpetit it says:

> If in the opinion of the Chair the issue raised relates to privilege...then the committee can proceed to the consideration of a report on the matter to the House. The Chair will then entertain a motion which will form the text of the report. It should clearly describe the situation, summarize the events, name any individuals involved, indicate that privilege may be involved or that a contempt may have occurred, and request the House to take some action. The motion is debatable and amendable, and will have priority of consideration in the committee. If the committee decides that the matter should be reported to the House, it will adopt the report which will be presented to the House at the appropriate time during the Daily Routine of Business.

First of all, it's "If in the opinion of the Chair the issue raised relates to privilege", so that falls to me. If I feel it is appropriate, then it goes back to the committee. If they decide it is appropriate, then we send it to the House; they deal with it and they decide if it's appropriate.

There are a number of checks and balances built into the process here. In my opinion, we can't have people just saying, well, the rules don't apply to me; I can talk and make comments about what happened during in camera meetings. Other people feel quite constrained and say no, I can't talk about what happened in camera because in camera is in camera and that's confidential.

As I said, if I make this ruling, then the decision falls to the committee, who would then report to the House, which would then have a chance to discuss it and decide. I don't think it's for me to cut this off at the pass right at the very beginning. There are a number of steps, a process, with appeals that can be entertained.

First, I read "If in the opinion of the Chair the issue raised relates to privilege", and then I read:

> Liberal committee member Mark Holland said the committee is being asked to examine something that has already been cleared by the auditor general. He said that is why he pushed for the committee to hear from Dodge and Fraser as well as O'Leary, Cutler and Kinsella.

To me, that appears to be a matter of privilege. Therefore, I'm going to say it's a matter of privilege. Then it's for the committee to decide if my ruling is appropriate, and if so, it will get referred to the House, which then will decide if the matter is appropriate, and it goes on from there.

First of all, let me ask, is this motion in order as presented? It says here "I would therefore move that", so we'll assume the motion is in order and is debatable.

Mr. Carr.

● (1555)

Mr. Gary Carr: I'm just wondering if Mr. Kramp wants to include Mr. Sauvageau as well, because it says in the article that Mr. Sauvageau, "who initiated the move to examine the Earnscliffe contracts, said he was pleased the committee has agreed to investigate the question". So my question to Mr. Kramp is, further to the chair's ruling, does he want to include Mr. Sauvageau in that as well?

The Chair: He had said in his statement, and I quote—you just quoted Mr. Sauvageau in the article, so I don't have to do it again—"Mr. Sauvageau's comments did not directly refer to the proceedings of an in camera meeting of this committee and therefore are not part of my point of order".

Now, as I said, it has been common knowledge for quite some time that we will look at chapter 5. That is in the public domain by virtue of the fact that we adopted a motion, and motions adopted by committee become part of the public record. I do not feel Mr. Sauvageau's comments pertain to a discussion. He said "we will learn"; he was speculating about what witnesses may say in the future about what Mr. Guité, Mr. Gagliano, and Mr. Chrétien were thinking. That is why I think Mr. Holland is perhaps in breach of the privileges of the House, but I don't think Mr. Sauvageau is; that's my opinion.

● (1600)

Mr. Gary Carr: This is just for clarification; I won't repeat it because I know you don't want to have it repeated. He commented by saying he was pleased as well. Information was leaked out about who moved a particular motion, according to this article, so who leaked that? How did that get out there?

My suggestion is that if you're going to use one standard, the same standard can be applied to Mr. Sauvageau...the way you read it.

The Chair: Well, I don't know who put it out in the public domain about motions and so on. The clerk advises me that when a motion is adopted in camera, it just says it was moved and carried. It doesn't say who moved it or who carried it; it was a decision of the committee. That's as far as the public record is concerned.

At this point in time I only have a suggestion from Mr. Kramp that Mr. Holland has breached the privileges of this committee. I have said, because I'm in essence the first step in deciding whether or not this is appropriate, that I don't feel it's for me to cut off the debate. But I do feel also that Mr. Sauvageau did not breach the privileges of the committee by talking about what happened in camera.

Mr. Gary Carr: It's a double standard.

The Chair: Well, it may be a double standard, but he was speculating about what might happen at a future date, so it couldn't have been about what had happened.

Mr. Kramp.

Mr. Daryl Kramp: If I could, I'll ask for the indulgence of my colleagues on this. I'm really of two minds, and maybe I'll ask for your consideration while I'm talking and deliberating.

I really feel that were this a first-time occurrence of a misstep before this committee, it would be very easy just to carry on. When this is obviously another occasion, it adds a great deal of concern with respect to where we are going with the committee. The most important thing to me is not who's wrong or who's at fault but where we're going. For the good of this committee, for the job we have to do, for the respect of the guests we have here today, and in conference with my colleagues today, I'd be prepared to suggest that we either table this motion or that I withdraw it, with a firm understanding that the line has been drawn in the sand.

Mr. Lastewka made a very apt comment. We have a number of new members, me included; we are all limited and we all make mistakes. Sometimes, when an occurrence happens time after time, that eliminates the possibility it's a mistake. I don't believe it's an error, but at this particular time I do believe that consideration for my colleagues is more important than making a simple punitive assessment of an individual and/or a colleague when we have very serious work to do.

With the indulgence of the chair and my colleagues, at this particular time I am prepared to withdraw my motion. Let's just get down to business. I don't know what your thoughts are on that, but it's important to me for us to work together here.

The Chair: You said you are prepared to withdraw it, but the decision is yours. Are you withdrawing the motion or are you leaving it on the table?

Mr. Daryl Kramp: I am withdrawing the motion.

The Chair: My clerk has just advised me that we require unanimous consent to withdraw a motion. Mr. Kramp has asked that the motion be withdrawn. Is there unanimous consent that the motion be withdrawn?

Some hon. members: Agreed.

The Chair: There being no opposition, the motion is withdrawn. The issue is now behind us.

Mr. Holland would like to speak, but before Mr. Holland speaks, I just want to make it clear to all committee members, especially the new committee members, that the Parliament of Canada has been around for about 138 years and has developed a great number of precedents. We live by trust, not just trust in our colleagues in our own party but trust in our colleagues in Parliament. If we're not going to be governed by rules, then the whole system will fall apart. Therefore, when people take advantage of the system and go outside the rules, thinking they can do so with impunity, we debase the whole process, and that applies to all members.

Therefore, Mr. Kramp has been magnanimous, I think, in withdrawing the motion, and the motion is behind us. But I don't think he will be so magnanimous the next time. We've all been advised, so be governed accordingly.

A very brief final comment, Mr. Holland.

● (1605)

Mr. Mark Holland: It's not necessary.

The Chair: That being done, we will now turn to our witnesses for the opening statement from the Auditor General's office.

Mr. Timmins, please.

Mr. Douglas Timmins (Assistant Auditor General, Office of the Auditor General of Canada): Mr. Chair, thank you for this opportunity to discuss the results of our audit on information technology security.

Joining me at the table, as you mentioned earlier, are Richard Brisebois and Guy Dumas, the principal and the director responsible for this audit.

We last audited IT security in 2002. Since that time cyber threats to information technology have increased dramatically. In 2002 a revised government security policy had just been released, but the operational standards needed to implement the policy were outdated or did not exist.

Since 2002 the Treasury Board Secretariat has worked with lead security agencies and some departments to issue several operational and technical security standards. For example, standards have been issued for business continuity and for the management of IT security, referred to as MITS. However, several other operational standards remain to be developed, mostly in areas that affect IT security such as threat and risk assessments, contracting, security training and awareness, and the identification of assets.

To be effective, policies and standards must be translated into real actions by the departments and agencies. In general, we found that departments and agencies do not meet the core requirements of the policy and standards, or if they do, it is not done consistently across all business sectors and geographic locations.

[*Translation*]

As part of our audit, we looked at the results of an IT security self-assessment questionnaire administered by the Treasury Board Secretariat where, our of 46 departments and agencies, only one stated that it met the baseline requirements. We complemented this questionnaire with a survey of our own of 82 departments and agencies and obtained similar results.

[*English*]

We looked at 20 reports of technical tests conducted over the past two years in various departments and agencies. Most of these reviews identified significant weaknesses in IT systems that, if exploited, could have led to serious breaches of security, loss of confidentiality of information, and damage to unsuspecting citizens or businesses.

Mr. Chair, we have also reviewed IT security practices in the four departments we had examined originally in 2002. While some of these departments made significant improvements in specific security practices, none met all of the baseline requirements of the policy.

In our survey we found that out of 82 departments and agencies, only 37—or 45%—had prepared threat and risk assessments of their programs, systems, or services as was required by the policy. In most departments and agencies, senior management is not made aware of the results or is unaware of the IT risks and therefore may not attach sufficient priority to addressing them.

[*Translation*]

In our report, we also note that the Treasury Board Secretariat has not completely fulfilled its oversight role as defined in the Policy. It did not have processes in place to collect and analyze the IT security findings identified in departmental audit reports. The Secretariat also has not completed the mid-term report to the Treasury Board on how effective the Government Security Policy is in strengthening security. This report was due in the summer of 2004. As a result, little baseline information continues to exist on the state of IT security across the government.

● (1610)

[*English*]

Mr. Chair, specific and timely action to address IT security concerns is important. The committee may want to ask the Treasury Board Secretariat the following questions. How will it ensure all needed IT security standards are developed and issued in a timely manner? How will it ensure departments and agencies implement a reasonable level of IT security and are held accountable for its implementation? How will it fulfill its oversight role concerning IT security and monitoring IT security audits in departments? And when will the mid-term report on the government security policy be prepared?

That concludes my opening remarks. We'd be pleased to answer any questions the committee might have.

The Chair: Thank you, Mr. Timmins.

Now we'll turn to Ms. McDonald, the chief information officer, for her opening statement.

Ms. McDonald.

[*Translation*]

Ms. Helen McDonald (Chief Information Officer, Treasury Board of Canada Secretariat): Thank you, Mr. Chairman.

Good morning. I'm Helen McDonald, Acting Chief Information Officer for the Government of Canada. I am accompanied by Simon Gauthier, Deputy Chief Information Officer, and by Pierre Boucher, Acting Senior Director, Enterprise Architecture and Standards. Mr. Gauthier and Mr. Boucher helped me to develop the response of the Government of Canada to the points raised by the Auditor General.

On behalf of Treasury Board Secretariat, I would like to begin by thanking the committee for this opportunity to discuss the chapter on information technology security.

I want to say first that the Government of Canada fully subscribes to the recommendations of the Auditor General. We thank the Auditor General and her office for the report on progress in strengthening information technology security since the audit conducted in 2002.

[*English*]

Indeed, the Auditor General's findings are consistent with our own IT security self-assessment results, which were part of TBS's monitoring and oversight functions. On this note, I would like to briefly share with this committee the work that has been done since this last audit and describe our way forward on this most important issue in the weeks and months ahead.

Treasury Board Secretariat and lead security agencies, namely the Royal Canadian Mounted Police, Public Safety and Emergency Preparedness Canada, and the Communications Security Establishment, play a key role in developing and renewing IT security standards, technical documentation, and guidance to respond to new IT challenges and opportunities.

Ms. Helen McDonald: For example, last May TBS introduced the management of information technology security or MITS standard, which covers the 40 standards that had been identified in 2002 as key to an effective Government of Canada IT security posture. MITS establishes in a succinct, plain-language document the IT security baseline requirements for all departments. The Office of the Auditor General used this standard as the compliance baseline in its most recent audit. This new standard requires all departments and agencies to annually complete an IT security self-assessment as well as an action plan to address IT security gaps. Departments and agencies are expected to be compliant with MITS by December 2006.

In 2004 TBS also visited 90 departments and agencies to review their progress in implementing other aspects of the government security policy. The finding from these visits will be included in our mid-term report on the effectiveness of the government security policy, which we expect will be ready in May 2005. Overall, we found that larger federal institutions were either more mature in their overall security posture or had government security policy implementation plans well under way.

TBS is also leading the development of a performance measurement methodology for IT security that will identify the indicators, tools, and measurements to validate departmental compliance. We are looking at ways to integrate the information acquired from vulnerability assessments, threat and risk assessments, incident management reports, and IT security self-assessment reports, as well as departmental visits, into a coherent view of the state of IT security within departments and within the government of Canada. We are also exploring the possibility of including IT security as a measurement in the management accountability framework that is used for discussions between deputy ministers and the Secretary of the Treasury Board in order to assess performance each year.

In conjunction with the lead security agencies, the RCMP, the CSE, and PSEPC, as well as with the participation of Public Works and Government Services Canada, TBS is moving towards the provision and use of common and shared IT infrastructures and services solutions, for example, the Secure Channel, common intrusion detection and incident management solutions, and the sharing of threat and vulnerability information.

In addition to these measures, the secretariat has taken several steps to increase awareness of IT security in the government and to help Government of Canada institutions comply with its policies and standards. These efforts include a variety of security training programs that are offered across Canada through the RCMP, the CSE, and the Canada School of Public Service.

Despite all the challenges facing such a large organization, the Government of Canada is able today to share information more effectively than ever amongst its departments. The 2002 government security policy and the December 2003 creation of Public Safety and Emergency Preparedness Canada clarified roles and responsibilities and identified leadership in areas such as the sharing of threat and vulnerability information.

We also continue to provide opportunities for discussions of IT security in communities of interest, such as at departmental security officers' briefings, IT security committees, and the CIO Council, as well as in meetings with IM/IT specialists andinternal auditors. As a result, I have much confidence in the government's ability to actquickly and cooperatively to prevent, detect, and respond to securitybreaches across the government of Canada.

● (1615)

[*Translation*]

We are also strongly determined to closely monitor the strengthening of IT security throughout the federal public service. Our objective is to consolidate the heightened awareness of deputy ministers and senior departmental managers to the importance of IT security in the routine functions of the federal government.

As the Auditor General has already done, we also want to ensure Canadians that their on-line transactions, as well as the information the government holds about them, will continue to be properly protected. I am confident that the federal government can achieve its objective of strengthening and standardizing its IT security procedures throughout the public service.

● (1620)

[*English*]

My optimism in our ability to meet our IT security objectives in the context of the dynamically changing risk environment rests in the government's broad action plan, which includes the following four points: improving our monitoring and oversight activities, including the completion of the mid-term report in the weeks ahead and annual IT security self-assessments by departments and agencies; secondly, ensuring that GoC institutions take IT security risks into account as part of their corporate risk profile; thirdly, requiring IT security action plans from government departments and agencies, signed by deputy ministers and heads of agencies, no later than summer 2005; and fourthly, supplementing the MITS with technical documentation as required.

We are also committed to completing, by December 2006 at the very latest and in participation with PSEPC, a set of standards pertaining to intrusion detection and incident management.

Ultimately, the government's goal with respect to IT security is to improve the resilience of departments and agencies in order to ensure the continued delivery of services to Canadian citizens and businesses.

[*Translation*]

Mr. Chairman, that completes my remarks. My colleagues and I would be pleased to answer questions from members of the Committee.

[*English*]

The Chair: Thank you very much, Ms. McDonald.

Before I ask Mr. Fitzpatrick to begin, I'm going to ask a question right off the bat. You state in your opening statement, “I have much confidence in the government's ability to act quickly and cooperatively to prevent, detect, and respond to security breaches across the government of Canada”, which is in direct contravention of what Mr. Timmins and the Auditor General are saying.

Ms. Helen McDonald: The Auditor General also noted that the central agencies had improved the clarification of their roles and responsibilities and were working much more successfully together, and that includes the sharing of incident information and the speeding up of the response to threats to our systems.

The Chair: Would you say that comment is a bit too optimistic, Mr. Timmins?

Mr. Douglas Timmins: Well, our audit revealed the fact that there were certainly threats and risks out there that were not being managed. That doesn't mean we could conclude whether they would be able to adequately respond to those threats and risks should they materialize.

The Chair: Mr. Fitzpatrick, please, for eight minutes.

Mr. Brian Fitzpatrick: I'm going to focus in on just one area, and that is the terrorist threat. Part of the era we live in is the presence of terrorism as a very real and present danger in our society. The Air India thing brings to everyone's mind that it was just a sort of snapshot of the future when it occurred. If we could look back at that period of time, we'd see, even with the RCMP or the security people involved in that, that there may have been serious breakdowns at that time in the information technology systems for information that might have prevented it. I know it's a new era, but that's one observation I would make on that.

I recall the power blackout we had a year ago last summer, I believe. We could all see the serious consequences if there was a breakdown in the system. It's often crossed my mind that if the terrorists really wanted to cripple Canadian society or American society and so on, one way would be through explosives. Another way is to get into systems and cause a lot of problems. All we have to do is see a blackout like the power blackout to know how vulnerable we are.

That leads me into point six of Mr. Timmins' report, though I'm going to direct my question to Ms. McDonald. It says out of 46 departments only one met baseline requirements. I'm interpreting "baseline requirements" to be bare, essential standards. The Auditor General's office said they surveyed 82 other departments and found similar results.

Now, I know you have a lot of confidence from the way you were presenting, saying everything is under control and everything is being met and so on, but are you saying today, Ms. McDonald, that if we went back and did these risk assessments at random again, we would find all the departments and agencies would meet this minimal baseline requirement?

Ms. Helen McDonald: What was done in 2004 was an assessment against the baseline established by our MITS—-management of information technology security—standard. That set the baseline. I think the Auditor General's office would agree with that because they used that as their assessment tool as well.

The MITS standard was only approved in 2004; it was available in draft form in late 2003. When you measure departments against it, you find they are not completely compliant with it, absolutely. According to the study we did, only one was meeting the baseline requirements. MITS establishes the baseline, and by that we mean it's the minimum security level we want to see across all departments and agencies.

Mr. Brian Fitzpatrick: Well, that's my point; you want to pass that test. That's the first hoop to get through, and we only have one out of 46.

My question is this. That was 2004, but are you confident today that if we went back to these departments, we'd find there was real improvement?

● (1625)

Ms. Helen McDonald: I am confident you would see improvement, but we have given departments until 2006 to fully meet the terms and conditions of the MITS standard. We realized when we put this out that most departments would not be fully compliant with it and that it would take some time for them to get there.

Mr. Brian Fitzpatrick: Mr. Timmins, would you share her enthusiasm or confidence about the progress being made?

Mr. Douglas Timmins: Well, we do certainly support the idea of setting a deadline and setting targets to be met. Whether there's been progress made to date, we have not assessed that.

I think the only other factor I would mention is that what was particularly troublesome to us in looking at the audit was, what's in this baseline standard? Yes, it was established in 2004, but some of those requirements had been around for 10 years before that. The state is generally of some concern to us, but we are certainly encouraged by the fact that a deadline has been set and somebody's going to—

Mr. Brian Fitzpatrick: That raises another point, because in the area of information technology, if there's any area where the outside world is way ahead of the public sector and government, it's technology. We're ten years behind on some of these things, if I interpret that correctly. I've never seen the government looking ahead to try to get ahead of the pack; they're always leading from the rear.

The question I'm asking is, is the government really in contact with some of the leading private sector technology firms in the world, ones that are really in the know on security, or are they relying on their internal bureaucracy to determine their standards and the way they deal with these sorts of threats?

In my view, this is one area, definitely, where the government should be reaching outside the bureaucracy, going out in the private sector, finding the very best people out there in this area, and making sure they're on the leading edge and not ten years behind. Are you confident that's what we're doing here in Ottawa?

Ms. Helen McDonald: Yes, we are. We are not only trying to learn from the best companies, like Microsoft—we're avid users of their product—to make sure we're keeping on top with the patches and other security fixes, etc., but we're also trying to ensure that the private sector right across Canada increases its sharing of information with the government about risks. If we're a target, it's also because private sector firms are a target, and we can learn from each other about new threats or what worked.

We are also trying to adopt, where possible, international standards. We don't make them up. We try to use international standards because this is where considerable effort is spent internationally in getting the architectures right and making sure there's lots of software that fills that space.

Finally, we do import, through interchange, leading security practitioners in the private sector arena within Canada so we'll have that expertise available to us within government.

Mr. Brian Fitzpatrick: I'm short of time, but I really want to get another question in.

If by chance your systems fail and a department crashes or there's some major problem in that department, is there a plan B in place in these departments to deal with that matter? The only reason I raise it is that only 45% of your departments have even done a threat and risk assessment. If they haven't done that, I really question whether they have a contingency plan in place in case the system does crash. That would be the thing that comes to mind with me, and I'd be curious as to whether that's in place.

Ms. Helen McDonald: Certainly there were plans of that nature put in place for Y2K. More recently, we have required departments to have business continuity plans in place for just that eventuality.

The Chair: Do you have a comment, Mr. Timmins?

Mr. Douglas Timmins: It's just to add something. We do refer to the business continuity plans in our report, in paragraph 1.65, where we said 53 departments, 65%, had business continuity plans but only 24 of them, or 29%, had tested them in the last two years. There's progress, but we felt testing was an area that needed a little bit of work.

● (1630)

The Chair: Thank you very much, Mr. Fitzpatrick.

[*Translation*]

You have eight minutes, Mr. Sauvageau.

Mr. Benoît Sauvageau (Repentigny, BQ): Welcome, Madam, gentlemen.

I have several questions for you. First of all, I'd like you to shed some light on the whole issue of threats. If the system isn't secure, then it would seem to me that we're vulnerable to threats. Without giving away any secrets, could someone, either from Treasury Board or the Office of the Auditor General, tell us what kind of threats the Canadian public is facing because the system isn't secure? Could you be brief, because I do have several questions.

Mr. Simon Gauthier (Deputy Chief Information Officer, Treasury Board of Canada Secretariat): I can give you a brief answer.

The Canadian public faces numerous threats. Typically, they are the result of shortcomings in the design or implementation of the code or software.

Mr. Benoît Sauvageau: Can you give me an example of a threat? I know what a threat is. For example, is it possible for someone to wipe out all of their debts owing to Revenue Canada?

Mr. Simon Gauthier: No.

Mr. Benoît Sauvageau: I see. So then, give me an example of a threat.

Mr. Simon Gauthier: An example of a threat...

Mr. Benoît Sauvageau: This may not be a very good example, but I'll give it anyway. The Standing Committee on Government Operations heard from one witness who worked at the consulate in Hong Kong. He claimed that because the computer system wasn't secure, there was a possibility that passport or visa fraud could occur. This employee was fired for his comments. The RCMP conducted an investigated to ascertain the veracity of these allegations. The lead investigator for the RCMP proved that the claims were in fact true. He also ended up losing his job. The legislation to protect whistle-blowers was not in force at the time and still has not been enacted. The witness testified before the Government Operations committee that because the computer systems in the vast majority of embassies and consulates were not secure, passport and visa fraud was an ongoing possibility. Would this be one concrete example of a security threat?

Mr. Simon Gauthier: I can't answer that question.

Mr. Benoît Sauvageau: Perhaps the question is too specific.

Mr. Simon Gauthier: I really can't say, sir. I'm not aware of the incident. However, it's one example of a potential threat. Having said that, I think that in the case of most systems directly linked to the Internet — which is the source of these threats — steps have been taken over the past two years to minimize system vulnerabilities or shortcomings. I wouldn't go so far as to say that all problems have been eliminated, but at least they have been alleviated somewhat.

Mr. Benoît Sauvageau: If you received reports on a more regular basis, you would be in a position to state, not merely speculate, that the problem has in fact been corrected. For example, the Office of the Auditor General has stated that you do not receive reports often enough. You maintain that all, or part of the problems, have been corrected, as far as you know, but if you had a report, you would be able to state this with conviction.

If you have no objections, I'd like to ask Ms. McDonald if , considering that 20 out of approximately 80 departments have plans of this nature in place, the lack of a framework or of monitoring procedures puts the passport and visa systems in grave jeopardy. Does this mean that someone could easily tamper with the computer system without fear of reprisals?

[*English*]

Ms. Helen McDonald: I can't respond directly on the passport system. On incident reporting, it's less important for it to come to Treasury Board Secretariat. It's more important that the community of IT security coordinators knows immediately when something has happened or when there's a new virus or computer threat of this nature, and that corrective action is taken.

I think the Auditor General was looking for Treasury Board Secretariat to have more effective monitoring of the progress in the implementation of the government's security policy and the IT security standard. That's the kind of thing we will be improving with the reporting by departments on their action plans to correct the IT security gaps that they have identified within their departments.

[*Translation*]

Mr. Benoît Sauvageau: I wasn't attacking you personally, Madam. Let me use a pseudonym. I'll talk about the Department of Optimism. I also served on the Standing Committee on Official Languages. The Treasury Board Secretariat, the body with oversight responsibility, is optimistic. It is very hopeful that the situation will improve in time. You're optimistic as well. You also believe things will improve. In that case, why weren't the action plans implemented in the past, as they were supposed to be? Perhaps that would have curbed your enthusiasm somewhat, but perhaps it would also have improved the effectiveness of procedures.

I had prepared many questions. There were others I wanted to ask, but this one was drafted with considerable care.

Paragraph 12 of Mr. Timmins' presentation contains four questions. If someone were to put these questions to you, how would you respond? Do you what these questions are?

● (1635)

[*English*]

Ms. Helen McDonald: Yes, I do.

What would be the assurance of an appropriate pace of development for IT standards? We are proposing that all of them be complete by December 2006 at the latest. We have a plan in place that says that, month by month, these are the twelve standards that are needed, that are remaining to us. We have three in draft that have been circulated, and we have a plan for how fast that will go.

How do we ensure that departments are actually implementing? We have been spending a lot of time lately trying to ensure that the standards that we do put in place are also accompanied by appropriate guidance to departments. You don't just put them up on your website. You want to work with the communities to make sure they're aware of these requirements and understand these requirements, and to try to understand what tools they might need across the government to help them in being effective.

At the senior levels, we need to promote awareness of the importance of IT. Perhaps my optimism comes because I think every deputy minister in town is concerned about continuity of operations and is conscious of the fact that so much of what we do is now on IT systems. They may not read that as security, they may read that as integrity or they may call it the integrity of their operations, but I think they're very concerned about it. We are therefore asking that the deputy ministers sign off on these action plans in the fall—not just the DSOs, but the deputy ministers—so that they are aware of where their strengths and weaknesses are in IT security, what they're going to do, and what timeframe they're going to improve them in.

In terms of oversight, we've asked for these action plans to be in by August, and we've been working with departments to make sure they understand this. They're starting to get ready for this, and we will be reviewing those and providing a report to the secretary at the end of the calendar year. In the next year, 2006, we're contemplating getting them to redo the IT self-assessment so that we can not only see what the change has been, but also to update their action plans so that we can both assess the progress that has been made and what still remains to be done. We will be taking this information and putting it together with other sources, such as vulnerability assessments, in much the way the Auditor General's audit is done, and we will be providing this material to Treasury Board in early 2007.

As you may know, the security policy is under a five-year mandatory review. Before that, one would have to know how effective we have been in implementing it. And on the mid-term review, May.

The Chair: Merci, Monsieur Sauvageau.

Mr. Lastewka, please, for eight minutes.

Hon. Walt Lastewka: Thank you, Mr. Chairman, and thank you, witnesses, for being with us today.

I'm going to take a three-phase approach.

Ms. McDonald, you've been acting chief information officer for how long now?

Ms. Helen McDonald: I've held the position since May.

Hon. Walt Lastewka: Who was before you?

Ms. Helen McDonald: Michelle d'Auray.

Hon. Walt Lastewka: I wanted to find out some of the whys. Why is it that only one department met the baseline requirements? I want to go back now to what Mr. Fitzpatrick was saying. Why was it only the one department? Was there a lack of concern, lack of understanding, lack of communication? Give me the whys—why was there only one department?

Ms. Helen McDonald: The management of information technology security standard set the baseline. This is the minimum requirement that all departments and agencies must meet. Because it took up what we had thought was going to be almost 44 separate standards, it's a fairly complex set of requirements covering physical security, personnel security—sorry, I'm talking MITS. It's focused on the IT security, but it covers off what you would need to do in terms of access to systems, protection of information, the use of specialized technologies, etc.

This only came out last year. It was approved in May 2004. I believe the audit was about to start around that time. So departments had this clarification—this is exactly what we're looking for—about the same time that the auditors went out.

When we had it approved, we told departments they had until 2006 to put it into play. So of the 46 departments who fed information to us, you found one indicating it was fully compliant with all aspects of the MITS standard. It's not lack of concern or lack of interest. It's more that we have a new standard now, and people are working their way towards it.

● (1640)

Hon. Walt Lastewka: Okay. I'm not sure I'm going to buy that. I'm really concerned. We, as members of Parliament, look to the Treasury Board Secretariat as the example-setter for other departments, and when I see a comment made that it "has not completely fulfilled its oversight role as defined in the policy," I have a real concern that this is written this way.

When it says "The Secretariat also has notcompleted the mid-term report to the Treasury Board on how effectivethe Government Security Policy is in strengthening security", was the Treasury Board lax in not maintaining or not going after the secretariat, number one? Number two, was the report that was due in the summer of 2004 ever done?

Ms. Helen McDonald: The mid-term report that's referred to was originally to be done by the summer of 2004. It is this report I'm referring to that will be done by May 2005.

Yes, we are running late on that report. We wanted to make sure that we had the necessary standards in place, helped departments understand how they would implement them, and received information from them on what their baselines are now. So the baseline we have is really a bit of a starting point with respect to the 2004 management of information technology security standard.

Hon. Walt Lastewka: You mention in your report that this report will be done no later than the summer of 2005. Is that correct? We have small departments and larger departments and so forth. How many of the departments have already completed their reports and had them signed off by their deputy ministers?

Ms. Helen McDonald: I don't expect any of them have signed off. We're looking for an August action plan; we wouldn't expect to get them before August.

Hon. Walt Lastewka: So if we have you back in September or October, are we going to hear that they're not signed off yet? What I'm seeing is we've moved out the deadline; we didn't fulfill our oversight rule; we've given them time until August. Does this mean that everybody is going to sign off in August?

Ms. Helen McDonald: I'm going to complete the mid-term report irrespective of the action plans. I don't want to delay it; I'd like to get the report out. The action plans will be coming in through the summer, and we're proposing August as a deadline. The formal call letter has not gone out.

I want those action plans in because that is our best source of information on how people are going to bridge the gap between where they are and where they need to be. We have been working very closely with other line departments and agencies to make sure they understand the requirements of the action plan, and they've got the capacity to complete it. We will be using both my office and the Secretary of the Treasury Board to stress the importance of the completion of these action plans.

Hon. Walt Lastewka: I'm getting the feeling that the Treasury Board Secretariat has to persuade deputy ministers to understand the risk and get their job done. What forceful hammer do you have over them to make sure it's done? You can't use persuasion on this; it's too serious. What mechanism do you use to make sure that come October, when we've asked you to come back, it's done?

● (1645)

Ms. Helen McDonald: If a department or agency wishes to avail themselves of the secure channel offerings, they have to certify and accredit that their systems are compliant with the IT security best practices. So that covers off a portion of it. We certainly do rely on deputy-to-deputy pressure, if you like. We have been thinking about whether a score card would also be helpful in showing deputies where they rank relative to other departments, as a way of trying to provoke more rapid action among perhaps the more laggard.

Another way we can help them, rather than just beat them up, is to continue to put stress on common IT services that can provide, particularly for smaller agencies, a much higher level of security than they would otherwise be able to afford. If we can provide network protection, perimeter protection, and intrusion detection services once at a whole-of-government level, that's certainly going to help increase the level of security.

The Chair: Thank you very much, Mr. Lastewka.

Mr. Christopherson is next, please, for eight minutes.

Mr. David Christopherson (Hamilton Centre, NDP): Thank you, Mr. Chair, and thank you all for taking the time to be here today.

I am also sort of struck by your comments, Ms. McDonald, regarding your optimism, especially when we look at some of the language that's been used by the Auditor General. There's a real disconnect between what's been reported to us as having been done, versus the positive attitude you're reflecting.

Let's also put this in context. This is a huge issue. I'm surprised that things have been as tame as they've been so far. This is incredibly crucial to just about every aspect of governance, shot right through.

For the record, I'd just like to read a paragraph that the Auditor General has in her report. She says:

> A general lack of concern for IT security risks leaves systems vulnerable, where weaknesses could be exploited. As a result, sensitive data, including information on the privacy of Canadians, payroll and financial transactions, program information, and other mission-critical data are at increased risk of unauthorized disclosure, modification, or loss—possibly without being detected.

The only thing worse than having our systems breached is not even knowing about it. That could go on for who knows how long. Let's underscore the absolutely critical importance of getting this right. It's disappointing that the government doesn't seem to have made this the priority it should have.

Again reading directly from the Auditor General's report, on page 5 of the document we're working from there are a few paragraphs. Let me start at the second one—and this is juxtaposed against your optimism, Ms. McDonald:

> Overall, however, the government has made unsatisfactory progress in strengthening IT security. Two and a half years after revising its Government Security Policy, it still has much work remaining to translate policies and standards into consistent, cost-effective practices that will result in more secure IT.

IT systems in departments and agencies continue to be vulnerable to breaches in security. Unless somebody on this panel representing one of the ministries wants to come forward to refute this, that's pretty damning and alarming.

> Vulnerability assessments, conducted in departments and agencies over the last two years, have revealed significant weaknesses that, if exploited, could result in serious damage to government information systems.

Let's remember this is the second go-round. It's not the first time. It's not like you have the excuse of starting something new and it takes a while. We've been at this for some time.

The last paragraph on page 5 says:

> I am concerned that members of senior management are not aware of the risks to IT security in their departments and do not understand how breaches of IT security could affect their operations and the federal government's credibility.

That takes me directly to page 12, where there's a box at the bottom of the page that reads in part:

> The Government Security Policy and its related operational standards require that departments and agencies certify and accredit any new or modified system or application before it is used.

Jumping down to the second paragraph:

> However, IT security is not always taken into consideration at the start of the project.

I read that to mean in reviewing the model.

> In addition, the risk of failing to meet IT security requirements is increased because senior management, as the project review committee, has not met in over a year.

But you still maintain you're very optimistic, Ms. McDonald.

The last sentence in there says:

> Fisheries and Oceans Canada and the National Parole Board have yet to comply with this requirement.

I'm sorry, but what I'm seeing here does not square with optimism on the part of the government, and saying that they take this as a serious matter.

Could you please comment on whether or not senior management takes this issue seriously? According to the Auditor General—in black and white in front of us—they don't.

● (1650)

Ms. Helen McDonald: I would not want my optimism to be confused with.... Let's be realistic. We agree with what the Auditor General has said. We agree that we are not following the standards to the extent we should be. I am optimistic that even the Auditor General is seeing some signs of progress. I am optimistic that some of the things I've been talking about today on the filing of action plans, the review by Treasury Board, will help focus more attention on this. But I have to agree we need to do a better job in getting senior management to understand the issue and therefore care about the issue. That's why I referred a bit to whether we have been successful enough in putting it in terms that senior managers, deputy ministers, are going to understand. I think they see security as something that's added after the fact.

We are trying to get people to understand that when you start thinking about a system you have to look at the IT security, and you have to embed it at the outset. That's why we have an architecture program to try to help departments understand how to build in good security when they configure or think about their systems, when they do the designs, and not retrospectively after the fact. We don't want breaches.

Mr. David Christopherson: Well, I have to tell you, it's all well and fine that you're hoping, wishing, and praying and that everybody is clicking their heels three times and wants to go back to Kansas, but in the real world it's not going to happen unless somebody does something about it. I'm sorry, but that's not satisfactory. It would maybe have been acceptable some time earlier on, but not now, not at this stage, not with what's going on in the world, and not with a damning report like this. It says in this report senior officials don't take this seriously enough, and then you tell me you're hoping and you want to persuade them.

You almost started, I think, to put the question back to me as to how we should go about this. That's the question we put to you.

I want to take another example, on page 18, under “Monitoring security practices in departments”. Here we go again: “In the four departments we examined, practices for monitoring IT security varied from unsatisfactory”—that was the high mark—“to non-existent”.

We have to start getting reports that don't inflame the members of the committee the way these do, because as much as we laugh and have a few chuckles, this is pretty damned serious. What we're getting now is a second report from the Auditor General saying it's not up to speed. This is not good enough. I'm not hearing anything, Ms. McDonald, from you or anybody else that satisfies me that this government is taking this seriously or that you're even in a position to do something about it.

If you walked out of here with a resolute determination you were going to make this happen because it's clear now that Parliament is serious about this issue, what would you do differently than you're doing right now?

Ms. Helen McDonald: I'm not sure I would do things differently, and I do have a determination and a resolution to get this fixed. Let's recognize that it's not just the Treasury Board Secretariat that provides IT security; it is also each department in playing their role and each deputy minister in deciding this is important.

The encouraging signs are that there is progress being made. We have clarity. We have a bit of a baseline now as to what the state of play is, which we didn't have a couple of years ago. The audit did not look at things like the role of the secure channel or the provision of common services. It did not look at the increased ability to share incident information across the government.

We have not had a major breach within the government of Canada. Yes, we would know—

● (1655)

Mr. David Christopherson: That you know of.

Ms. Helen McDonald: I think we would know of any.

Mr. David Christopherson: Well, one of the concerns the AG had was that you wouldn't know.

The Chair: Thank you very much.

I just would like to make the comment that I remember, when we were dealing with Y2K about 1997 or 1998, maybe 1996, that the problem we identified then was that the Treasury Board, which was in charge of making sure Y2K would not be a catastrophe, couldn't get the departments to buy in because the Treasury Board wouldn't insist that they get the job done.

I'm hearing the same thing again, that while you have the roles, the oversight, the checking, and so on, these deputy ministers seem to be masters of their own destiny. If they don't follow up, there is no penalty for them. This is now six, seven, or eight years later and we hear this in other agendas, where the Treasury Board, the central manager of government, doesn't compel departments to get the job done even though, as Mr. Christopherson has pointed out, there could be serious problems and issues that would arise from that.

Mr. Allison, eight minutes, please.

Mr. Dean Allison (Niagara West—Glanbrook, CPC): Thank you, Mr. Chair, and thank you, witnesses, for showing up.

David read my original paragraph I wanted to read, so I won't read that back in. I have two lines of thought, though, I would like to look at. One is identity theft and the second is the whole issue of responsibility in departments: who's responsible or accountable at the end of the day?

My concern with identity theft is that, as we know, in the U.S. and around North America it's so easy now to get access to people's information. We also understand that the damage done to individuals is irreparable, whether it's financial, it's to their reputation, or whatever the case.

The challenge I have is that as a government, you guys are the largest and you possess the most personal information on anyone of any organization, any outlet, or any company in Canada, and I may even go so far as to say in North America. What guarantees can you give us, given the fact that we have breaches and we're not even sure if people are accessing our data or information, that Canadians' personal data is safe and that when they communicate with you guys over the Internet, as is happening more and more, it is secure? What kinds of guarantees can you offer Canadians?

Ms. Helen McDonald: It's that we know who you are, that we have the right person, and that we're able to establish, without doubt, your identity. That's why a lot of thinking went into how we can effectively deal with Canadians or businesses when they appear to us over the Internet, when they want to deal with us online.

How do you know who HelenMcDonald@hotmail is? What we do is we require a series of shared secrets that are between you and the department, based on your history with the department. In those cases, our threat risk assessment says we can establish your identity to our needs, based on these multiple shared secrets.

In other instances, you might not have a relationship pre-established with a government department. That's where it becomes a little trickier, where we would need a face-to-face, where you would bring in some original documents, perhaps, so we could establish who you are.

As you're probably aware, identity is kind of a chain, where you get something—a SIN, a driver's licence, or this or that. What the federal government has been looking at, with the provinces and territories, is that chain of trust. Are we handing out, based on a library card, something much more serious than that? How can we be sure that the base documents that establish identity go through an appropriate process in all jurisdictions and that they can be trusted? How can we assure ourselves that when someone born in one province dies in another province, we understand that the person has died and that identity cannot be reused?

That's a big effort that we have been pursuing for the last few years, to try to reduce the possibility of identity theft through our interactions with citizens or businesses. We have a lot of silos between programs and departments. The silos actually protect your information, because you can prevent people from seeing it. You can control access to it. But we're also trying to balance that with value for money. Is it possible to have more effective, more efficient government operations where you share information across program silos, if you like?

So it's cheaper. Perhaps it's easier on the client who doesn't have to keep repeating the same information. But you want to do that in a way that both respects the privacy rights of Canadians and doesn't increase the security risk of having this information floating around. That's why we use things like public key infrastructure to protect information as it transits around and why we're looking at ways of ensuring that each piece of data, almost, has the appropriate privacy and security protection associated with that piece of data no matter where it might go.

● (1700)

Mr. Dean Allison: That's fair enough. I guess what I'm more concerned about is whether the networks are secure.

I look at paragraph 1.55 in the Auditor General's report, which says:

> Networks were not secure. Networks are interconnected devices and software that allow individuals to share data and computer programs. Sensitive programs and data are stored and transmitted on networks. For this reason, networks must be made secure against unauthorized access—

That's really where my concern is, the unauthorized access, not the normal person popping into there.

> —manipulation and use by outsiders. Organizations can secure their networks by limiting the services that are available and installing devices that deny unauthorized requests for access to services and data.

In my mind, securing networks is a pretty basic function. It says here, "Networks were not secure," and there were inadequate network access controls. So these are things that are not the normal everyday person moving through for data, but the back-door approach, which is what I'm really concerned about. It's not the systems up front that you're putting in, which seem to make sense; it's the back-door approaches and the quick fixes.

In 1999, a project tested the level of cyber threat to federal government Internet space. It lasted three months and generated more than 80,000 alarms and over 500 attempts to penetrate department systems. Have more tests been done?

Ms. Helen McDonald: Have more tests been done to...?

Mr. Dean Allison: Have more tests been done to find out what type of cyber threat we have with our Internet space?

Ms. Helen McDonald: We continue to do them all the time and continue to report on them. It's probably something that Mr. Gauthier can expand in a little more detail.

Protecting the back ends, which was where your original question was coming from, is also absolutely essential. What we have to look at is not just the threat from outside, but the threat from inside, that employees who don't have the right to see that information or access that database don't, that we have audit trails and can tell who went in and who didn't.

We have to make sure that the information isn't changed through some malicious wayward employee or rogue attack as well, because we have to ensure that one can have faith in the transactions we have, from both sides, that we have an audit trail such that no one can deny that the transaction took place. That's why we're increasingly using technologies like public key infrastructure, because they provide those assurances. That has to be coupled with the security of personnel screening, the physical use of passwords, things like that, the sequestering of data, and so on.

Yes, absolutely, all these things have to go together. Are we perfect yet? No.

The Chair: One minute, Mr. Allison.

Mr. Dean Allison: Okay.

What I probably should have talked to first—Mr. Christopherson talked about this, as did Mr. Lastewka—was the whole issue of responsibility. At the end of the day, it doesn't sound to me like you do have the hammer to make things happen in your department. We have obviously the Treasury Board Secretariat looking after it, plus other agencies.

What can be done? What is your recommendation so that someone is responsible at the end of the day, and we can go to someone and ask why these departments are not up to speed, and why the reports are not filled in? Who is going to face the music when this is not done correctly? My concern is that at the end of the day, we're going to have a major catastrophe in terms of that, and everyone will just start pointing their fingers, saying, as we've heard before, “It wasn't my fault”.

So what is your suggestion?

Ms. Helen McDonald: I have two suggestions. The government security policy in 2002 required that IT systems be certified as compliant with good IT security. This means that someone within the department has to run it through this checklist and say, this is how we can prove that we are compliant with good IT security practices. The business owner has to sign off on that and accept all residual risk. It's a piece of paper. They're signing it. There's an accountability there.

As CIO, I do the same thing; I accredit all the common infrastructure, the common IT systems, that cut across all departmental lines. That again is something I'm putting my signature to. I'm accepting residual risk. And I'm only going to do that if I'm reassured that the system itself is following the best IT security practices.

I think that's one way of doing it. I can't say that all systems have been certified and accredited. That's a process that's starting. Certainly all the new ones are.

I think on the notion of a scorecard—and maybe you have advice on this—if we can get to what dimensions we're looking for in departments, is there merit in having almost a dashboard that shows senior managers, “This is where you are, and you're not looking that good”? I think you've got to be able to point out where you are and where you need to go.

● (1705)

The Chair: Mr. Timmins, do you have something to add?

Mr. Douglas Timmins: Yes, Mr. Chair.

I think Ms. McDonald said earlier that the deputy ministers are the ones who are ultimately accountable. Part of the package of getting them to recognize the risk of IT and the risk profile of their overall department...because they have other priorities they worry about. So efforts to move it in that direction, including getting them to sign off on the action plans, are all steps that I think are positive in terms of getting that accountability.

I just wanted to add that.

The Chair: Thank you very much.

Mr. Murphy, please, eight minutes.

Hon. Shawn Murphy (Charlottetown, Lib.): Thank you very much, Mr. Chairman, and thank you to the witnesses for appearing today.

I just want to follow up on that last point, Ms. McDonald. In a normal line department, which person—and I know the answer may be that the deputy minister is ultimately responsible—would be responsible for this function in the line department? Would that be at the associate deputy minister level, or would that be under the finance end of it?

Ms. Helen McDonald: The departmental security officer.

Hon. Shawn Murphy: So every line department would have a departmental security officer. Would that person normally answer directly to the deputy or to the associate deputy minister?

Mr. Simon Gauthier: Perhaps I can answer.

It does vary for departments, but all departments do have a DSO. They also have an ITSC, an IT security coordinator. Yes, they do eventually report to the deputy minister, but it does vary among departments.

Hon. Shawn Murphy: Again, on the whole issue of responsibility, let's say there is—and obviously there is—a line department out there that is delinquent or just not up to scratch, or that hasn't got its systems in the state that you think they should be. What levers do you have at your disposal there? And I hope it's more than persuasion.

Ms. Helen McDonald: We can refuse to let them connect to the secure channel.

Hon. Shawn Murphy: Have you ever done that?

Ms. Helen McDonald: No. And I'm saying no.... The secure channel was completed relatively recently. Departments are starting to migrate to it. Perhaps it's the state of maturity.

I don't want to lose sight of the certification or accreditation. I also assume that we could stop new spending on IT projects where we felt the security was...or I'm sorry, I'm not assuming; we can stop IT spending on projects where the security is not properly reflected in the project design, because the larger projects come to the Treasury Board for approval. But that's not all of the projects that are done by a department, it's the larger projects above a certain authority level.

Hon. Shawn Murphy: And all the agencies, then, are under the same basic framework?

Ms. Helen McDonald: Most of them, I believe, but they may have different levels of signature.

Hon. Shawn Murphy: I guess my point, Ms. McDonald, is that it puts quite an onus on you and your department and your staff. Would it not be better to have a system similar to that seen in a lot of facets of life? You develop the checklist, you develop the standards, you develop what the requirements are, and the onus is on them to come forward on a quarterly or a semi-annual basis to provide you with a very clear, unequivocal certification that they are meeting every standard that you've set. It's similar to an airplane. Every six months or whatever an airplane goes through an inspection process, and if the airplane either doesn't go through the process or goes through the process and fails, then that airplane doesn't go off the ground. That's it; it stays with the airport.

Would it not make a better architecture if the system were...? And in a way it would lessen your work if the department or agency didn't go through this, and if they didn't provide you with the certificate signed by the departmental officer and the deputy that they've met all the standards. If they didn't do that, they basically would cease to operate, and this would have to come right from the very top, from the Clerk of the Privy Council.

You can see the point I'm making. You're taking the onus from your department and your staff and putting it in these 130 agencies and departments that they have to do it. If they don't do it, they cease to function.

● (1710)

Ms. Helen McDonald: That's what the certification and accreditation process is intended to do. Within the department for their own things that are unique or shared across one or two departments, they actually have to certify that it's good and someone has to accept that and sign off for that. Where we might consider using more of the audit tools is to look at how far that process is being done.

As I said, it's certainly hitting the new projects, but it's not back in time and it needs to be back in time. It's an aspect we're going to have to monitor, so we're not just focused on the new, but we also understand that the legacy systems have also got good IT built into them.

I think the other, the action plans being signed off by deputies, is also a way for them to recognize their accountability for improving or ensuring an adequate level of IT security.

Hon. Shawn Murphy: But you do think there's a risk that within a year's time when you appear before this committee again that you would still be pleading with some departments and some agencies to bring their standards up to what is required by both the Auditor General—and by yourself too, I should add?

Ms. Helen McDonald: I would suspect that the majority of the larger departments are actually making good progress. At least the assessments and the visits seem to suggest that the larger ones have a greater capacity to go there, and with the large tax and other databases they're certainly very concerned about privacy, security, and their reputation. People won't file taxes if there's a breach.

I think the problem is more with the smaller departments and agencies. I think looking at a common approach.... Why let smaller departments build or provide their own IT security, rather than saying let's have a more centralized approach to help the smaller ones, so you don't have to have in each of the smaller agencies the capacity to do it? We can have that done centrally and therefore raise the level of security across. So I think perhaps it's somewhat different solutions, depending on the nature of the problem, but I think it has to be a multifaceted approach; it can't be just persuasion.

Hon. Shawn Murphy: Thank you, Mr. Chairman.

The Chair: Thank you, Mr. Murphy.

Mr. Kramp, please. We're now into round two, so this will be five minutes.

Mr. Daryl Kramp: Thank you.

Thank you for coming here today. The one comment in particular I'd like to make follows around an old saying: you can't fix a problem if you can't identify the problem.

Of course, when I take a look at the Auditor General's report on the vulnerability assessments, mentioned by Mr. Fitzpatrick here earlier, 46 out of 82 departments have reported that they had completed some form of vulnerability assessment. This means that close to half of our departments don't even know if they have a problem. They could have a problem, but they don't even know, and I say to myself, well, how do we fix potential problems if we don't have the problem identified?

Now, why do they not have this problem identified? Why have they not put themselves into a position to at least be able to assess their capacity to react to a contingency situation? I ask you, is it one of three reasons: Is it either a lack of resources that they haven't done this, is it a lack of manpower that they haven't done this, or is it a lack of willpower that they haven't done it? Where does the fault lie?

● (1715)

Ms. Helen McDonald: Of the 82 departments, we had 46 who fed us their self-assessments in that timeframe. We have a number that came in later. The Auditor General's office went to the same 82 and got 82 self-assessments, plus some additional questions.

So I think we can say that all of those 82 departments have a pretty good sense now of what's wrong, because they have all completed the self-assessment with respect to the management of information and technology security standard.

Mr. Daryl Kramp: So you're confident they are at least aware there could be a problem?

Ms. Helen McDonald: They are aware of where the problems should be, and we expect to see that reflected in their action plans in late summer.

Mr. Daryl Kramp: Now, going back to another situation....

Mr. Timmins, you had a comment?

Mr. Douglas Timmins: I just wanted to clarify that we're talking about two different types of assessments. I think Ms. McDonald has responded to the self-assessment. I think Mr. Kramp's question was related to paragraph 151, where we refer to 46 departments that had completed vulnerability assessments—which is different from the self-assessment. I just wanted to make sure that the answer was to the right point.

We do have a chart that breaks down those 46. All of the six larger departments did do vulnerability assessments; so it is some of the smaller departments that are not doing vulnerability assessments.

Mr. Daryl Kramp: Okay.

I wanted to do a doomsday scenario. When we were preparing for Y2K, everybody jumped on the bandwagon and we were relatively ready across the board for Y2K, but all of a sudden it seems to have fallen off the radar screen now.

To echo Mr. Christopherson's concern, we have so many people in this country who depend on.... We're now an IT nation. For instance, if all of a sudden the cheques stopped going out, if somehow we had a glitch in the system and the cheques didn't go out for two or three weeks to a month, any person who relied on a social system would not have a cheque. We might say, “Well, we'll fix that”. Well, that isn't good enough for many people who live day to day, week to week, hand to mouth.

Do we have emergency backups? What kind of a fail-safe mechanism do you have? What kind of a safety assurance do we have that in the case of a worst-case scenario you have an alternative plan for us?

Ms. Helen McDonald: I can't speak for the HRSD or so on, but I know they have contingency plans to try to deal with not just a power breakdown, a malicious attack, or a strike, but plans to make sure that the essential services, the critical services, are continued in states of emergency.

Mr. Daryl Kramp: Have they stated that or have they registered those with you?

Ms. Helen McDonald: No, they have not registered those with me. We require them to be done.

Mr. Daryl Kramp: I would make a strong suggestion that you should have some type of validation, if such exists. Words alone don't pay the bills.

Mr. Simon Gauthier: If I may add, sir, as per the GSP or government security policy, we request that departments file with PSEPC. As per the national security policy, they are now the agency in charge of, I would use the word, “auditing” those business contingency plans.

The Chair: Thank you, Mr. Kramp.

Mr. Holland, please, for five minutes.

Mr. Mark Holland: Thank you, Mr. Chair.

Thank you to the witnesses.

I have a couple of things. First of all, I think there is an emergent theme, and that is the ability to force the deputy ministers into compliance or having a mechanism to more forcefully engage them in this particular process. Obviously, it is very serious, but I think we need context too. I need to understand some terms that are fairly relative in their nature. For example, when we talk about risk or significant risk, these are obviously very relative terms.

Obviously, the nature of technology is that it's vulnerable. Anybody who says that they have an invulnerable system only needs to wait a couple of months before a 16-year-old comes along and invents some work-around to attack it. The reality is that technology is ever-changing, it's vulnerable, and there are new holes being found. When we talk about the process and implementing the process today that Ms. McDonald said we wanted to do by 2006, obviously there also has to be an ongoing process, because this is an ever-changing environment and that's difficult.

It's also difficult for large organizations because you're dealing with a very complex and diverse IT system. You want to have the most robust protections that you possibly can, but implementing that protection across the board in a timely fashion can present a challenge with a large and complex organization.

There are really two questions that I have. I guess they're to Mr. Timmins because I need to understand this.

There are baseline regulations. We were also talking about international standards. Are those one and the same? What constitutes a significant risk? At what point do you draw the line, recognizing that really at any point, with any system, you could say that it's vulnerable and it's weak? Where do you draw the line such that we don't create a situation where people are unnecessarily worried but we are addressing a legitimate concern?

The other one is on the ongoing process of review and change. How do you see that being dealt with?

● (1720)

Mr. Douglas Timmins: Thank you.

On the issue of drawing the line or the baseline, as Ms. McDonald has said, we use the standards that were set by the government, by the Treasury Board, in government security policy and standards. I think we would require, we would expect, that the departments would do threat and risk or vulnerability assessments to know what they are on a fairly regular basis.

We weren't prejudging what those risks were. We know that those risks and threats exist. I would certainly agree that we would not have an expectation that you would eliminate all risk. That's not possible. We've said that in our chapter, and we are not expecting that, but it is an obligation, I think, to stay current and stay on top of that.

That's why we think that raising it on the radar screen of deputy ministers by integration into the overall risk profile gets back to questions on business continuity. Not in all departments would it be as essential to have services up and running in the event of a disaster or an attack as it would be for others, as we experienced in the planning for Y2K and as people experienced in the major power outage that we had a couple of years ago.

In our minds, it was not an expectation of having everything perfect and everything protected. It was more a matter of having a procedure and a process that would keep it current.

Mr. Mark Holland: Yes. Of course we know that other large organizations, particularly large corporations, also face similar concerns and have had security breaches. In fact, when we were dealing with a number of banks, there were a number of different areas. It's something that's inherently a risk with technology, and we want it to be as robust as possible.

The last question, Mr. Timmins, is this. In light of the comments, we now understand that baseline actually means the government-adapted standard. We heard Madam McDonald talk about seeing that embraced by 2006 and now maybe accelerating that for the larger departments, the ones that have the key security concerns. Are you satisfied with that progression if at the concurrence of this committee as well, maybe as an outcome of this process, we get some additional levers, if you will, to deal with deputy ministers to ensure that they embrace these changes more rapidly?

Mr. Douglas Timmins: We would certainly encourage earlier adaptation. There is the target of 2006. If we achieve that, it would be great. If we could achieve it earlier, that would be better. I think that a prioritization on the larger departments, getting an action plan and a commitment from them earlier, is certainly the right way to go.

Mr. Mark Holland: Thank you.

The Chair: Thank you very much, Mr. Holland.

We're going to wrap up here, but I have an observation, Ms. McDonald. In the chapter, the Auditor General has raised some serious concerns about the potential security breaches of our IT in the Government of Canada. You've heard the comments of the members who have been more than a little concerned about what seems to be a lack of attention by the departments, and by the deputies too, to ensuring that we are as secure as possible.

When I read your opening statement, apart from where you say “the Government of Canada fully subscribes to therecommendations of the Auditor General” and “the Auditor General's findings are consistent with our own ITsecurity self-assessment results”, you would never think there was any problem whatsoever. You don't acknowledge problems and you don't say you're addressing problems. Apart from these two allusions to the fact that, yes, you agree with the Auditor General, you make no reference to the seriousness of the issues raised by the Auditor General. I find this quite disconcerting, because you're not here to tell us how good things are, you're here to answer because the Auditor General has found some deficiencies.

I'm not going to ask you to really comment on that, but I am going to tell the clerk that when we ask future witnesses to come to this committee, we expect that they will acknowledge in their opening statements the issues raised by the Auditor General, and that they will speak to these issues raised by the Auditor General. We don't need some statement that all is wonderful. We want to deal with the problems identified. Therefore, I'm going to ask the clerk to make sure that witnesses coming before the committee from here on in are told that they will be expected to address the deficiencies raised by the Auditor General. That's what it's all about.

Mr. Timmins, do you have some closing comments?

● (1725)

Mr. Douglas Timmins: Mr. Chair, I would just reiterate that I'm very pleased that the committee has shown interest in this chapter. I just encourage the committee to keep an interest in this subject. We have some indications of plans of action over the next year or so. The committee may want to look at a way to make sure their implementation does actually take place.

The Chair: Thank you very much, ladies and gentlemen.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliamentary Internet Parlementaire at the following address:
Aussi disponible sur le réseau électronique « Parliamentary Internet Parlementaire » à l'adresse suivante :
http://www.parl.gc.ca
