House of Commons
Chambre des communes
CANADA

Standing Committee on Public Accounts

PACP • NUMBER 086 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, April 23, 2013

Chair

Mr. David Christopherson

Standing Committee on Public Accounts

Tuesday, April 23, 2013

● (1540)

[*English*]

The Chair (Mr. David Christopherson (Hamilton Centre, NDP)): I now declare this 86th meeting of the public accounts committee of the House of Commons to order.

On your behalf, colleagues, I welcome our guests today. We have quite a few affected by this chapter. They were good enough to be here, and we appreciate that.

First off, on behalf of all the members, may I extend our apologies. We had a ruling from the Speaker, followed by a vote, all of which had to happen before we could leave the chamber. Our apologies for keeping you waiting.

Unless there are any interventions to the contrary, we will begin with our usual procedures.

Just going by the order that's on my paper here, we'll start with the Auditor General's opening remarks. Then we'll move to Mr. Guimont. Then we'll move to the Treasury Board, to Communications Security Establishment Canada, and last but not least, to Shared Services Canada. Following that, we will begin the usual rotation. My sense is that we should be okay time-wise, but we'll continue to monitor that as we go through.

Unless there are concerns or questions to the contrary, I will now call on Mr. Ferguson, the Auditor General of Canada, to begin his opening remarks.

Mr. Ferguson, you have the floor, sir.

Mr. Michael Ferguson (Auditor General of Canada, Office of the Auditor General of Canada): Thank you.

[*Translation*]

Mr. Chair, thank you for inviting us to appear before the committee today to discuss our fall 2012 chapter on Protecting Canadian Infrastructure Against Cyber Threats.

I am accompanied by Wendy Loschiuk, assistant auditor general, and Tedd Wood, a recently retired principal, who was responsible for this audit.

Our work on this audit was completed in July 2012, so we cannot comment on actions that may have occurred since then.

[*English*]

Mr. Chair, much of the country's critical infrastructure is privately or provincially owned, but the federal government has an important role to play in helping to prevent attacks and reduce vulnerabilities. It has access to information sources that may not be available to infrastructure owners. It can collect and analyze threat information, and establish partnerships with stakeholders to help share that information.

In 1999 the Special Senate Committee on Security and Intelligence recommended that the government review its ability to, first, assess and reduce infrastructure vulnerabilities, and second, prevent or respond to physical and cyber-attacks. A federal task force was established in 2000 to advise ministers on protecting critical infrastructure. It found that a national strategy was needed. In 2001 the government stated that it would protect critical infrastructure by establishing partnerships and by monitoring and analyzing cyber-threats to federal systems.

Mr. Chair, we found that between 2001 and 2009 there had been limited progress in both those areas, despite the release of several policies and strategies, and recurring funding.

[*Translation*]

A key element of establishing partnerships was through sector networks. The government was to establish these networks and bring together key stakeholders by May 2011; some networks are in place, but there is still work to be done.

Of the 10 critical infrastructure sectors identified, only six had networks that included all the industry representatives who should be at the table, and only five had included cyber security in their discussions.

[*English*]

The government needs to have all the sector networks fully operational. We noted, for example, that the energy and utilities sector network is active and its members have a high degree of satisfaction and commitment to it. I believe this shows that networks can work and provide the government with a way to partner with stakeholders. The government has agreed to provide guidance on appropriate coverage for sector networks by December 2013.

[*Translation*]

In 2005, the government established the Canadian Cyber Incident Response Centre, which was intended to monitor and analyze cyber threats around the clock. However, this centre has never operated on a 24/7 basis as planned, nor are there plans to do so, although it has increased its operating hours since our audit.

[*English*]

We also found that the Cyber Incident Response Centre did not always have a full picture of the national and international cyber-threat environment because it was not always given timely or complete information. Without complete awareness of the cyber-threat environment, the centre's ability to analyze and provide advice on threats is limited. In some cases, critical infrastructure stakeholders were not aware of the centre or its role.

In its response to our recommendation, the government agreed to strengthen the centre's operational capacity and capabilities. Since 2010, with the release of the cyber-security strategy, the government has made progress. Shared Services Canada has been created to consolidate some of the government's information technology services. The government expects that this move will improve security. The IT incident management plan has clarified the roles and responsibilities of federal lead security agencies. There have been multi-industry and government forums, and a web-based information sharing portal has been set up.

However, one of the key challenges facing the government is the rapid pace at which cyber-threats evolve. In fact, officials raised concerns with us that the cyber-threat environment may be evolving faster than the government's ability to keep up with the changes.

● (1545)

[*Translation*]

We found that while there were policies and strategies for addressing cyber security concerns, Public Safety had not released action plans to identify priorities and timelines for keeping on track. Without these action plans, it was difficult to measure progress to see how well the government was able to keep pace with changing threats. In responding to our recommendation, Public Safety agreed to release an interdepartmental action plan for implementing its cyber security strategy.

Mr. Chair, this concludes my opening remarks. I would be happy to answer any questions the committee may have.

Thank you.

The Chair: Thank you, sir.

[*English*]

Thank you for that presentation. Before I move on, let me recognize that Mr. Reid is with us today replacing Mr. Williamson.

Welcome, sir. I hope you enjoy your time with us.

Mr. Scott Reid (Lanark—Frontenac—Lennox and Addington, CPC): Thank you.

The Chair: Thank you.

Monsieur Guimont, you have the floor, sir.

[*Translation*]

Mr. François Guimont (Deputy Minister, Department of Public Safety and Emergency Preparedness): Thank you, Mr. Chair.

[*English*]

l'm pleased to be here to discuss the progress made by Public Safety Canada regarding chapter 3 of the 2012 Fall Report of the Auditor General of Canada.

[*Translation*]

Joining me are:

From Public Safety Canada, Lynda Clairmont, senior assistant deputy minister of the National Security Branch, and Robert Gordon, special advisor from Cyber Security.

From Shared Services Canada, Benoît Long, senior assistant deputy minister of Transportation, Service Strategy and Design.

From Communications Security Establishment Canada, Toni Moffa, deputy chief of Information Technology Security, and Scott Jones, acting director general of Cyber Defence.

[*English*]

From the Treasury Board Secretariat, as you noted, we have Corinne Charette, chief information officer, and Colleen D'Iorio, executive director of identity management and security.

Mr. Chair, I welcome the Auditor General's report, which included a number of important recommendations on how to keep our cyber-networks secure both within and outside government .

[*Translation*]

Since October, my department has made great progress and, today, I am tabling a management action plan that outlines our next steps.

[*English*]

Mr. Chair, cyber-security is a shared responsibility of all government departments and agencies at all levels, of international allies, of industry partners, and of individual Canadians.

We can only keep our networks resilient and secure through an integrated approach, as established in Canada's cyber-security strategy. The strategy comprises three pillars: securing government systems, partnering to secure vital cyber-systems outside the government, and helping Canadians stay safe online.

[*Translation*]

The federal government has backed this strategy with significant funding—a $90-million investment at its launch, and just recently, an additional $155 million over five years to further address the evolving cyber threat.

[*English*]

I will use the first two pillars of the strategy as guideposts as I discuss our progress on the Auditor General's report.

Related to the first pillar, the Auditor General asked Public Safety Canada to develop a public action plan with deliverables and timelines for our strategy. I am pleased to say that this plan has now been developed and was released last week. It sets out an active partnership-based approach to help us communicate our progress more clearly to Canadians and underscores the need for all Canadians and owners and operators of vital systems to do their part. Furthermore, we have developed a horizontal performance measurement strategy with key departments and agencies, which will help us track our progress in the coming months and years.

● (1550)

[*Translation*]

Related to the second pillar—that of securing vital systems networks outside the federal government—the Auditor General recommended that we bolster the capacity of the Canadian Cyber Incident Response Centre…

[*English*]

The Chair: Excuse me.

Could you slow down a tad for the interpreters, please?

Mr. François Guimont: Yes, for sure, I'll slow down.

[*Translation*]

The CCRIC, our centre…

[*English*]

provides advice and support, and coordinates information sharing and incident response to cyber-threats on systems outside the federal government.

Since last October, CCIRC has among other things done the following. It has implemented a national cyber-threat notification system to provide automatic notifications of cyber-incidents to owners and operators of vital cyber-systems. It has improved dialogue with its partners through information and tools on its website, including establishing an online community portal; and finally, it has expanded its operational hours to 15 hours a day, seven days a week, with on-site coverage, to cover the full business operating hours of its clients.

Through a new telephone system, CCIRC personnel are directly accessible 24 hours a day, seven days a week, to serve its public and private sector partners. It's worth noting that since initiating the 15-7 operations in November, CCIRC has not received any call outside that timeframe.

[*Translation*]

Mr. Chair, looking ahead at the coming months, we will continue to strengthen engagement with provincial and territorial deputy ministers, and increase our meetings with critical infrastructure sectors to raise awareness of the cyber threat.

[*English*]

Finally, we will continue to work closely with our counterparts in Australia, the U.K., New Zealand, and the United States to share policy and operational responses to cyber-security concerns.

With that, Mr. Chair, I thank you for your time. I look forward to your questions.

The Chair: Thank you.

We'll move over to Madame Charette.

Ms. Corinne Charette (Chief Information Officer, Treasury Board Secretariat): Mr. Chair, good afternoon.

I'm pleased to be here to report on progress made by the Treasury Board of Canada Secretariat regarding chapter 3 of the 2012 Fall Report of the Auditor General of Canada.

As Deputy Minister Guimont indicated in his remarks, cyber-security is a shared responsibility. As chief information officer of the Government of Canada, I am committed to ensuring that the secretariat does its part to protect federal information systems against the ever-evolving cyber-threat. In the fall 2012 report, the Auditor General asked TBS to update relevant policies and plans to reflect the new information technology security roles and responsibilities of Shared Services Canada.

I am pleased to say that we have already updated the information technology incident management plan—the IT IMP—to define the roles of SSC with respect to incident management, and we continue to improve this plan on an ongoing basis. We are currently refreshing our security policy suite to embed the roles and responsibilities of SSC. This refreshed suite remains on target to be published later this year.

[*Translation*]

The Auditor General also noted that TBS had placed a renewed emphasis on increasing awareness of best practices for IT security across government. These efforts have led to the development of a security awareness training program that will provide all government employees with a standardized foundation of security principles.

Going forward, we will continue to work with our partners and support the security community, focusing on setting a common government-wide direction for security, establishing key security priorities and leading coordinated efforts to strengthen our collective security posture.

Thank you for your time, Mr. Chair. I would be pleased to answer any questions from the committee.

● (1555)

The Chair: Thank you very much.

[*English*]

We'll move to Madame Moffa. You have the floor, ma'am.

[*Translation*]

Ms. Toni Moffa (Deputy Chief, IT Security, Communications Security Establishment Canada): Thank you.

Good afternoon.

[*English*]

As part of its IT security mandate, CSEC provides advice, guidance, and services on the protection of electronic information and information infrastructures of importance to the government. CSEC also produces intelligence on foreign cyber-threats. We share this cyber-threat information and mitigation advice with Public Safety as well, for further dissemination to other levels of government and the private sector, as appropriate.

In his report, the Auditor General expressed concern that CSEC was not consistently providing the Canadian Cyber Incident Response Centre at Public Safety with timely and complete information about threats to Government of Canada information systems. CSEC and CCIRC have developed a close relationship, and at the time of the audit, adequate, secure communications for the transmission of classified information were lacking.

We have bridged this gap and we have also integrated a CCIRC official into our cyber-threat evaluation centre two days a week. We have added not only secure voice communications capacity but more easily accessible secure computer communications on their presence.

The report also referred to funding that CSEC has received since 2001. CSEC has invested some of this funding in activities to improve what we produce on intelligence on foreign cyber-threats. We've improved our detection, analysis, and mitigation of cyber-threats on federal systems. We are developing training for federal practitioners who need to respond to cyber-threats. With our colleagues from Treasury Board and Shared Services, we are designing and developing secure architectures for federal systems. These funds were also used to improve our overall program capacity, which supports all of our mandate activities, including but not exclusively, cyber-security.

While much of the information we produce is highly classified, CSEC continually seeks opportunities to share threat information and IT security advice and guidance beyond the federal government.

[*Translation*]

Thank you for your attention, and I am happy to answer any questions you may have.

The Chair: Thank you very much.

[*English*]

We'll move to Monsieur Long. You have the floor, sir.

[*Translation*]

Mr. Benoît Long (Senior Assistant Deputy Minister, Transformation, Service Strategy and Design Branch, Shared Services Canada): Thank you very much, Mr. Chair.

[*English*]

I am pleased to be here to report on progress made by Shared Services Canada in the context of the Auditor General's report, released last October, on protecting Canadian critical infrastructure against cyber-threats.

Shared Services Canada was created on August 4, 2011, with the mandate to consolidate and modernize the IT infrastructure of the Government of Canada, including enhancing the security and safety of the digital infrastructure supporting the government's own systems, particularly with respect to e-mail, data centres, and networks.

Shared Services Canada's new and evolving role is consistent with the Auditor General's recommendations with respect to the security of IT infrastructure. The integrity of the Government of Canada's critical IT infrastructure is a priority for Shared Services Canada.

[*Translation*]

Shared Services Canada plays a key role with four facets.

First, it prevents cyber threats by using trusted infrastructure products and services, by enhancing security by design, and through security awareness and training.

Second, it detects cyber threats and unwarranted intrusions into government networks through real time, government-wide monitoring, detection, identification, prioritization and reporting of incidents. This would include forensics, log analysis and investigations, as well as security and vulnerability assessments.

Third, it responds and coordinates responses to cyber and IT security incidents, including through remediation, threat assessments, communications, post incident analysis and reconfigurations and replacements.

Lastly, it recovers through rapid and effective restoration of services using specialized IT security incident recovery services, mitigation advice and guidance, as well as vulnerability remediation.

[*English*]

As mentioned in the Auditor General's report, we are working with officials in the Treasury Board Secretariat to address the recommendations included in the audit, including revisions to the policy on government security to incorporate Shared Services Canada's new IT security roles and responsibilities.

Shared Services Canada is also enhancing the federal Information Protection Centre for its 43 departments, which will give them access to a centralized 24-7 centre with better recovery capabilities and a specialized IT security incident recovery team. As part of this work, we are establishing a cyber-asset recall system as well as updating security provisions for the procurement of products and services.

Finally, Shared Services Canada works extensively with partner departments and agencies, at both the planning and an operational level, to ensure continued efficient, high-quality, and secure IT service delivery to Canadians.

● (1600)

[*Translation*]

Mr. Chair, I will be pleased to answer any questions committee members may have.

The Chair: Thank you very much.

[*English*]

That ends our opening remarks.

Now, colleagues, we'll begin the speaking rotation in the usual fashion, beginning with Mr. Saxton.

You, sir, now have the floor.

Mr. Andrew Saxton (North Vancouver, CPC): Thank you, Chair.

Thanks to our witnesses for being here today. My questions will be directed to the deputy minister of Public Safety and his officials.

My first question, Deputy Minister, is that the previous Liberal government did not have a cyber-security strategy in place. Can you explain when that was put in place?

Mr. François Guimont: Thank you for the question. The strategy was put forward in 2010 and it is a piece that in some ways reflects international approaches. So if one was to look at the Canadian cyber-strategy versus other nations that also had a strategy around the same time period, without being identical they have similar attributes.

Mr. Andrew Saxton: Thank you.

Can you explain the role of the Canadian Cyber Incident Response Centre?

Mr. François Guimont: The first point I would make, Mr. Chairman, is the centre, which is under our responsibility, is directed at issues on the outside. So if I were to compare that with CSEC, they deal with cyber-threats to the government systems and respond accordingly. CCIRC, our response centre, therefore deals with threats outside, private sector, provinces, territories. So at the macro level, that is the first one.

The second point is that it essentially has a responsibility to take on calls when they come, informed by people who are facing a cyber-attack. They will assist the company or the person in establishing what kind of a threat they are facing, what kind of a malware they may be facing. After that's done and they're trying to support and respond to the person in question, since they called to inform us and look for assistance, they will also, after doing triage and understanding, disseminate information for people who may be facing a similar malware to protect themselves. So they do carry out notifications.

If I remember, in 2012 they carried out something like 11,000 notifications very broadly. That's basically their function. They are also responsible for training, communication, partnerships, and as I mentioned in my remarks, we also have now a portal that provides them and people with access to either information or advice.

The last point I would make, if I remember, again in 2012, their website was used something like 227,000 times. So there are quite a number of interactions with people asking a number of questions. This is not necessarily only cyber-attacks but information of all sorts.

So those would be, in a nutshell, the functions of CCIRC.

Mr. Andrew Saxton: Thank you.

I understand there have been some questions with regard to their hours of operation. Could you explain the level of service that they provide to Canadians?

Mr. François Guimont: Thank you for the question.

Earlier on I mentioned that the cyber-strategy was put forward in 2010 with $90 million. When the Auditor General came forward with his report, a further injection of resources was made of $155 million over five years. About $13 million went to CCIRC to augment their capacity to not only respond to threats but also carry out their work. So they're now operating on a 15-hours-a-day, seven-days-a-week basis, physical presence. As I made reference to in my remarks, there's also a new phone capacity, which essentially implies that they are on call 24 hours a day. So a CCIRC official will be answering should there be a phone call outside the 15 hours, seven days a week, to handle the situation that may rise.

● (1605)

Mr. Andrew Saxton: Thank you.

I have a question for Shared Services Canada. Can you explain the role that Shared Services Canada plays in securing government systems?

Mr. Benoît Long: Shared Services Canada was recently created. Our primary mandate is to consolidate the existing infrastructure.

Today, as we manage the infrastructure and networks for 43 departments, our role is to monitor and to respond to any threats to that network. We work collaboratively with the security agencies in identifying any incoming threats. Our ability to respond is progressing and has been augmented through the strategy the government recently announced, including additional funding to provide a consolidated and centralized capacity to respond, as well as to extend our coverage to 24-7.

The Chair: Sorry. Time has expired, Mr. Saxton. Thank you.

We'll move to Mr. Allen. You have the floor, sir.

Mr. Malcolm Allen (Welland, NDP): Thank you, Mr. Chair.

Thank you to everyone for coming.

I feel as if I actually need a computer to track all of the places all of you go. I'm not quite sure how to track it. It would be nice to have a flow chart, actually, as to who does what, where, and who reports to whom. Quite frankly, all of your testimony quite clearly indicates there is a whole whack of you doing a whole whack of things—pardon the language—and I'm not so sure all of you are actually talking together anymore, but there's a whole whack of work being done.

Through you, Chair, if there's an overarching agency that actually has some sort of chart that shows who goes where, and who reports to whom, and what the systems are, it would be immensely helpful in tracking.

We know we have CCIRC and CSEC. We have Shared Services. We have another group over there, somewhere else. We have some engaged partners and some not engaged partners. Quite frankly, what I just heard of agencies that have bits here, bits there, in different departments, under different ministries, under different deputy ministers, and under different cabinet ministers is a bit of a mishmash, to be truthful. I don't see an overarching umbrella, with somebody holding the umbrella handle. Quite frankly, that's not encouraging, from my perspective.

Mr. Ferguson, what I think you were trying to indicate in your report was that we need cyber-security. It's an essential tool that's needed for government and for private sector. Somehow we need to have a managed system that works for both. I believe that's what the report was trying to indicate to us. I'm not so sure we have a system in which we actually have a sense of who's doing all of this.

I ask this question, Mr. Ferguson. You talked about CCIRC and the fact that the mandate was 24-7. Do you still believe that, sir, in the sense that we should still follow that mandate, or is that something you wouldn't be overly concerned with? We've heard from Mr. Guimont that we've increased the hours but not to where the mandate was.

Mr. Michael Ferguson: Thank you, Mr. Chair.

At the time of the audit, we noted that CCIRC's mandate was to operate 24-7. We noted it wasn't doing that at that time. Since then, we are aware that CCIRC's timeframe has been expanded.

What's important for us is that there be some way that, around the clock, incidents can be gathered so that the information can be acted on as quickly as possible. Whether that is the incident response centre having its doors open 24-7, or whether there are other ways of doing that, the fundamental issue is to make sure coverage is there 24-7, one way or another.

I can't give you any assurances about what's been done since the audit or whether the changes that have been put in place are effective that way. Certainly, for us, fundamentally what would be most important is that there is somebody who is available to collect the information around the clock.

Mr. Malcolm Allen: I noticed, Mr. Guimont, in your presentation you said we're up to 15 hours a day, seven days a week, which is an update from where the audit was. I suppose that's a positive. It's closer to 24 hours than the eight hours it was before. Then you're relying on a new telephone system, so that people are accessible 24 hours a day.

I hate to be naive about this and I'm not trying to be flippant, but that assumes you're awake by the telephone. If you're a heavy sleeper, you don't hear the telephone, and you're on call, what did we accomplish? I think the answer is self-evident: not much. I'll answer my own question.

The reality still is, sir, do you not believe that someone on active duty, not on-call duty...? Those are two different things. Being on call means you're available. I'm assuming the 15 hours are probably not the overnight hours, which are the on-call hours that people normally do. Are you saying to me that the on-call individuals are supposed to be awake at that time? Does that mean they're working that shift, looking at the phone to see if there is anybody contacting them?

● (1610)

Mr. François Guimont: Thank you for the question.

The first point I would make is that the 15-7 is meant to cover our time zones from coast to coast. That's the first point, if you were wondering why we picked up 15. The second point I would make is that we tried to strike a balance between good user resources and providing that responsive service. We felt that 15-7 plus 24-hour phone line accessibility did that. The third point I would briefly make is that in that period that we've now augmented our capacity, there hasn't been a phone call that came in that would have indicated to us that there's a challenge, so we haven't faced that situation.

I'm looking to my colleague here, but I'm not aware of any calls. Until it doesn't work, I would suggest that we're equipped right now to give a good response to calls, should they come in.

Mr. Malcolm Allen: We don't do that with fire services, sir. We don't put them on call. We actually put them in the station, not looking for the fire but being there just in case. I would suggest security threats, because they haven't happened, doesn't mean to say they won't happen.

The Chair: Thank you, Mr. Allen.

Mr. Malcolm Allen: It means we actually need to have someone there.

The Chair: Thank you, Mr. Allen. Time has expired.

We'll move to Mr. Kramp. You have the floor, sir.

Mr. Daryl Kramp (Prince Edward—Hastings, CPC): Thank you, Mr. Chair.

Once again, thank you to all of our witnesses for coming here today. The thing that has struck me, of course, is the entire difference in technology from 20 years ago to today. If you were to mention cyber-security 20 years ago, people would have blinked their eyes and asked what you were talking about. Now, with the global expansion of IT technology, etc., it really presents a whole different ball park in which, in my personal opinion, there's no way you can do the job alone. This is where the partnerships, quite frankly, for the public are absolutely critical as well.

My thought would be, recognizing that no man is an island in this matter, we need to have as much input as possible from areas that we've not even considered. Quite frankly, cyber reaches into every niche, corner, and cranny, potentially, on the globe. So we have to have buy-in from the public as well to aid and assist us with this.

Where can Canadians go to learn more about cyber-security, to alert them to the possibilities and the vehicle by which they can participate in solving some of our own problems? We have to be able to engage Canadians to assist. How do they do it?

Mr. François Guimont: Thank you for the question.

Mr. Chair, may I go back for a second to the earlier statement that things must have changed a lot in 20 years? When I was doing science and I was testing my abilities vis-à-vis my staff when they were briefing me on cyber-issues, I made reference to my having learned Fortran and APL. They shook their heads as if I were in a different world. Yes, things have changed a lot. I'm not even sure those languages exist anymore.

Going back more specifically to the question, the third pillar of our cyber-strategy deals with empowering Canadians to take the right action. I find in the question a very important statement to be understood. It goes back to the earlier question as well about rules and responsibilities. There are a lot of us around the table and there's a reason for this. We all have a piece of the action on cyber-safety, cyber-security. What's true in government is also true in our society. We need the private sector—big, small, medium—our colleagues from the provinces and territories, and we need each and every Canadian. The third pillar addresses that very point, and I think it's fair to say that we have a very active campaign on cyber-safety that speaks to each and every Canadian. In my words, "tricks" or things have been provided that they should be affording themselves.

Members of the committee will probably know, as a result of background, that 80% of Canadians are now online, either for business reasons or social reasons, so there is exposure there. The government is not there to do and tell them everything, so there is an empowerment component to the cyber-strategy that is quite important. We have a campaign and we have put money into that campaign, but at the end of the day it's for each and every Canadian to also assume their responsibilities, and rightly so.

● (1615)

Mr. Daryl Kramp: Thank you.

Engaging them is one thing, but how far do we go with this? The concern I have, of course, is that Eaton's doesn't tell Simpsons their business. We have a lot of people who with a tremendous amount of information could be more damaging, so we don't want to aid and abet as well. How do we protect the integrity of what we're trying to do and still be transparent about our capacity, without giving away the shop to people who might potentially abuse it? How do you draw that line and what are your thoughts on this?

I'm not sure who would answer this best.

Mr. François Guimont: If I may, Mr. Chairman, I'll ask Madam Clairmont to answer.

Mrs. Lynda Clairmont (Senior Assistant Deputy Minister, National Security Branch, Department of Public Safety and Emergency Preparedness): In terms of awareness, on Public Safety's website we have what we call "Get Cyber Safe". It's a website where citizens can look at various things they can do to keep themselves safe. We are of the same mind as you are in the sense that it is a partnership. It requires the private sector, levels of government, and also our citizenry.

In addition, we're linked to "Stop. Think. Connect.", a cyber-awareness program that is co-sponsored in part by some private sector companies in the U.S. The Department of Homeland Security also offers citizens opportunities to assess their cyber-risk profile.

Mr. Daryl Kramp: That's fine, thank you.

Mr. Long, this government introduced the shared services initiative in 2011 and obviously the intention is to make information technology more secure. Have you been able to find that effective balance between security and transparency? What are your thoughts on that?

Mr. Benoît Long: Thank you for the question; I appreciate it. Yes, Shared Services Canada's mandate clearly outlines the steps we need to take to secure the infrastructure. So we've already started consolidating that infrastructure across the 43 departments, harmonizing the practices and the approaches that are taken in every department to secure those systems.

As you can imagine, before our creation every department would do what they could in their own ways at different levels of spending and of effort. Clearly now we're able to do this horizontally to ensure consistency, and also to ensure compliance with standards that are established through the Treasury Board. That is an important step forward.

Now we're also redesigning those services to have security by design to embed security principles, to embed security throughout the means by which those services inside the government will be consumed, and that's been fairly important.

Finally I would add that on the procurement side we've enhanced the security requirements that exist with the prospect of being able to secure both the goods and services that we purchase as a government through the department. That will enhance our ability to deploy and ensure the safety of that equipment and the services that leverage it.

The Chair: That's very good. Thank you, time has expired.

Now Madame Blanchette-Lamothe, you have the floor.

[*Translation*]

Ms. Lysane Blanchette-Lamothe (Pierrefonds—Dollard, NDP): Thank you.

I would like to talk a little bit about sector networks. First of all, people say that Public Safety Canada should ensure that all sector networks are fully established and operational, as set out in the national strategy and action plan.

My first question is simple. Are the 10 sector networks now operational? Can you provide me with some information about that development?

Mr. François Guimont: To my knowledge, the 10 networks are active. The Auditor General's observations were related to a certain point to the fact that the sectors were not all equal.

We are currently working on developing a document that will provide directions, because not all these sectors were managed by Public Safety Canada. We chair an intersectorial table, where members come and we can coordinate our work, but different sectors are managed by different departments. Therefore, we are developing a guide that will be ready in December 2013. A draft version will be available in June 2013. It will help the various departments ensure that the sectors are complete and that the activities in those sectors are as well.

The sectors also have a certain responsibility. It is not just incumbent upon the government to gather these people together; they must also create the links they need within their sector to ensure they are well represented. So we are going to increase the number of meetings because I think it is important. These sectors do not work only on cyberspace, but also in terms of general infrastructure. We are going to increase the weight given to the cyberspace issue in these infrastructure tables.

We are doing what we need to with respect to the Auditor General's observations, which we feel were appropriate in that area.

● (1620)

Ms. Lysane Blanchette-Lamothe: I imagine that you have addressed the issue with representatives that sit on these sector networks. We see that six out of 10 sector networks do not have representatives from industry groups considered to be the main stakeholders.

Are you saying that you are in no way responsible for that and that nothing will be put in place to improve the participation of sector networks?

[*English*]

Mrs. Lynda Clairmont: I guess the issue was: are all the members of the various sectors participating in the sector networks?

One thing we're doing, which we're on track to finish in June of this year, is to reach out to the sectors and to the departments that are involved with them, and ascertain whether they have the correct membership on each of the sector networks. That work is under way —just to confirm that.

[*Translation*]

Ms. Lysane Blanchette-Lamothe: If the composition of these networks is not satisfactory, are you going to take some responsibility and ensure that everything will be done so that it is satisfactory?

[*English*]

Mrs. Lynda Clairmont: Yes, absolutely we will. It's a partnership, though, so we'll want to consult with the sectors, with private sectors, to see who they think is most appropriate. Absolutely, our role is to coordinate these things and make sure they happen, and that's what we're doing.

[*Translation*]

Ms. Lysane Blanchette-Lamothe: Will you be able to keep us informed about your progress in that respect?

[*English*]

Mrs. Lynda Clairmont: Yes.

[*Translation*]

Ms. Lysane Blanchette-Lamothe: Thank you.

As for the private sector, we see that not all stakeholders are reporting to the CCIRC on attacks. It seems to be a problem. In fact, Mr. Ferguson mentioned in his report that without thorough knowledge of what is happening on the ground, it is difficult for the centre to analyze the situation and provide advice on the matter.

What could you do to improve reporting from the private sector?

[*English*]

Mr. François Guimont: If I may, Mr. Chair, Mr. Gordon will answer that one.

Mr. Robert Gordon (Special Advisor, Cyber Security, Canadian Cyber Incident Response Centre, Department of Public Safety and Emergency Preparedness): We've been engaging the private sector from two perspectives.

The first one is encouraging them, through showing them the products that the government will actually produce back, to show them the value in their telling us what's going on. We've had very positive feedback from them. The number of reports that we're producing each year has gone up, and the input we're receiving from the private sector is going up.

I recently was at a session with the Canadian Electricity Association where they were very pleased with the response from the government. They were encouraging their membership that the more information they provide to the government, the better quality the information is that the government's going to be able to put back.

The results of those ongoing discussions is that the quality and quantity of the reporting we've been producing in the last two years has been going up significantly. There's still more work to do and we'll be undertaking that as we go along.

The Chair: Thank you. Sorry, time has expired, madam.

We'll move along to Mr. Shipley. You have the floor, sir.

Mr. Bev Shipley (Lambton—Kent—Middlesex, CPC): Thank you very much.

Thank you, witnesses.

In the Auditor General's comments, he talked about critical infrastructures that are privately or provincially owned. The federal government has an important role in helping to prevent attacks and to reduce vulnerabilities. It has access to information that may not be available. They can collect and analyze threat information, establish partnerships and stakeholders.

There's a lot of non-directive contact or authority by the federal government. You mentioned partnerships in your comments. Do you feel there are appropriate partnerships with the private sector and government now?

● (1625)

Mr. François Guimont: Thank you for the question.

I'll say a few words, and then I'll turn to my colleague Madam Clairmont.

I think our partnerships and involvement with all levels of society, including Canadians more directly, have to evolve with the threat environment we're in. That's the first observation I would make.

Secondly, if we want individuals or companies to equip themselves and respond correctly, they need information—I very much agree with that premise. We have taken steps to be able to share with people fairly sensitive information that needs to be security cleared, so that they are aware of what they may be facing and their response is proportional to the knowledge of what the environment is showing.

I'll turn to Madam Clairmont for more information on that.

Mrs. Lynda Clairmont: I think we're reaching out to the private sector on a number of levels and in a number of ways.

One way is through CCIRC, through our CSIRT, the computer security incident response team. That's where we're encouraging, as Mr. Gordon said, that companies reach out to us when they have a vulnerability or see something on their system. The more we're getting out to them, the more they're seeing that there's a value added from CCIRC, the more they're approaching us. That's developing out as well.

We're dealing with the private sector through the critical infrastructure sectors, which meet fairly regularly; through multi-sector forums, where we're briefing at different levels; and also the cross-sector forum, which brings together all the sectors and deals with issues of common interest, of which cyber-awareness is one.

We continue to engage at various levels with various stakeholders, both here and with our allies in the private sector. As Monsieur Guimont said, I think it's a work in progress, and one that is more like a journey than a destination, if I could put it that way.

Mr. Bev Shipley: Thank you very much.

That helps to outline a bit about the growing need as well as the development of working with the private sectors and other levels of government too, because there is a lot of sensitive material that we maybe just don't understand or don't have access to.

Mr. Guimont, I want to go back to your comments about the funding that had come through, the $90 million and an additional $155 million over five years. You talked about the 15 hours, and you touched on how that works with the different time zones across Canada.

Can you tell us how it actually works with the time zones across Canada? The reason I ask is that you said, in those off times, there haven't been any calls needing to be responded to. I'm not sure of the exact words so I paraphrased it.

Could help you me with that? How does that work across the country, then, with the four and a half hours of time zone difference? How does that work, with not having someone there during those off hours? I know the phone system is there but—

Mr. François Guimont: Yes, indeed. The 15-7 essentially represents what I would call a normal workday, business hours, from one coast to the other. That is the premise. Seven days is exactly that, so a full week.

I'll let Madam Clairmont or Mr. Gordon address.... There is someone, probably through a rotation, who is to be available for phone calls if and when they manifest, but I will let them expand on that.

Mr. Robert Gordon: There are two dimensions to my response. One is that in addition to the on-call availability of being able to reach out through the telephone system to one of our operational response staff, we also have available the Government Operations Centre, also part of Public Safety, which is staffed 24 hours a day, seven days a week. So in the event that there was ever a disruption in our ability to reach out to our on-call person, they have the immediate availability of someone 24-7 in the Government Operations Centre.

Mr. Bev Shipley: Is that as a backup agreement?

Mr. Robert Gordon: That's correct.

Mrs. Lynda Clairmont: It's part of Public Safety.

Mr. Robert Gordon: Yes. They're also part of the escalation process, so if an event became significant, the Cyber Incident Response Centre would reach out to the Government Operations Centre to draw in a broader range of government response, in a number of ways, and also to reach up to more senior levels within the government if it were required.

The other thing is, when we're dealing with our clients—the people who would likely be phoning in, the business clients—the nature of the cyber-attacks we're dealing with are things where the identity of that attack occurs over a period of time. It's not likely that you sit and watch it occurring in live time, so typically the companies watching this will see it and will be working during the day—hence, we're working essentially the same hours—because the detection of these attacks can actually take many days to occur and there'll be a lot of analysis going on by the companies themselves. Once they see that, they will then contact the Cyber Incident Response Centre.

A similar program is also in place with our allies. The United Kingdom, Australia, and New Zealand run the same system.

● (1630)

The Chair: Sorry, time has expired, Mr. Shipley. Thank you.

Mr. Byrne, you now have the floor, sir.

Hon. Gerry Byrne (Humber—St. Barbe—Baie Verte, Lib.): Thanks, Mr. Chair.

My question is to the Auditor General.

Mr. Ferguson, would you be able to describe the value of action plans to Parliament, and to you as an officer of Parliament, in reviewing progress on a legislative audit?

Mr. Michael Ferguson: Mr. Chair, I think I'll use the example of this chapter, where we identified that those action plans didn't exist at the time of our audit and because of that, we didn't have any way, really, to measure the progress that had been made in this area.

I think that sums up the value of an action plan. It lays out what needs to be done, when it needs to be done, and then you can measure progress against it.

Hon. Gerry Byrne: Thank you very much.

In your opinion, would it be true to say that whether a department was a principal focus of an audit, or part of an audit but not necessarily a number-one priority—for example, there were approximately 13 departments that were included, that were touched by this particular performance audit.

Would it be valuable to Parliament and to you as an officer of Parliament if each and every department that was a subject of the audit tabled an action plan in response to a legislative audit?

Mr. Michael Ferguson: In general, it would depend on the recommendations we made. If it's an action plan in response to one of our audits, we would expect the department or departments to which our recommendations were addressed to be the lead on producing an action plan. If they felt they needed to get more information from some of the other organizations, then we would expect them to do that.

Hon. Gerry Byrne: Do the action plans that have been tabled at the committee today meet those qualities and characteristics?

Mr. Michael Ferguson: I can't give an opinion on that. We haven't looked at the action plans in any detail.

Hon. Gerry Byrne: The action plans, I understand, were released just recently, but it was indicated from Public Safety that an action plan was released last week.

Mr. Guimont, was the action plan that was tabled before the committee today identical to the action plan that was released last week?

Mr. François Guimont: The management action plan, as per the request of the committee, is specific to the recommendations of the OAG—systematically, blow by blow. We've tabled that. It was developed and tabled, and if I remember correctly, it's been carried out, except for one or two actions.

The other action plan is the more comprehensive action plan that the OAG has been looking for. We very much agree with him. We have now developed it, though it took a while, and now it is published. We rendered that plan public on April 18, I believe. By the way, it includes multi-departmental actions, so that departments are committed to carrying out certain tasks against a deadline of sorts. Along the lines of what the OAG is saying, it is grouped under the various pillars that we have for the strategy, which makes sense because that's our framework.

Departments, including my own, are expected to deliver a number of things. We have combined existing, ongoing, and completed tasks. The bottom line is that the comprehensive action plan includes some of the elements we produced as a management action plan in response to the OAG report.

Hon. Gerry Byrne: Thank you very much, Mr. Guimont.

One of the issues that was flagged for me is that a parliamentary committee receives a two-page action plan so that Parliament can hold the government to account on a critical issue like cyber-security. But what has been issued by the department for public consumption was—I assume as a communications method—a more comprehensive action plan, and the two don't seem to mesh for me.

What's tabled here is an item of record before a parliamentary committee, but what you're telling us is that you produced a much more comprehensive action plan that was not tabled before Parliament. Still, we're supposed to hold you to that standard. Is that correct?

● (1635)

Mr. François Guimont: In reality, just to be clear, the management action plan tabled before the committee as per your requirements, which we acknowledge, included having to develop a more comprehensive action plan. Our action plan for the OAG, for the committee, was developed very quickly, because we needed to be able to answer the various recommendations of the OAG. The more comprehensive action plan took some time. It was a fair amount of work and consultation to get the buy-in.

Hon. Gerry Byrne: With respect, I have to interrupt. You said you issued the comprehensive management plan last week, and you issued the more important action plan to the committee today.

The Chair: Give us a response, and then time will have expired.

Madam.

Mrs. Lynda Clairmont: The plan we tabled with the committee today is the action plan that responds to the audit, but it's not the action plan that responds to the entire cyber-security strategy, which was released in 2010. The 2010 cyber-security strategy had a number of actions under the three pillars, as Monsieur Guimont said. The action plan that was posted on the website, which was mentioned in the OAG audit, is our response to the government's way of laying out the actions they are taking in response to the strategy that was released.

The Chair: Mr. Byrne, you'll be up again in four slots, so if you want to pick up on this then, you certainly can.

Mr. Aspin, you have the floor, sir.

Mr. Jay Aspin (Nipissing—Timiskaming, CPC): Thank you, Chair.

Welcome to our witnesses.

Mr. Guimont, I too took Fortran and APL, so I share your astonishment.

Voices: Oh, oh!

Mr. Jay Aspin: The OAG report made a number of statements about the progress with critical infrastructure sectors. Could you elaborate on what progress has been made?

Mr. François Guimont: Indeed. I'll say a few words, and then I'll turn to Madame Clairmont.

The first point is that essentially we have a 10-sector table—for instance, transportation, finance, energy, water production. There are 10 of them.

Second, we have a cross-sectoral table, where we essentially extract and meet together these various sector tables so that we have a common agenda.

The three basic functions that these tables, either the cross-sectoral one or the sector ones, deal with are critical infrastructure overall: multi-hazard-type risks that we may be facing. So it's cyber but it's not only cyber. To the point I was making earlier, cyber-threats now have taken more space and time, and we are focusing on that very point.

We deal with partnerships and relationships through those tables, with information sharing so that we bring people up to speed on various issues that they may be facing or that they are facing. We share that, and generally speaking we deal with risk management issues.

I'll turn to Madame Clairmont to add to this.

Mrs. Lynda Clairmont: Actually, Bob was going to lead on this one.

Mr. Robert Gordon: Thank you.

There are actually some very specific actions we've been able to take in addition to the broad ones that Mr. Guimont was speaking to. We've established, on the risk management perspective, a number of guides and planning guides that are useful to a cross-range of critical infrastructure sectors.

We've also engaged in a United States action plan for critical infrastructure. We've engaged with the Americans on a regional resilience assessment program where we're actually doing cross-border assessments. For example, in New Brunswick this past year we completed six assessments. The first round was looking at the physical issues relating to it. This would be things like the cross-border sections or the border crossings at Woodstock and Edmundston, the port of Saint John, the Irving Oil plants, and the LNG plant, where we've actually undertaken those assessments and provided the advice back to the owners and operators of those systems on how they can improve the security of those.

We are now moving those out across Canada. We are doing another pilot in Ontario, and another one in Saskatchewan. We'll be adding into those a cyber component.

We've also established a number of information-sharing...both a framework to guide the sharing of information within critical infrastructure sectors, and information-sharing gateways to facilitate some of that sharing as well.

● (1640)

Mr. Jay Aspin: Thank you.

If I may, Mr. Guimont, I know you alluded to this previously, but I wonder if you could focus in on what the Government of Canada has done to ensure that Canadians can use cyberspace safely.

Mr. François Guimont: It's the third pillar. We've had a campaign website, and Canadians can ask questions and get some information. But as I said earlier on, while we provide this information, at the end of the day they have to assume some responsibility, and I think they are. People are more sensitive to cyber-realities than they were five years ago, let's say, or three years ago. Frankly, it's also because of the media stories that have existed out there.

I'll turn to Lynda, or to....

Mrs. Lynda Clairmont: I can start it off.

In addition to our Get Cyber Safe website and Stop. Think. Connect., which I mentioned earlier, we're also working with the U. S. and other allies around the world to have a cyber-awareness month, which is in October. We're doing all kinds of activities with the private sector and with citizens to enhance cyber-security awareness.

One example is working with stores that sell a lot in terms of telecommunication—iPods and other stuff that kids would use. There is safety information inside, but we're having pamphlets that.... We would give them out so that parents would see them more, as opposed to children.

So there are number of things we're working through and coordinating, inside of Canada with the provinces and territories, but also externally with international partners.

The Chair: Real quick, Mr. Aspin, please.

Mr. Jay Aspin: Are we safe in cyberspace?

Mr. François Guimont: It's an interesting question because certain threats in the environment we live in may be a bit more static in time.

Mr. Gordon was explaining to me, Madame Clairmont, and other specialists, that the cyber-world evolves very quickly. When you think about it, it's a world where you don't need much. You need minimal, technical apparatus, servers or computers, brain power, and time on your hands, if I can use that terminology.

It is an evolving threat in that sense. I think we are as active. We have a strategy, players are involved, and we have resources. I don't think one can put his or her guard down. The cyber-world evolves quickly and we have to keep up with that reality.

The Chair: Very good, thank you.

Monsieur Guimont, I appreciate the shortness of that answer.

Moving along, Monsieur Giguère, you have the floor.

[*Translation*]

Mr. Alain Giguère (Marc-Aurèle-Fortin, NDP): Thank you, Mr. Chair.

I would like to thank the witnesses for being here.

First of all, I would like this document to be tabled. It is the Action Plan 2010-2015 for Canada's Cyber Security Strategy.

I would like to point something out to Mr. Guimont.

You say on page 7 of your report that you are going to spend $155 million in over five years and, on page 6 of the same report, it says that that amount will be spent over four years. That is a difference of $30 million. I would like the numbers to be a little more balanced in future.

Mr. Auditor General, in paragraph 3.20 of your report, you say that $780 million has been spent since 2001. You also indicated that a $200 million-budget had been approved especially for cyber security, which did not correspond in any way to the funding related to activities to protect against cyber threats. Still, that is a lot.

Can we know where the money went? How is it that, with such a budget, all the services did not manage to establish a security service against cyber threats?

● (1645)

[*English*]

Mr. Michael Ferguson: In terms of the budget what we lay out in the chapter is the fact that when many of these budgets were allocated cyber-security was considered to be part of a bigger security apparatus, early on. As has been discussed, the cyber-world is something that has evolved. Early on, it was just considered to be one of a number of threats.

Really, what we identified here was.... Because it was folded in with funding for other types of threats, it wasn't possible for us to separate how much money was just for cyber-security. Also, what we were looking for, in general, were overall plans, so that we could see what activities were supported to be conducted and then measure progress against it.

[*Translation*]

Mr. Alain Giguère: Thank you very much.

We saw that, of the $780 million, $570 million was given to the Communications Security Establishment Canada. After spending so much, how is Canada better protected? I would also like you to give us a detailed report on how that $570 million was spent, please.

[*English*]

Mr. François Guimont: I will turn, if I may, Mr. Chair, to my colleague from CSEC.

Ms. Toni Moffa: Thank you.

As I said earlier, and as the Auditor General mentioned, the numbers that total the $570 million include program activities for cyber-security that are not necessarily directed at cyber.

The investments we made in our activities for our contribution to cyber-security include improving and increasing intelligence production on foreign cyber-threats, because that's part of our foreign intelligence mandate. Also, we improved our capacity to detect and analyze threats on federal government systems. On those government networks, particularly the ones that are run by Shared Services Canada, that consolidate Internet connections for the government's systems, we deploy technologies that are able to detect cyber-threats that are not detected by commercial technologies because they are based on classified information about threats. That gives federal systems an added layer of security.

We do detection and analysis of the information we find there. As threats occur or are occurring, we can notify departments and provide mitigation advice on how to stop those threats from happening, and also longer-term advice so they can strengthen their systems to stop those problems from recurring.

With part of the funding we received, we run an IT security learning centre—

[*Translation*]

Mr. Alain Giguère: I would still like details on how the $570 million was spent…

Ms. Toni Moffa: Detail on the spending?

[*English*]

To answer that question certainly would reveal our level of capability in these areas, which we would consider classified information. It would not be prudent to disclose to those who seek to do us harm.

I will try to provide you an outline of the various activities, but the actual level of investment in those areas, particularly on our technological capabilities, is something we consider classified information for national security reasons.

The Chair: We're starting to get into some constitutional grounds here.

Mr. Giguère, your time has expired, but I'll forward you an opportunity if you have a comment about the information you're requesting, so I can get a sense of where this may or may not be going.

Did you want to pursue this, sir, or are you satisfied with the answer you have? If you are, that's fine. We'll move on.

[*Translation*]

Mr. Alain Giguère: No, I cannot be satisfied with an answer like that.

Canada has invested significantly in the Communications Security Establishment Canada, to the tune of $570 million.

We were told that work has been done and that Canada is better protected than before. Unfortunately, the report indicates that we are not…

● (1650)

[*English*]

Mr. Andrew Saxton: On a point of order, Chair, I believe my honourable colleague's time is up. You're extending his time.

The Chair: No, I am not doing anything I haven't done for anybody else. I'm giving him an opportunity. He's going to wrap up very quickly. Then I'll move along. Then we'll determine whether we have an issue or not.

Right now I don't hear one, but I'm looking to see if I do or not.

Continue and wrap up quickly, please.

[*Translation*]

Mr. Alain Giguère: We are the Standing Committee on Public Accounts. We must ensure that taxpayers' money is being spent properly and that it is spent where the government has said it needs to be.

We have given $570 million to this organization, and we are being given general information. I am asking for details. I want to know what this money went to.

We asked that the money be spent on a particular system. I want to know that it was. That is the essence of this committee.

[*English*]

The Chair: Very well.

We'll leave that for the time being and deal with it going forward, if we have to.

Mr. Hayes, you have the floor now, sir.

Mr. Bryan Hayes (Sault Ste. Marie, CPC): Thank you, Mr. Chair.

My question will be to Mr. Guimont.

Jim Burpee, president and CEO of the Canadian Electricity Association, has stated, “Through the National Strategy and Action Plan for Critical Infrastructure, launched two years ago, all of these players are engaged and working together to address Canada's cyber security challenges.”

I'm going to get there, but back to this action plan. I'm confused, because he's speaking to an action plan of two years ago, and you're speaking to an action plan that was released on April 18.

Can you shed some light? How many action plans are there? What was the reason these action plans were released? On what dates were they released?

Mr. François Guimont: Thank you, Mr. Chairman, for the question. First, there is essentially, as I should call it, the management response to the OAG recommendations, which was filed with the committee, and that is very specific to the recommendations that were made and accepted by the department. That's number one.

Number two, one of those recommendations was to develop a comprehensive action plan in order to be able to track progress as well as results measured. We have done that. It took us a while to do that, months. It was a lot of work. It's normal. It's not unusual. Now that's been made public as of April 18. Not only that but we have also developed a framework to track progress, so that is also available.

The sector tables all have an action plan of sorts. They're busy looking at risk, managing risk, sharing information. As well, we are going to, on cyber, augment the frequency of meetings, and we will do that against actions that we will collectively agree we need to take in order to manage a cyber-risk, as a for instance. They all kind of fit together, but “separate but connected” is the way I would describe that.

Mr. Bryan Hayes: On this plan that the president of the Canadian Electricity Association refers to, according to him it's working extremely well. In other sector networks, it doesn't seem to be working as well. I wonder if you could elaborate for me why in the Canadian Electricity Association the plan seems to be unfolding very well, and in some other sectors it doesn't seem to be.

Then, what sector is the next priority? I'm getting a sense that it's a challenge to manage all the sectors at the same time. Is there a sector priority implementation plan, so to speak?

Mr. François Guimont: I'll turn to Madame Clairmont to have a stab at this, please, if you may.

Mrs. Lynda Clairmont: I think you're referring to the critical infrastructure strategy and action plan that was developed with the provinces and territories. Each of the sector networks is part of that, and I think in the electricity sector it's working very well. I think other sectors are not maybe necessarily at the same level, but they're developing and coming along.

Mr. Bryan Hayes: So what are the lessons learned in terms of why it's working so well in one sector and not so well in other sectors?

Mrs. Lynda Clairmont: I think some of the sectors are more diverse. Some of the sectors were already more organized to start off with. Some of the sectors are more coherent. They have similar functions. When you take, say, the food sector or the food networks, it's a broad range of things, whereas some things like banking and the electricity grid are fairly centralized.

● (1655)

Mr. Bryan Hayes: Mr. Guimont, where are we in relation to two of our closest security and intelligence partners? In the report that was the U.K. and Australia. How do we compare in terms of our cyber-security systems with these two nations?

Mr. François Guimont: Thank you for the question. I will start with the relationship we have with the U.S. They're very close. Our economies are connected in a meaningful way, so we have a lot of relationship. I was in Washington a couple of months ago and I sat down with a number of people, and cyber is a top-priority topic. That is my first observation.

The second one is that it's not just flying down and meeting. We also have essentially committed to a number of actions with the U.S. We've done that formally. Madame Clairmont will speak to it in a minute.

Third, we also deal with other countries, so not only the United States, the U.K., New Zealand, etc., and it's always the same thinking: sharing information; where we can have common strategies; and being ahead of the issues potentially coming our way. Madame Clairmont just had a meeting very recently on the so-called Five Eyes and she can speak to that as well specifically.

Mrs. Lynda Clairmont: I would say a couple of things. One is that our cyber-strategies closely align with those of our closest allies. They're all very similar. They were all announced at separate times, but we are different countries so we implement these things a little bit differently.

When I was preparing for the committee and thinking about how we align with our allies, I was thinking really thematically, that there are a couple of themes that we see in all of our like-minded countries that we deal with. Information sharing is key to all the strategies and approaches to cyber-security—that's the right information to the right people at the right time. Also, I think the public-private partnerships are really key as well. International engagement, making sure that we are having similar messages internationally is also key. Lastly, protecting our citizens through awareness campaigns, through anti-crime and anti-fraud kinds of situations.

With respect to the U.S. specifically, we announced our public safety-department of homeland security action plan in 2012, and that had basically three goals. One is to enhance our cyber-incident management—that's our CCIRC to their US-CERT—with more exchange of information, more timely information, and actually exchanging people. Second was the joint engagement and information sharing with the private sector, because a lot of the private sectors are common across the borders. Also, we have the continued collaboration on our cyber-awareness campaigns.

The Chair: Okay, that does it. Time has expired, so thank you very much.

We'll move along now and go back to Mr. Byrne. You have the floor, sir.

Hon. Gerry Byrne: Thanks, Mr. Chair.

One of the preoccupations of this particular committee and of Parliament is that we hold the government to account. One of the issues that was raised by the Auditor General in the report was a seeming reluctance to identify specific dollar figures spent on cyber-security threats.

The Auditor General did indicate there was approximately $780 million appropriated for various activities, but departments seem very reluctant to actually dig down and define how much of the $780 million was specifically identified and spent on cyber-security. Would you be prepared to provide that information to the committee, Mr. Guimont?

Mr. François Guimont: Thank you for the question.

Mr. Chair, I can certainly provide some information on the $780 million, starting with the fact that four Treasury Board submissions were approved. This was over a 10-year period for 13 departments. I accept that this is not a straightforward topic. There is a bit of concern about resources and where they went.

Over that 10-year period, $21 million went to cyber, so I would like to take a moment to say that cyber 10 years ago is not what cyber is today, in the sense that this funding was for critical infrastructure, all hazard-type issues, including cyber. But 10 years ago cyber was at a given place. We all have to remember this was post-9/11 and we were in that world, if you wish.

Of that $780 million, $570 million went through the Treasury Board process, RPPs and DPRs, and all that reporting, to CSEC, the way Madame spoke to the resources and how they were invested at the macro level.

The last one I would mention briefly is that $190 million went to different infrastructure-type issues, writ large, not specific to cyber.

That's the macro, and I have examples here of how the resources were spread.

I want to make a little segue, and I won't be too long, on the very valid question of how come you had $155 million recently announced over five years and the action plan makes reference to four years. It's simply because when an announcement is made, the resources don't flow automatically. We had to go through an approval process that consumed a period of time, for due-diligence reasons, and now we have four years to invest that $155 million. I want to be on the record on that point.

● (1700)

Hon. Gerry Byrne: Thank you very much, Mr. Guimont. I appreciate that.

Regardless, however, the Auditor General did identify $780 million within the audit period. He identified $570 million specifically for Communications Security Establishment Canada.

One of the things we always are a little bit concerned about is the process of double counting, where the government may suggest $780 million was spent on cyber-security in the advent of a cyber-security threat and then in the advent of a domestically radicalized insurgency threat all of a sudden $780 million is spent there as well.

It's useful from a parliamentary accountability point of view to have some clarity. I'm not asking for specific projects, which may infringe on national security requirements, but to have some clarity as to what exactly is prioritized for cyber-security versus other things.

Now with that said, I'll have to move on because my time is dear.

We appreciate, Mr. Guimont, that a very thorough, much more detailed publicly available document was provided on an action plan related to cyber-security. Would you be prepared to have that submitted to the clerk—that document entitled, “Action Plan 2010-2015 for Canada's Cyber Security Strategy”, which is a cross-governmental strategy—as a government-wide departmental action plan in relation to the Auditor General's report?

Would you be prepared to have with it and bear with it the same parliamentary accountability and scrutiny, which holds the government to account? That is, that which is found in this document is the same as that which is found in these two pages, in terms of its accountability requirements to this committee and to our report writing.

Would you agree to have this document submitted as a departmental action plan for the benefit of the committee and to be held account to that departmental action plan?

Mr. François Guimont: The answer is yes.

The Chair: Thank you.

You have 17 seconds.

Hon. Gerry Byrne: I think I'll pause with that.

The Chair: Very good. Thank you. We appreciate your discretion.

Moving on, Mr. Dreeshen, you now have the floor, sir.

Mr. Earl Dreeshen (Red Deer, CPC): Thank you very much, Mr. Chair.

Thank you to Mr. Guimont. I can add Pascal, COBOL, and BLISS as well to that. Had I learned how to type without just using one finger, I would probably have stayed in that particularly area, but now we're back to one thumb so it works out not too badly for me.

On the website, you had talked about having 227,000 hits come in. It's being used well, and I think that's something that is important. Of course you were also talking about how you get zero off-hour calls.

I know one of the things we talked about back in the fall when we first discussed this was the idea of going from the eight hours to the fifteen hours, which basically took our five-and-a-half time zones and made sure we were there for business hours. I think that was important. I can see the rationale for what we were talking about there, and again perhaps from the discussions we had maybe you bolstered a little bit in the other nine hours we have, to make sure that was being covered. I respect that part.

When I look at the Auditor General's report and I see the Auditor General talking about the $780 million and how the other split was, with the public safety officials talking about the $20.9 million of the remaining $210 million, I see that accounting and I respect that accounting. I believe that's what the Auditor General was looking at and saw those numbers and went through from there.

I guess I have a couple of points I really want to talk about as well. Could you speak to the steps the National Cross Sector Forum was taking with regard to the risk management activities and looking at how that partners throughout Canada? I wonder if we could have some comment with regard to what we have seen.

Auditor General, what did you see with this National Cross Sector Forum? Is that doing what you think should happen as far as risk management is concerned?

● (1705)

Mr. Michael Ferguson: I'll ask Ms. Loschiuk to deal with that question.

Ms. Wendy Loschiuk (Assistant Auditor General, Office of the Auditor General of Canada): Thank you very much.

We looked at the National Cross Sector Forum as an activity that had happened since 2010. It was something we saw as improvements in the communication, so we wanted to talk about it a little bit. In the chapter we do mention it in paragraph 338 where we talk about what has been going on that we noted was good progress. This National Cross Sector Forum we saw as something that was in there to help bring groups together that had not yet had an opportunity to fully coalesce as sector networks.

From that perspective we saw it as an active thing that was taking the place of sector networks that were not yet fully in place.

Mr. Earl Dreeshen: Thank you.

Ms. Charette, in your opening remarks, you talked about how TBS had placed renewed emphasis on increased awareness and best practices for IT security across government. I wonder if you could go through what some of those best practices are.

Ms. Corinne Charette: Thank you very much.

That's an excellent question. In fact, we have done a number of things. The first thing we did was we surveyed our community departmental security officers extensively to understand what they believed were the needs across the community for more security awareness. With them we have essentially developed a Government of Canada security training framework and a security professionals training working group. We recognize that working on the awareness of every public servant regarding cyber-security is also an important part of the effort. Development through the framework of training materials is under way.

As part of the October cyber-month, we also try to participate and stress that to all public servants. We're also working quite a bit on the issue of awareness of good cyber-behaviour on a departmental basis regarding things like, for instance, not opening up all attachments when they come in through e-mails, because despite the best spam filters or filters in general, there are very clever ways of luring people into accessing e-mails that are in fact bearing malware.

We're also currently nearly finished developing an IT policy information notice that will go out to departments on what they need to do to secure portable media, and to raise awareness of the fact that portable media are a way to introduce threats if you load them into government systems. So we're working on a number of areas to raise awareness within the community at all levels, at the employee level, at the IT level, at the departmental security officer level, as well as with all executives to ensure that everyone understands their role in maintaining proper security.

The Chair: Sorry, Mr. Dreeshen, time has expired. Thank you.

We have two more spots left. The next one will be Mr. Allen. I understand you're going to share your time with Madame Blanchette-Lamothe and that is fine. You have the floor.

Mr. Malcolm Allen: Thank you, Chair.

To Mr. Ferguson, on page 10 of the English version of your report at paragraph 3.20, you said you identified $780 million in funding approvals. You said you were unable to specifically find out where it was allocated. At the bottom of the paragraph, you said you also identified a further $200 million.

Is that a cumulative thing, sir, so $780 million plus $200 million? Is that what's being said to me in that paragraph?

Mr. Michael Ferguson: That's right.

Mr. Malcolm Allen: We're now approaching $1 billion, $980 million to be precise, so my question to the departments is this. Based on the fact that we are unable to tell the Auditor General how we spent the money especially on the cyber-aspect, first, can the department track those pieces?

Also, through you, Chair, I would like that to be set back as a line item, to determine how that money was allocated across those 13 departments, because now we're talking $1 billion. I'd actually like to know where it went, including the stuff that didn't go directly to cyber. I'd like to know just exactly how that piece was spent. I'll leave that for you, Chair, to rule on and to instruct the witnesses accordingly.

I'll now turn the rest of my time over to Madame Blanchette-Lamothe.

● (1710)

The Chair: Madame.

[*Translation*]

Ms. Lysane Blanchette-Lamothe: Thank you.

I have a question about the January 2011 intrusion mentioned in the Auditor General's report.

This intrusion, which was quite serious, was aimed at obtaining information, taking control and extracting information of a sensitive nature. We know that reacting to that attack was costly and that it took time to recover completely.

What do you think about a mandatory mechanism that would provide notice in the case of loss of data or unauthorized access to data? It might ensure better protection of the personal information of Canadians in the case of a cyber attack.

If that is not an option you are considering, what do you plan to do to protect the personal information of Canadians?

[*English*]

The Chair: Who would you like to answer that, Madame?

Is there anybody who wants to? Somebody jump in, please.

Mr. Robert Gordon: Mr. Chair, I'd be happy to answer that—

[*Translation*]

Mr. François Guimont: Mr. Chair…

The Chair: Mr. Guimont, you have the floor.

Mr. François Guimont: Mr. Chair, if I may answer this question which, if I've understood it, has to do with protecting personal information, in some way, like the third pillar of the strategy mentions.

I am thinking only of Canadians. People are responsible for protecting their own information. That is the first thing.

Furthermore, regarding the government systems where my colleague, Mr. Long, works, I would simply like to note that we have a very high number of email systems and that we are moving toward a single system.

We also have over 200 data centres. Some of them are a little older, some a little newer; it is a mix. We are moving toward about 20 data centres.

All that means that we are trying to close windows that may be at risk and susceptible to cyber attacks. Of course, if that information includes personal information, we are reducing the risk of Canadians' personal information being made public.

Those are the two examples I would give of what we are doing.

Ms. Lysane Blanchette-Lamothe: I have one last question for you.

A little earlier, my colleague asked if our cyberspace is secure, and you answered that that was pretty much the case. However, we know that the Auditor General's report expressed doubts about our capability to respond to and prevent cyber attacks.

What could be added to the action plan that you put in place and to all your resources to maximize our efficiency in countering cyber attacks and our capacity to respond to them?

Mr. François Guimont: I joined the department in November and, since then, the issue of cyberspace has been a priority for me. It was not so much my decision as it was the nature of the issue; we talk about this issue a lot within the department. That is my first observation.

Furthermore, I am also speaking for my colleagues in the federal government and in the private sector. I have had discussions with John Manley, of the Canadian Council of Chief Executives. I also want to meet with a group of people who could help us better understand the dynamic within the private sector.

I would say that there is an awareness, and that is where we need to start. I do not want to say that it was absent before, but we realize that, with the development of cyber threats, we need to work together more than we did before. This is not a magic formula, but if there was something to put on the table that could be important when it comes to protection, I would say that it should ultimately be better cooperation, a good exchange of information, action plans and following up on the actions we take. I know that there are more, I acknowledge it now. I think that is the recipe for better prevention of threats.

Ms. Lysane Blanchette-Lamothe: With respect to follow-up…

[*English*]

The Chair: Sorry, Madame, time has expired.

Mr. Saxton, you have the floor.

● (1715)

Mr. Andrew Saxton: Thank you, Chair.

I'll share this time with my colleague, Mr. Dreeshen. I propose that he begin and then I'll wrap it up.

The Chair: That's a funny way of going about that, but okay, we're good with that.

Go ahead, Earl.

Mr. Earl Dreeshen: Thank you very much.

I kind of just jumped in, so that's the reason for that.

For the Auditor General, if we could go back to 3.21, I just want clarification because of the question that Mr. Allen had presented over there. It says in the first sentence, “Of the $780 million, we did identify that about $570 million was approved for Communications Security Establishment Canada”. Then, if we go to the bottom of that paragraph, it says, “Nevertheless, Public Safety Canada officials informed us that about $20.9 million of the remaining $210 million was directed toward cyber protection”.

To me then, it is the $570 million plus the $210 million that made up the $780 million? So, I believe when I heard Mr. Allen say that makes it nearly a billion dollars, it wasn't really that?

I was taking that from what I had read there.

Mr. Michael Ferguson: We have Ms. Loschiuk to deal with the question.

Ms. Wendy Loschiuk: When we identified the allocations of funding, we were trying to track it all and see where it had gone. We could only break it down as far as what's in this report. What we were able to identify was that, as you explained, $570 million went to one organization, plus we wanted to know where the remaining $210 million went, to other organizations.

In the course of looking at the work, though, we were also able to identify that there was some ongoing funding over the course of many years and that was the other $200 million, although we don't have a whole lot of detail on that information. There's just ongoing funding to departments.

Mr. Earl Dreeshen: Thank you, then. I just wanted clarification on that. I didn't see where that other $200 million was in the report. I was just going with the $570 million plus the $210 million.

I'll give my time back to Mr. Saxton.

The Chair: Very well.

Mr. Saxton.

Mr. Andrew Saxton: Thank you, Chair.

First of all, I'd like to thank Public Safety for providing the action plan that our committee had asked for through a motion dealing with the Auditor General's recommendations. My thanks also for the action plan that was released on April 18. Those were both very helpful.

I'd now like to ask the deputy minister to kindly explain and give an update on the three pillars, which are: securing government systems, partnering to secure vital cyber-systems outside the federal government, and helping Canadians to be secure online.

Mr. François Guimont: Thank you, Mr. Chairman.

I hope, Madame Clairmont, that your voice will allow you to bring the update to the committee. I would appreciate that.

Mrs. Lynda Clairmont: Okay, if it's a bit sketchy, I'll ask Bob to jump in.

Basically, what we did in the action plan was look at the various activities that were under way and how we could frame them. In terms of the government systems, we are working a lot to enhance CCIRC, CSEC, and the Treasury Board systems, as well as Shared Services. I think we have a really good approach to protecting government systems.

We're also doing a number of other activities that both Corinne and Benoît referred to as well. The second pillar, the partnerships in securing vital systems outside, is focused on the critical infrastructure sectors—further developing them, reaching out more to the private sector, engaging the sectors bilaterally, and improving those relationships. In that area, I would include the relationships and the outreach we're doing with like-minded countries—the U.S., the U. K., Australia, and certain European countries.

The final piece is about making sure that Canadians have opportunities to make themselves aware of the cyber-threat and to provide them with tools to protect themselves. I would encourage everyone to look at Get Cyber Safe as well as Stop. Think. Connect., because they have good advice for all of us. Sometimes we don't take the time to implement those.

That's it in a nutshell.

Mr. Andrew Saxton: Thank you very much.

The Chair: That exhausts our rotation of speakers. What we have to do before we go, however, is deal with some information that was requested.

Just before I do that, I wanted to call your attention to the Auditor General's comment in his ninth paragraph, where he ended it by saying that officials raised concerns that the cyber-threat environment might be evolving faster than the government's ability to keep up with the changes. If that's true, it's inevitable that at some point we're going to lose the race and be in serious trouble.

Mr. Guimont, give us your thoughts.

● (1720)

Mr. François Guimont: I mentioned that the OAG report was welcome. This is a good review. These are good recommendations, and the long action plan we produced is meant to bring us up to where we should be. But I'll be very direct on this. It's an evolving trend. It's morphing, changing all the time, and we have to keep up with the game. It's a collective effort. This is not just the federal government. Everybody has to be in. We are going to invest a lot of energy in sitting down with people and making sure everybody is on the same page.

The Chair: Thank you. I appreciate that.

Colleagues, a number of you have asked for some information. This has become a bit of an issue within the committee as to how we proceed in this regard. We have an informal committee struck to deal with that, which has not yet started to meet. I noted six items that we need to get some understanding on. I'm going to ask for the extraordinary cooperation of members. Please bear in mind that we haven't yet worked out what the rules we will be in terms of doing this.

We're going to try to do this one at a time, ad hoc, and see if we can come to an agreement. Where we can't, let's get a quick process in place. Then, at least on an ad hoc basis, we will have dealt with these individual requests that are coming up. I'm going to start with what I think are the easy ones—although one never knows—and work my way to the more difficult ones.

Early on Mr. Allen requested an org chart, and I believe that I saw a nod from the deputy that this can be provided. When would that be possible, Mr. Guimont?

Mr. François Guimont: If you don't mind, Mr. Chairman, normally we are given a window of two weeks. If that's okay with the committee, we will provide that to you in that window.

The Chair: All right, committee? Two weeks. Can we all live with two weeks?

Some hon. members: Yes.

The Chair: Okay. That's good. Fine, thank you. That's one.

Second, there were progress updates asked for by Madame Blanchette-Lamothe. It was kind of quick, but I did make a note of it, and I think I saw a nod there, too, for those progress updates. The nod was yes, but I didn't hear how that was going to happen.

Could I get some indication as to how you will honour the commitment you made in terms of giving us that information?

Mr. François Guimont: Just to be clear, Mr. Chairman, is this specifically on the progress made by the sector tables?

The Chair: Let me clarify with the member who asked the question.

Madam?

[*Translation*]

Ms. Lysane Blanchette-Lamothe: Thank you.

Given all the very interesting action plans presented today, it would be good to have follow-up on the progress of these action plans in general.

Since I had only five minutes, I asked questions about one specific aspect of an action plan. However, I would like to know about the progress of these action plans in general, if possible.

[*English*]

The Chair: We do that; I think we do that. That's done, isn't it?

Usually that's in our committee report, and then it goes into our matrix, and then we follow up on it. So that should be captured by virtue of the draft report, and if not, you can make a note or have your staff make a note that you want to raise it during draft writing.

Alex is here, and I'm getting a sense from him that there will be something in there that addresses that because it's a matter of routine. We do get the action plans, but the other half is our obligation to follow up and make sure these things are being done, and if they aren't, haul in the folks that are responsible and ask them why.

Does that work for you, madam?

[*Translation*]

Ms. Lysane Blanchette-Lamothe: Yes.

[*English*]

The Chair: Thank you. That's two down.

The third one I'll come back to later.

Four, Mr. Byrne asked a question of Mr. Guimont vis-à-vis the $780 million and the $570 million. Were you seeking where the full $780 million went, Mr. Byrne? I come back to you now for clarification.

Hon. Gerry Byrne: Thanks, Mr. Chair.

I asked Mr. Guimont a question, and to answer on behalf of the government. The Auditor General identified 13 departments and agencies that could have been ascribed up to $780 million related to security activities for critical infrastructure and government systems. It appeared to us, readers of the Auditor General's report, that there was an attempt or a desire to identify what, if any, of that $780 million could be ascribed to cyber-security specifically.

I did not ask for a catalogue of projects or expenditures, but if each of the 13 departments that were recipient of some of the $780 million could account to Parliament, through us, what specifically was provided for cyber-security activities and capital purchases, that would be very helpful. I would include with that the $200 million subsequently identified as well.

Mr. Chair, it is clear that $570 million was identified for the Communications Security Establishment Canada. Obviously, some of that would be for electronic eavesdropping; some of it would be used for cyber-security. Not all of it, however, would be used for either one. I would ask in the provision of this data from these 13 departments that they be very specific what money was provided for cyber-security. Where there is an identifiable cross purpose that some of the money could be used for cyber-security as well as, for example, electronic eavesdropping, it should be clearly identified what percentage or what basis, so that we can determine what has been established by the Government of Canada for expenditure on cyber-security.

Is that clear, Mr. Chair?

● (1725)

The Chair: I'm going to have two parts to this. I'm going to ask the deputy, number one, is it clear to him? Does he know what's being asked, and secondly, what is his response to that actual request?

So, two parts, do you understand the question and, if so, are you able to provide the information, Deputy?

Mr. François Guimont: I understand the question. The challenging part lies in the fact that these resources were spread over 10 years.

The Chair: I'm sorry. Pardon me?

Hon. Gerry Byrne: I'm sorry, Mr. Chair. That was me.

We could ask the AG as well, Mr. Chair, if that would meet his—

The Chair: Well, let's start with the deputy minister and see where we are.

Sorry to interrupt. Go ahead, please.

Mr. François Guimont: It's okay, Mr. Chairman. I apologize for cutting you off like that.

I was saying the challenge we have is one of 10 years, investment over 10 years. I mentioned very clearly four Treasury Board submissions, so requirements were put by ministers and approved, people made investments...most likely reported. It's about reconstructing the past. In part, that's the challenge, if you wish. These resources existed. Investments have been made. There are examples, clearly, of how the investments were carried out, but reconstructing the story precisely from 10 years ago, over that period of time, with 13 departments, I would say is the challenge.

So the question is clear. The issue is more one of specifically creating what I just described.

The Chair: Okay, I think it's fair.

Mr. Ferguson, do you have any thoughts on this?

Mr. Michael Ferguson: Thank you, Mr. Chair.

Not really, other than obviously when we were putting the chapter together we were having trouble getting all of that information as well because we recognized that the money was not just earmarked for cyber-security, it was earmarked for broader things. Certainly, though, one thing we can make sure of is that we will look at the level of detail of information we have in our file that we would have received from the departments and make sure they know what we have on that basis, and then they could augment that if they have any additional information.

The Chair: Let me try one thing and then I'll come back.

Can you take an attempt at this, Deputy? One of the things that we're looking at in terms of making requests—and I can't get too far ahead of my own committee—one of the things that we're factoring in is that it's one thing to ask for information in order to do our job, to hold you and the rest of government to account, but it has to be within reason. We can't just trigger a question that suddenly generates a million dollars' worth of expenses without being able to justify that this million dollars was well spent.

I sense from your comments we're into that realm of explanation. In the absence of our again having our definitive rules as to how we're going to approach these—I'm asking my colleagues to listen as much as I'm proposing this to you— could you take an initial run at this with the assistance of the Auditor General, who has said that he will provide some information that might help to provide some framework? Provide us with what you can, and as much as you can, as quickly as you can, and then we'll have to make a determination from there as to whether we consider the information received to be complete and acceptable or not.

Can that work? Can we try it that way, Deputy?

● (1730)

Mr. François Guimont: I will undertake to discuss this with the OAG as you are suggesting, and it may take a bit of time, Mr. Chair.

I haven't seen the body of information that the OAG has, and the only caveat I would put, and I hope that the committee will understand that, is that should there be information in that information that is sensitive from our posture vis-a-vis cyber-threats, I would appreciate knowing that the committee will understand that.

As Madame Moffa has mentioned, certain things would be quite sensitive. So with that caveat, I will undertake to discuss it.

The Chair: I'll tell you what. I'd appreciate it if you just held that caveat and just brought it, because that doesn't end the discussion. You well know what I'm talking about when I say we're getting into constitutional matters here of Parliament's unfettered right to ask for information. There are procedures that deal with this—what if it's considered a security issue?—and then we have some negotiation to the whole procedure in the rule book. But at the end of the day, you know, sir, that you can't just say to this committee, “You can't have it.” That is not the end of the story at all.

But, we want to stay away from those waters, those shark-infested waters. It would be so much better if we could come to a meeting of the minds.

So Mr. Byrne, and members of the committee, if we could try to be reasonable here, I think it's fair. The Auditor General has acknowledged that it was a lot of research, and even he didn't get it when he asked for that information, and I'm sensing—I'm not putting words in his mouth—some acquiescence on his part that he agreed with that argument.

Can we agree to ask the deputy minister to provide us with a report on the matters we've talked about? Then when we have it in hand, can we take a look at it and see whether that does it or not?

Go ahead, Mr. Saxton.

Mr. Andrew Saxton: Chair, we have specifically organized a subcommittee to deal with these issues. I think we're meeting very soon. I think we should deal with it in that committee, which was your initiative and your recommendation. So let's deal with it in that subcommittee.

I do note that the bells are ringing, and they have been ringing for several minutes now. I would, as we normally do when that happens, move to adjourn and thank our witnesses.

The Chair: You know you can't move a motion on a point of order, but your point is taken.

Are we on a 30-minute bell, clerk?

We're on a 30-minute bell, so we have a little time.

I hear what you're saying. If that's where the majority ends up going, saying we'll stop this process of discussing with the witnesses and we're going to defer to a group that's not meeting. I was hoping we could come to an agreement here on some basic things. As I said, if there's an area where we can't agree, if we can get a process in place....

Otherwise, I don't know how we're going to reassemble all these people and be able to do this as quickly as possible. We're more than halfway through. If you can give me a little latitude, because we have agreement so far....

Mr. Andrew Saxton: We could always write a letter as well—

The Chair: Okay, but bear with me.

Mr. Andrew Saxton: —following up. We don't have to reassemble the witnesses.

The Chair: Let's see if we can continue to get cooperation, and we can get the job done. That's why we're here, so if I may, let's try that.

When would that come to us, sir?

Mr. Daryl Kramp: I have a point of order, Mr. Chair.

The Chair: Yes.

Mr. Daryl Kramp: Chair, I don't agree with that.

Mr. Bryan Hayes: Nor do I.

The Chair: Okay.

Mr. Bryan Hayes: It's after 5:30. As far as I'm concerned, the committee's—

Mr. Daryl Kramp: There's a way to do it. That's not the right way to do it.

The Chair: What's the right way?

Mr. Daryl Kramp: The right way is to use some common sense in this committee. We have a difference of opinion. I want as much information as possible too. But as you, the chair, has said, there's a difference between “reasonable” and....

If we have a smoking gun here, it's one thing. We are going to create an onerous responsibility if we go down this road. It is going to be a momentous task to deliver the information. Is it information that is pertinent to the Auditor General's statement, to the investigation right now, to that outstanding problem? I think we need to have that discussion on that particular issue.

I have no problem going through some issues we all agree with. Let's just go ahead and do it.

The Chair: Okay, but we're close.

Mr. Daryl Kramp: But with a difference of opinion....

The Chair: But we're not at a difference of opinion, folks. I hear what you're saying.

Mr. Gerry Byrne: Chair, lower the temperature.

The Chair: Can you?

Mr. Gerry Byrne: Yes.

The Chair: All right, if you can lower the temperature, I'm listening.

Hon. Gerry Byrne: Mr. Chair, I think we should all recognize that Mr. Guimont is a trusted public servant, who not only has our confidence, but has earned our confidence. If he can do this, he will.

But also, I'll send a message not to Mr. Guimont but to the government. God forbid, should some provocative cyber-security threat occur, should the government ever stand up and claim they are spending *x* amount of money on cyber-security, when they know it's not true, because they can't tell a parliamentary committee how much they're spending on cyber-security. I would not want to walk in the government's shoes, that being the case.

So let's trust the public servant to come forward. If he can provide the information in a timely way, great. If he can't, because it's simply a task...the Auditor General has said he has records and files that may assist him. If there comes a point the department cannot provide this information, we can ask the Auditor General what information he flowed to them. But at the moment, a request has been made. Let's see if we can provide....

● (1735)

The Chair: The whole point was to give Monsieur Guimont an opportunity to provide us with what is reasonable, and so I don't think anybody's in disagreement. Monsieur Guimont's going to give it a shot, give us what he can. When we receive it, we'll see where we are. That gets us through that piece.

Next, there was another request, also by Mr. Byrne, for a broader departmental action plan, but I think we've already done it. You asked for that to be tabled, included. I think we can assume that's done pretty much now, right? It's here.

Yes, that an easy one. Consider that done.

Mr. Daryl Kramp: Chair, I don't consider the other one done. You said that's done. I don't believe it is.

The Chair: The one I just mentioned now?

Mr. Daryl Kramp: That's correct. The one we were discussing.

The Chair: It's the report right there that Mr. Byrne had, and it was just—

Mr. Daryl Kramp: No, no, the request.

The Chair: Yes.

Mr. Daryl Kramp: The request. You just said that's okay as far—

The Chair: For the one before?

Mr. Daryl Kramp: Yes.

The Chair: I thought we had agreed to it.

Mr. Daryl Kramp: Well, no, that's my point, we don't agree to it.

The Chair: We asked Monsieur Guimont what he could provide —

Mr. Daryl Kramp: No, Mr. Chair—

The Chair: Just what is easy to provide, can he provide us with that? Then we'll take a look at it and see where we're at. That's why I asked where the disagreement is. He offered that, and I took him up on his offer.

Where we could get into a ditch is if we get it and decide...and we get into a big discussion about whether it's enough or not enough. But that battle is not here now, that may be another day. Right now we all have agreement that the deputy is going to send us what he can. That seems to me to be fairly easy.

Then we did the next one, and I have one left, and then we go to the other one. There was a question asked about where the $1 billion went. I jotted that down. I don't see anybody jumping on it, I'll let that go. The last one I want to do the same way we just did with the deputy. This is the obvious one that gets us into real trouble right away.

Madam Moffa, again, I'm going to try the same process. Would you be kind enough to send us what you will need, send us what you can? If the committee decides that they need more, and that starts to get us into security issues, there are procedures to address that. I'm not putting you on that dime right now, we're not into those constitutional waters. Like the deputy, I'm merely asking you if you can, as you offered, give us an initial response of what you can.

But just hold the caveat part, because as soon as you do that you put me into an awkward position defending the rights of members to have unfettered access to documents. So if you could also provide us with what you can, what you have, within a couple of weeks, similar to what the deputy is doing, the committee will take a look at things. Then if there's going to be a fight, we'll have the fight. This at least gets us through today, it gets some information flowing and allows us to leave on such a happy note.

I like happy notes. Happy notes work.

I'm going to grab the moment to thank our witnesses very much, in particular the Auditor General, the deputy, and all the delegations.

On behalf of my colleagues, thank you very much. We enjoy working with you and we appreciate what you do. No doubt we'll see you all again soon.

This meeting is adjourned.

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

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

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

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca