



House of Commons  
CANADA

## Standing Committee on Public Accounts

---

PACP • NUMBER 022 • 2nd SESSION • 40th PARLIAMENT

---

EVIDENCE

**Tuesday, May 26, 2009**

—  
**Chair**

**The Honourable Shawn Murphy**

Also available on the Parliament of Canada Web Site at the following address:

**<http://www.parl.gc.ca>**

## Standing Committee on Public Accounts

Tuesday, May 26, 2009

• (1530)

[English]

**The Chair (Hon. Shawn Murphy (Charlottetown, Lib.)):** I'd like at this point in time to call the meeting to order.

On behalf of all committee members, welcome to all witnesses and guests in the room. We extend to everyone a very warm welcome.

This meeting is called pursuant to our Standing Orders, and today we're dealing with chapter 1, "National Security: Intelligence and Information Sharing", of the 2009 status report of the Auditor General of Canada.

The committee is very pleased to have with us today, first, from the Office of the Auditor General, Sheila Fraser, the Auditor General. She is accompanied this afternoon by the assistant auditor general, Hugh McRoberts; and principal, Gordon Stock.

From the Privy Council Office, we have Marie-Lucie Morin, national security advisor to the Prime Minister and associate secretary to the cabinet.

From the Department of Public Safety and Emergency Preparedness, we have the accounting officer and deputy minister, Suzanne Hurtubise.

From the Department of Transport, we again have the accounting officer and deputy minister, Louis Ranger. He's accompanied by Marc Grégoire, the assistant deputy minister.

From the Royal Canadian Mounted Police, we have Mr. Tim Killam, deputy commissioner, policing support services. He's accompanied by Madame Guylaine Dansereau, director of Canadian Criminal Real Time Identification Services.

Again, welcome everyone.

We do have a large crowd today, so I'd ask that you keep any opening comments to five minutes.

We're going to start with the Office of the Auditor General.

Ms. Fraser.

**Ms. Sheila Fraser (Auditor General of Canada, Office of the Auditor General of Canada):** Thank you, Mr. Chair. We thank you for inviting us to discuss chapter 1 of our 2009 status report, entitled "National Security: Intelligence and Information Sharing".

As you mentioned, I'm accompanied today by Hugh McRoberts, assistant auditor general; and Gordon Stock, the principal responsible for our audits of national security.

The audit examined progress the government has made since the audit observations made in chapter 10, "Other Audit Observations—Independent Reviews of Security and Intelligence Agencies", of our November 2003 report; and certain of our recommendations from chapter 3, "National Security in Canada—The 2001 Anti-Terrorism Initiative", of our March 2004 report.

[Translation]

I would like to start by saying that we were encouraged by the government's progress in addressing the deficiencies noted in our original audits. Overall, we found that the federal government had made satisfactory progress in 8 of the original 12 recommendations.

In 2003, we recommended that the government assess the level of review and reporting to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion. At the time of our follow-up audit, the government had completed its assessment and considerable preparatory work had been done. However, no decisions had been made on whether or when changes would be introduced.

We also found progress had been made in a number of other areas: organizing and coordinating priorities among federal departments and agencies involved in security; reducing the fingerprint backlog and progressing in its development of a computerized system to analyze digitized fingerprints, and improving the reliability of watch lists of individuals considered to be of interest to intelligence organizations.

[English]

In 2004 we noted that a barrier to information sharing was the lack of a government-wide system that would allow communication at the "secret" level among departments and agencies. While progress on this complex project was slow to start, better progress had been made in the latter period under examination; therefore, the government received a satisfactory rating for progress against this recommendation. However at the time of our audit, the project was still in the limited implementation stage and its success was contingent upon its receiving additional funding and user acceptance.

An area where we found little progress was in the balancing of privacy concerns with information sharing. The Department of Justice Canada had been tasked by the Deputy Minister Committee on National Security, which includes representatives from the Privy Council Office, the Treasury Board of Canada Secretariat, and Public Safety Canada, to prepare an inventory of legal problems related to the sharing of national security data. The Treasury Board of Canada Secretariat collected 16 instances where departments and agencies reported legal barriers to information sharing. However, resolution of these barriers has not been achieved and the Department of Justice Canada and the Treasury Board of Canada Secretariat have provided little direction to government departments and agencies.

We also found that Transport Canada and the Royal Canadian Mounted Police were not sharing criminal intelligence information effectively. Transport Canada had implemented additional procedures for screening applicants for access to secure areas of airports; however, the process did not include looking at all information contained in the RCMP data systems. In addition, there were indications that Transport Canada and the RCMP did not give full information to each other. As a result, Transport Canada may be granting clearance to high-risk individuals for work in secure areas of Canada's airports. As noted in our report, Transport Canada does not see its role as preventing criminal organizations from infiltrating airports. If it does prevent unlawful activity at airports as a result of its screening process for airport workers, this is seen as a side benefit.

[Translation]

In the world of security intelligence, information sharing is critical; therefore it is important that the government find a way of resolving legal constraints, where appropriate. And for Canadians to have confidence in their security and intelligence organizations, they need to know that government agencies and departments maintain a balance between protecting the privacy of individuals and ensuring national security.

Since the 31<sup>st</sup> of March 2009, the date we tabled our report, I understand that the RCMP and Transport Canada have signed a memorandum of agreement on information sharing, but we have not reviewed this document. For the other new recommendations contained in the chapter, the committee may wish to request from departments and agencies an action plan that addresses our recommendations.

Mr. Chair, thank you. That concludes my opening statement. We would be happy to respond to the committee's questions.

• (1535)

[English]

**The Chair:** Thank you very much, Ms. Fraser.

We'll now turn to Marie-Lucie Morin, the national security advisor to the Prime Minister and associate secretary to the cabinet, for her opening remarks.

[Translation]

**Ms. Marie-Lucie Morin (National Security Advisor to the Prime Minister and Associate Secretary to the Cabinet, Privy Council Office):** Mr. Chairman, members, I appreciate the

opportunity to share some of the accomplishments of the government in the area of security and intelligence.

I will not introduce my colleagues again given that Mr. Murphy has already done so.

Today therefore, I would like to briefly bring you up-to-date on our achievements within the context of the Auditor General's status report of March 31 and to present you with a description of our priorities for the way ahead.

The departments and agencies have made great headway on many issues identified in the original audits of 2003 and 2004. Specifically, the overall coordination of the security and intelligence community has improved. But some challenges remain, and those are challenges shared by all western democracies. We must strive to find the necessary balance between protecting the collective rights of Canadians to live in a secure environment under the umbrella provided by our security agencies, and respecting individual rights of Canadians.

As members of the committee can appreciate, there are some limitations to what can be said in this forum due to on-going investigations, sensitive operations, investigative methods, and cabinet confidence. But, as the Auditor General's report demonstrates, there's much that can be said about the work we do.

Allow me to first say a few words about the threats to the global environment. Terrorism and extremism remain global security challenges highlighted by brazen attacks in Mumbai, Islamabad and Lahore most recently. Canada cannot be complacent and act as if it is immune to the threats from both established and emerging terrorist groups.

Al-Qaeda has evolved and its satellite affiliates in the Maghreb, North-East Africa and South Asia are actively engaging in terrorism. The recent kidnapping of Robert Fowler and Louis Guay demonstrated, too harshly, the impact these regional groups can have.

Canada and its allies are also working to confront an increasingly sophisticated cyber threat. Not only are our own communications threatened, but the Internet itself, upon which we are all so dependent, is used to plan and execute terrorist attacks. Another continually evolving threat is the proliferation of weapons of mass destruction.

[English]

As you may recall, the position of national security advisor to the Prime Minister was created in 2003, very much as a reflection of the new security environment following the attacks of 2001. Three elements of my work are particularly relevant to the Auditor General's report.

First, my role is to support an integrated approach to intelligence. The collaboration and coordination among agencies within the security and intelligence community has improved significantly since 2004, a fact echoed by the Auditor General in her report. Intelligence priorities for the community are established annually by cabinet as required in the National Defence Act.

The community is working together in the implementation of priorities, which, in turn, has resulted in significant improvements in the use of our collection assets and the production of coordinated intelligence assessments on a range of threats and issues. While there has been progress, a number of community-wide challenges remain, particularly in the area of information-sharing between agencies. Information-sharing issues vary widely, reflecting the laws, mandates, and statutory requirements of individual departments, and there is no single solution that will address all of them.

Second, coordination among departments and agencies is also an essential component of my work. The Privy Council Office plays a key role in ensuring that the demands of the security environment are met in a coherent manner. We are fortunate, in fact, that in Canada we can achieve coordination in a single room. Our American partners have 17 agencies to work with. A robust committee structure exists up to the level of deputy minister to manage issues and tackle challenges.

Finally, Canada's international security and intelligence relationships are an important part of addressing the range of global interconnected threats we face. Canada provides high-quality intelligence to our partners and receives it in return. The benefits of these relationships are clear, and my recent travels have only confirmed that Canada is a respected contributor to the international security and intelligence community.

In this context, strengthening the Canada-U.S. relationship, particularly in the area of security and defence, remains a key priority. As with any relationship, there are irritants, but it goes without saying that the Canada-U.S. security and defence relationship is fundamentally important. This winter, during the visit of President Obama, the Prime Minister said "a threat to the US is a threat to Canada".

I conclude by saying that we are pleased with the findings of the Auditor General's report, which found that the government has made overall satisfactory progress in managing security intelligence. We collectively continue to address those areas where further progress is required.

Thank you.

• (1540)

**The Chair:** *Merci, madame Morin.*

We're now going to hear from Suzanne Hurtubise.

[Translation]

**Mrs. Suzanne Hurtubise (Deputy Minister, Department of Public Safety and Emergency Preparedness):** Thank you Mr. Chairman.

Mr. Chairman, members of the committee, I am pleased to be here today to discuss the progress made on the various recommendations stemming from the Auditor General's status report and ongoing challenges.

As mentioned by Ms. Morin, the government has made significant strides since 2004 towards a more integrated approach among agencies within the security and intelligence community.

[English]

In addition to the elements Madam Morin mentioned, the creation of the Government Operations Centre has improved the level of coordination. It allows for more effective and coordinated responses across all departments and agencies of the federal government, and as well enhances coordination with provinces and municipalities for issues as they arrive, including issues as diverse as natural disasters, such as recent flooding in Manitoba, pandemics, such as the recent outbreak of H1N1, or indeed any acts rooted in terrorism and extremism.

The security and intelligence community has worked collectively over the past two years to address all of the issues raised in the Auditor General's report. For example, through the committee structure established by the Privy Council Office, we now share and review post-exercise reports and recommendations with interested departments and agencies. We also now together review lessons learned from major events to help us better manage future events.

In terms of our approach to interoperability, we have shifted our focus to a more pragmatic, project-based approach aimed at enhancing information-sharing across the public safety and security community. Examples of such projects include the secret communications interoperability project and working with Canada's first-responder community in support of advancing interoperable radio and voice communications.

[Translation]

There remain very significant challenges as our risk environment evolves. While we are pleased with the progress made to date, we recognize that there is a need for further work in some areas.

Thank you, Mr. Chairman. I would be pleased to respond to the questions of committee members.

[English]

**Mr. David Christopherson (Hamilton Centre, NDP):** I have a point of order, Mr. Chair.

**The Chair:** Go ahead, Mr. Christopherson.

**Mr. David Christopherson:** Mr. Chair, would you please ask the clerk to get a copy of that immediately, and give us copies of that statement?

**The Chair:** I should point out to Madame Hurtubise, and I believe to Mr. Ranger too, that normally in this committee we would expect to receive a copy of your opening statement. I believe you've been before this committee before, Madame Hurtubise.

We don't have copies, Mr. Christopherson. We did of the Auditor General's remarks.

• (1545)

**Mr. David Christopherson:** I realize that, Chair. I was asking if you could direct the clerk to get a copy and circulate it now.

**The Chair:** Do they have it in both official languages? We can't circulate it if....

Is it available in both French and English? Mr. Ranger, do you have a copy of your statement in both French and English?

**Mr. Louis Ranger (Deputy Minister, Department of Transport):** I do. We provided copies. We do have extra copies.

**The Chair:** You did provide us copies?

**Mr. Louis Ranger:** I understand we did.

**The Chair:** We understand that the opening comments from Madame Hurtubise are available in both official languages. They are being copied now and will be made available and circulated very shortly. I understand that the opening remarks of Mr. Ranger are only in English, so we'll just ask you to present now.

**Mr. Louis Ranger:** My apologies.

Mr. Chair, members of the committee, thank you for the opportunity to address the comments in the Auditor General's follow-up status report. At the outset, I would like to say that I welcome the opportunity to describe the concrete steps Transport Canada has taken to improve intelligence and information sharing. I also welcome the opportunity to answer any questions the committee may have.

Transport Canada is the lead department, as you know, for transportation security in Canada. Our job is to prevent unlawful interference with civil aviation and marine and surface transportation, as well as to provide oversight to ensure compliance with regulatory requirements.

[*Translation*]

Overall security at our airports and ports is a shared responsibility among departments and agencies that work closely with Transport Canada, including the RCMP, Canada Border Service Agency, the Canadian Air Transportation Security Authority, Canadian Security Intelligence Service, police of jurisdiction and local airport and port authorities.

[*English*]

Our transportation security clearance program was created in 1986, in the aftermath of Air India, to prevent unlawful interference with civil aviation. The program accomplishes this by assessing the risk posed by individuals who by the nature of their work require access to a restricted area of an airport. Since the program's inception, Transport Canada has processed over 600,000 applications. On average, we receive 40,000 to 45,000 applications annually. Currently there are 115,000 active transportation security clearances at airports and ports in Canada.

[*Translation*]

Transport Canada verifies the suitability of each transportation security clearance applicant with the RCMP, CSIS, and, if necessary, Citizenship and Immigration Canada. If Transport Canada obtains credible information that an applicant or an existing pass holder poses a transportation security risk, the department responds immediately by refusing, suspending or cancelling the clearance.

[*English*]

As recognized by the Auditor General, we continually strive to improve the program by implementing additional procedures. For example, following the Auditor General's recommendation of 2004, Transport Canada and the RCMP negotiated an inaugural MOU for background checks and subsequently did a review of all existing

transportation security clearances. As well, we began requesting applicants who live outside the country for a significant period of time to provide five years of verifiable information.

In addition, we introduced the marine transportation security clearance program for workers at the marine ports and facilities. An action plan has been developed to address the issues raised by the recent Auditor General's report, and progress is ongoing. Here are some of the concrete measures included in that plan.

First, on April 8, Transport Canada and the RCMP entered into a new information-sharing agreement to provide expanded criminal background checks on individuals working in restricted areas of Canada's transportation system. Transport Canada will share more complete data with the RCMP, and the RCMP, in turn, will perform expanded background checks using multiple criminal databases available to the RCMP.

Second, we are developing strengthened guidelines and criteria against which applicants will be assessed.

Third, we are amending the transport security clearance application form to address new consent and new criteria requirements.

Fourth, Transport Canada will review all current security clearance holders—all of them—based on these improved procedures to identify any previously unknown adverse information that could suggest that an individual may pose a risk to civil aviation.

• (1550)

[*Translation*]

All the while, we have been working closely with the Department of Justice to address privacy issues and these efforts are reflected in enhanced information sharing provisions in the new memorandum of understanding. Our action plan is ambitious. We are convinced, however, that it is attainable with the assistance of our many partners, and we remain committed to working with them to enhance intelligence information sharing and to improve security in all modes of transportation, consistent with the recommendations of the Auditor General.

[*English*]

Finally, I'd like to take this opportunity to recognize the level of cooperation that has prevailed throughout this audit between Transport Canada, the RCMP, and the Office of the Auditor General. I and my team believe that our security screening process will be improved as a result of this audit.

Thank you, Mr. Chair.

**The Chair:** Thank you, Mr. Ranger.

Deputy Commissioner Killam, you have opening comments. I'll turn the floor over to you now.

[*Translation*]

**D/Commr Tim Killam (Deputy Commissioner, Policing Support Services, Royal Canadian Mounted Police):** Thank you Mr. Chairman.

I'm pleased to appear today on behalf of the RCMP and Commissioner Elliott.

[English]

The commissioner has asked me to express his appreciation for the opportunity for the RCMP to participate today and to convey his regrets for not being here.

The manner in which the RCMP conducts national security criminal investigations and manages criminal intelligence has evolved considerably over recent years. We continue to adapt to our ever-changing operating environment, as we build on opportunities for improvement and greater accountability in how we investigate criminal threats to national security and share criminal intelligence.

The recommendations of Justice O'Connor, as well as reports from the Auditor General and the Privacy Commissioner, have been instrumental in helping plan the way forward. In fact, the recommendations in part one of Justice O'Connor's report are today at the very heart of the RCMP's redesigned approach to national security criminal investigations.

We continue to strengthen our good relations with law enforcement and government partners. The new memorandum of understanding with Transport Canada will provide greater safety to all Canadians by enhancing security at our airports and marine ports. Let me stress that maintaining the trust and support of Canadians is fundamental to the transformation under way in our national security and criminal intelligence programs. We have enjoyed a number of high-profile operational successes, but we do need Canadians behind us to perform at our best.

In closing, Mr. Chair, we are all well aware that there is no single agency uniquely positioned to tackle all threats to our national security. Mitigating the perils of organized crime and terrorism requires a collaborative and coordinated effort among domestic and foreign enforcement, intelligence, and government partners.

Key to this collaboration is gathering, sharing, and managing information effectively to protect Canadians while respecting individual rights and freedoms. The RCMP is fully committed to both principles.

We thank the committee for its ongoing review of criminal intelligence-sharing in Canada, and we appreciate your support in improving national security for all Canadians.

Thank you. I would be pleased to respond to the questions of committee members.

**The Chair:** Thank you, Deputy Commissioner Killam.

Ms. Ratansi.

**Ms. Yasmin Ratansi (Don Valley East, Lib.):** Thank you all for being here.

I do not know where to begin, but I'm going to begin with the Auditor General. Ms. Fraser, you stated that the need for effective security is important, that Canadians are sophisticated enough to know the events in the world and their interplay, and that local events have made it imperative that we have solid security systems. However, you also stated that for Canadians to have confidence in their security intelligence system they need to know that the government agencies and departments maintain a balance between

protecting the privacy of citizens and national security. You go on to say that you would have wanted an external, independent review. You suggest a system of external review and disclosure proportionate to the level of intrusion. There is preparatory work done, but it is not complete.

What are the risks this proportionality poses for Canadians? What comes to mind is Maher Arar, whose case has been our biggest albatross. It has been a shame on Canadians that we did it. Could you help me to understand what the risks will be? How would this independent review help alleviate the problems? I will ask all the agencies to answer. What lessons have you learned from the Air India inquiry, from the Maher Arar case and the other inquiries? If you have learned any lessons, why do we still have Canadian citizens sitting in jail in China and in Sudan?

• (1555)

**Ms. Sheila Fraser:** The report notes in exhibit 1.1 the various departments and agencies that are involved in intelligence activities. As we point out in this report and in previous reports, the level of external review or oversight varies significantly. There are some such as CSIS that have the Security Intelligence Review Committee and an Inspector General, but there are other departments, like the Department of National Defence, that have no external review. As to the RCMP, the Commission for Public Complaints is quite limited in the work it can do. It can only accept complaints, and the Commissioner of the RCMP determines what information the commission can have. As we point out, the degree of oversight varies significantly.

Many of these agencies and departments have received additional powers under new legislation, anti-terrorism legislation. We believe we need an ongoing review to ensure that there is external oversight over potential intrusion into private information and that the agencies are carrying out their mandates within the legal authorities given to them.

**Ms. Yasmin Ratansi:** Fair enough.

Who would like to tackle the question of lessons learned? Perhaps the RCMP would like to go with lessons learned from the Maher Arar inquiry and the Air India inquiry. What are the steps forward, and how can we ensure that we are not supplying information that will put Canadian citizens in jail in China and in Sudan?

**D/Commr Tim Killam:** The RCMP has implemented all the recommendations of the O'Connor inquiry. Changes to the national security criminal investigations program have focused on monitoring all national security criminal investigations through centralized control in Ottawa. We have enhanced our relationships with CSIS, DFAIT, and law enforcement partners. We've expanded and improved training, and we've made improvements to information-sharing practices. Some of these policy changes have served to ensure that information is properly shared and assessed for reliability and accuracy. We have written caveats attached to every piece of information in national security investigations. DFAIT is properly consulted, and the national security criminal investigations are centrally monitored and controlled for quality.

• (1600)

**Ms. Yasmin Ratansi:** Would you like to take a go at it, Monsieur?

**Mr. Louis Ranger:** Yes, I would. It's not just lessons learned; it's also things we've done. Two very specific measures were taken. I mentioned one in my introductory remarks: the background checks on airport workers, which is something that was done following and as a result of the Air India accident. But also, there is the matching of passengers and baggage, which is something that was identified as a very specific issue and which we have had in place for many years as a direct result of and as a lesson learned from Air India.

**Ms. Yasmin Ratansi:** However, according to the Auditor General's remarks, the report says that "Transport Canada and the RCMP did not give full information to each other" and "Transport Canada may be granting clearance to high risk individuals for work in secure areas". It also says, "As noted in our report, Transport Canada does not see its role as preventing criminal organizations from infiltrating airports."

Now, that's just incredulous. Can you please tell me why there is no information sharing and what is going on? Why are the silos not breaking down? How can you talk about reliability of information and the transmission of information, which is what the Maher Arar inquiry was demanding, a reliability of information and seeing that it is shared properly? Plus, there is this non-coordination between the two departments.

**Mr. Louis Ranger:** We've come a long way. The Auditor General looked at the process we had in place. There was an initial MOU. There were difficulties on both sides, with us having difficulty in sharing private information and the RCMP not being able to access all the databases, but we've come a long way. As we mentioned, on April 8, we did sign an MOU that addresses both sets of issues.

For example, on the privacy side, we now seek very explicit consent from applicants in terms of being able to share with the RCMP detailed information on not only their own history, but on history regarding their spouse, and also consent regarding to what extent the RCMP can share that information with others. We now have the consent of the applicant, which has cleared the way and has come a long way to addressing the privacy issue.

**The Chair:** Thank you.

*Madame Faillie, sept minutes.*

[Translation]

**Ms. Meili Faillie (Vaudreuil-Soulanges, BQ):** Thank you Mr. Chairman.

My questions will in the main be on the issues that my colleague raised.

The Privy Council officials mentioned cyber threats. Can you tell us whether or not National Defence, Transport Canada or any other departments have also received cyberthreats?

Can you tell us about the telecommunications monitoring systems? Are there currently any investigations into these systems?

My colleague also raised the issue of intelligence reliability and intelligence management security. Can you also talk to us about that?

**Ms. Marie-Lucie Morin:** Thank you, Ms. Faillie.

In my opening comments I did refer to cyber threats that are a danger to government installations all over the world as well as installations belonging to industry, the private sector and the non-governmental sector.

Of course we want to protect ourselves against these attacks. For security reasons I cannot refer to specific cases in which we could have been victims of these attacks. I can only tell you that we are very aware that these threats exist. We are currently developing policies to deal with these now and in the future. We know that we'll be living in a world where the "cyber" aspect will become more and more significant.

• (1605)

**Ms. Meili Faillie:** I understand the cyberthreat issue, I'm aware of that. However, I would like to know if departments are taking any action in that regard. We're talking about national security and intelligence security. You say you went to Afghanistan, did National Defence...?

Earlier my colleague also raised the issue of airport security, and all areas that fall under national security. If this is public information, can you tell us whether or not National Defence has been the subject of cyberthreats over the past year?

**Ms. Marie-Lucie Morin:** I can't share that information with you and no, I have not had the opportunity to travel to Afghanistan as of yet, Ms. Faillie.

Mr. Ranger, are you aware of what is happening with airports?

**Mr. Louis Ranger:** I can't provide any specific examples.

**Ms. Meili Faillie:** Who is currently responsible for telecommunications security for the federal government?

**Ms. Marie-Lucie Morin:** It's the CSE, the Communications Security Establishment, under the Department of National Defence.

**Ms. Meili Faillie:** Which company is responsible for that?

**Ms. Marie-Lucie Morin:** There's no company, it is a government agency.



**Ms. Meili Faille:** It's a government agency, but do they not use sub-contractors in the telecommunications sector?

**Ms. Marie-Lucie Morin:** Not to my knowledge, Madam.

**Ms. Meili Faille:** Then it's not Bell, it's not Telus, no one is responsible for running your telecommunications system?

**Ms. Marie-Lucie Morin:** Yes, we use private companies for the purposes of telecommunication.

**Ms. Meili Faille:** Fine. With respect to the Royal Canadian Mounted Police, apparently there's a backlog of applications regarding criminal records. Is there currently a shortage of analysts for criminal records?

[English]

**D/Commr Tim Killam:** I'll ask Guylaine Dansereau to answer.

[Translation]

**Ms. Guylaine Dansereau (Director, Canadian Criminal Real Time Identification Services, Royal Canadian Mounted Police):** With respect to criminal record analysis, some positions have become vacant following the information technology renewal. We use a very sophisticated staffing process to fill our vacant positions. We have filled 70 permanent positions.

**Ms. Meili Faille:** Seventy positions have been filled over the past year.

**Ms. Guylaine Dansereau:** Rather over the past few years. However, there are many people retiring, and some are leaving because of promotions. We always have an ongoing staffing process.

**Ms. Meili Faille:** What is your vacancy rate?

**Ms. Guylaine Dansereau:** The vacancy rate with respect to the...? I do not have the exact numbers.

**Ms. Meili Faille:** Perhaps you could provide them to us.

**Ms. Guylaine Dansereau:** Yes, we could do that.

**Ms. Meili Faille:** What has the impact been of the delay in 472,995 cases, in the month of April 2009, on the administration of justice, hiring in the public service and in the private sector, granting citizenship, etc.? There seem to be several problems.

As members of Parliament, we often have many citizens coming to speak to us about this issue. This also disturbs the hiring process and the functioning of the legal system.

Have you done an impact analysis in terms of the daily lives of people or businesses, or even the public service?

**Ms. Guylaine Dansereau:** We haven't done an impact analysis. The RCMP is not responsible for security issues, that falls under the department. We're only responsible for verifying criminal records.

**Ms. Meili Faille:** I understand that you wouldn't be aware of the impact on the whole of the process, but perhaps Privy Council could give us an analysis of the situation?

**Ms. Marie-Lucie Morin:** Unfortunately, I am not in a position to answer that question either, Ms. Faille.

**Ms. Meili Faille:** I am rather severe aren't I? I have another question about the Canada Border Services Agency, whose officials are absent today. There's a recommendation from the Auditor General in point 1.82 that involves improvements.

In light of the progress you have made in your exchanges with the agency, what is the current situation with respect the reliability of intelligence that this agency has?

• (1610)

**Ms. Marie-Lucie Morin:** Once again, I cannot answer that question. We could ask the agency to provide you with a written answer, Ms. Faille.

**Ms. Meili Faille:** Fine. Thank you.

[English]

**The Chair:** Okay. Before we go to the next witness, there were some issues.... They were going to get back to you on the vacancy rate within two weeks. Is that fine, Madame? Okay.

Mr. Christopherson, you have seven minutes.

**Mr. David Christopherson:** Thank you, Chair, and thank you all for your attendance today. It's much appreciated.

I have to confess to being a little confused, only because of the number of times memoranda and information-sharing were mentioned.

I will get to that, but I want to ask one straight-up question. It stems from a question asked by one of my colleagues. The Auditor General has noted that Transport Canada does not see its role as preventing criminal organizations from infiltrating airports. There were a lot of problems with information-sharing.

My question is this. If someone gets through and ultimately gets a security clearance to work in an airport, and it's found that they shouldn't have gotten the clearance, for whatever reason, who is responsible? Is it the RCMP or is it Transport Canada?

**Mr. Louis Ranger:** It is Transport Canada. If the information was provided to Transport, we act immediately. If the RCMP has new information, they will provide it to us and we will yank the person out immediately. That's how it works.

**Mr. David Christopherson:** Okay, but if there was a mistake—we're all human—that mistake is yours, technically, but the RCMP, on analysis....

**Mr. Louis Ranger:** We're on the front line. We deliver the clearance. We seek information from the RCMP, CSIS, and Citizenship and Immigration. But we are responsible for issuing the clearance based on the information we have. If we have more information, if a mistake was made, we will act accordingly. We will notify the individual that new information has become available that has forced us to withdraw the clearance.

**Mr. David Christopherson:** That means that this statement is no longer accurate. You now accept your role as having that responsibility.

**Mr. Louis Ranger:** I'm not sure what statement you are referring to.

**Mr. David Christopherson:** It is the one in the Auditor General's report we just heard 20 minutes ago, on page 3, paragraph....

**Mr. Marc Grégoire (Assistant Deputy Minister, Safety and Security Group, Department of Transport):** If I may, I think it's important to note here that your question is very good in that every system has some gaps and some inherent risks. This is why we have a multi-layered approach to security. We have other systems in place.

For instance, we screen non-passengers or workers when they go to work. The government just gave additional money, in its latest budget, to do more screening of workers. We're going to create new areas around the apron to do further screening. We have established the restricted area identification card, which is a further security enhancement. The cards contain biometric information of all the workers in the restricted areas. All these together comprise the security net. We can't rely on any one of those systems, but all of them together form the security net.

**Mr. David Christopherson:** Thank you.

I appreciate that, but my question was a simple one. The statement was made by the Auditor General based on the information she had at the time. Now I'm hearing you taking responsibility. I'm just trying to determine whether you have now changed your position.

I see that the Auditor General is trying to get in, so I'll offer her the floor.

**Ms. Sheila Fraser:** Mr. Chair, if I could, when we did the audit, Transport officials referred to their authority with respect to unlawful interference with civil aviation, and that has been interpreted to mean physical threat to aircraft and passengers, not criminal activity within an airport. It is a physical threat to aircraft. I note that the deputy uses the same terminology in his statement in talking about unlawful interference with civil aviation.

I think this is a very important point for the committee to clarify: the interpretation of the legal authorities that have been given to Transport Canada in this regard.

**The Chair:** Mr. Ranger.

**Mr. Louis Ranger:** I understand your question better. We're not involved in the control of narcotics or that kind of thing. Our mandate is quite clearly defined in the Aeronautics Act. It relates to making regulations respecting prevention of unlawful interference with civil aviation. We're always ready and more than happy to help other processes deal with the broader issues, but we deal strictly with unlawful interference with civil aviation.

• (1615)

**Mr. David Christopherson:** Thank you.

Again, I was mentioning the different pieces. On page 2 of the audit, it reads, "In addition, the memorandum of understanding between the RCMP and Transport Canada regarding information sharing was terminated by the RCMP..."

Is that the same issue, same document? Because I also note, looking at page 11, paragraph 1.21, that it says, "These national security units were not always functioning well. For example, not all relevant agencies were contributing staff to INSAC, and a memorandum of understanding between the RCMP and CSIS to share information had expired." That's why I'm talking about multiple agreements and sharing.

Can you help me understand this? Is that taken care of? Do you now have an agreement with CSIS?

**Mr. Louis Ranger:** I can clarify my part. I have a mandate under the Aeronautics Act. In delivering that mandate, we work with the RCMP. To make it clear, we have an MOU that defines our relationship.

**Mr. David Christopherson:** Right. So I guess my question would be to the RCMP representatives, because it's their memorandum of understanding that expired.

Where are we on that one, sir?

**D/Commr Tim Killam:** You're talking about two MOUs. The one with CSIS was with regard to conducting national security investigations.

I want to make it very clear that the RCMP does not do intelligence investigations. It does criminal investigations. We get all our intelligence from CSIS. CSIS is the front end, and we would be passed over. The memorandum of understanding is in how we interact at that point of passing over.

**Mr. David Christopherson:** That's now renewed, sir?

**D/Commr Tim Killam:** That has been renewed. I can't give you the exact date, but it was renewed quite a while back.

**Mrs. Suzanne Hurtubise:** I believe it was December of 2006.

**D/Commr Tim Killam:** Yes. It was quite a while back; I was involved in that.

**Mr. David Christopherson:** Okay. That's helpful.

**D/Commr Tim Killam:** The MOU with regard to Transport had to do with sharing of criminal intelligence from the databases that we have and that we are stewards of. There are different kinds of databases. We're the stewards for the national police services, CPIC and all kinds of others. It's not just our information; it's also that of other police agencies.

There were issues around how much information we were getting from Transport that would allow us to better do our searches. As well, there were issues around privacy and legal issues that were quite complex and took some time to hammer out, but we were able to do that.

**Mr. David Christopherson:** With these memorandums in place now, does that now also eliminate the concern around consensus decision-making? That delay is no longer built into the system, as the auditor mentioned on page 11, in paragraph 1.19?

**Ms. Sheila Fraser:** I can certainly talk to that.

Paragraph 1.19 refers to what we found in 2004. Paragraph 1.27 is what the situation was at the time of our audit.

You will note that in paragraph 1.28 we mention the new memorandum of understanding between the RCMP and CSIS, but we indicate that the committee still works very much on a consensus basis, so at times there can be delays in—

**Mr. David Christopherson:** The question is still relevant, then. It's still timely.

**Ms. Sheila Fraser:** Yes, absolutely.

**Mr. David Christopherson:** Okay.

Hopefully I can get an answer on how you're going to grapple with that.

**D/Commr Tim Killam:** Perhaps I can get more clarification on the question. Are you discussing a time gap with regard to sharing of information with CSIS?

**Mr. David Christopherson:** Well, to the best of my knowledge, what we're talking about is that a number of agencies come together to make decisions around what they're going to do with certain information, or how they're going to get information. Because it was on a consensus basis, often decisions weren't made. They couldn't come to an agreement, so it would wait.

The auditor is pointing out that this delay is a problem in the decision-making process in terms of security. She's indicating, as you just heard, that it still remains at least a question, if not a concern.

Is that fair...?

Yes. Okay.

**D/Commr Tim Killam:** I'm not sure I can answer that. In terms of criminal investigations and a national security point of view, there's no consensus. It's between CSIS and ourselves. We are independent with regard to when and how we start a criminal investigation.

We get information from CSIS on intelligence with regard to a target, or a number of targets. At that point, we continue independently with our investigations. There's no consensus.

I'm not sure exactly what issue we're talking about.

• (1620)

**The Chair:** We have to move on, Mr. Christopherson. You'll have another slot later on.

Mr. Saxton, you have seven minutes.

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

Thank you to all for coming out here today.

Madam Morin, in your opinion, are we safer today than we were in 2001, and if so, why?

**Ms. Marie-Lucie Morin:** Mr. Saxton, that's a very big question. I would have to begin by acknowledging that we are living in a very complex world from a security environment point of view. You all saw yesterday what happened in North Korea, so the complexity of the challenges we are facing has grown, if anything.

This being said, I believe we are much better organized today to face those challenges. From a coordination point of view, from an integration of intelligence point of view, I do believe that we have an

excellent security and intelligence apparatus in Canada. So I would tell you that I personally believe that much progress has been made since 2001 to bring this level of coherence and coordination that the Auditor General referred to twice before in her audits. We do have a very comprehensive deputy ministerial committee structure to analyze issues, to provide recommendations to government on policy. I believe this structure actually is serving the government and the country very well.

I am confident that we have done much to achieve the objectives of thorough coordination when it comes to security and intelligence. We have to remain vigilant, and we still have some progress to achieve.

That's what I would answer to that question. Thank you.

**Mr. Andrew Saxton:** Thank you.

Can you share with us some of the actions that have been taken to help us become better prepared, as you said we are now?

**Ms. Marie-Lucie Morin:** Certainly. First of all, I should refer to the yearly process of determining priorities for the intelligence community. As departments and agencies, we do take a full scan of security and intelligence challenges. We distill those, and on the basis of that analysis we are able on a yearly basis to present to the government recommendations in terms of intelligence priorities. So this is a process that I believe works much better today than was the case in years past.

What we have done as well is we have struck a number of working groups on very specific issues that we believe require specific attention on the part of the community. So we have both very broad discussions around what I would call horizontal challenges from a security point of view—they'd be, for example, the situation today in Afghanistan or Pakistan—and we will also meet and discuss very discrete issues as they relate to national security and intelligence.

My colleagues all work with me in this coordinated structure, and I'm quite confident they would agree that we are working very effectively as a community.

Perhaps one more point that I would like to volunteer is that of course we have here a Westminster style of government. The ultimate accountability for the various ministries and agencies goes to ministers, but the way we have sort of constructed our work around the security and intelligence community is very much similar to, for example, the United Kingdom, Australia, or New Zealand. So inasmuch as they are very important partners for us from a national security point of view, we are also very mindful of the value of exchanging best practices as we seek to ameliorate the way we carry out our duties here.

Thank you very much.

• (1625)

**Mr. Andrew Saxton:** Thank you, Madame Morin.

My next question is for the Auditor General. Madam Auditor General, can you explain to us what the government has done lately that assures that Transport Canada and the RCMP are working better together?

**Ms. Sheila Fraser:** Thank you, Mr. Chair.

As I noted in the opening statement, we are aware that the new memorandum of understanding was signed in early April, I believe. We of course have not assessed what kind of information exchange is going on, but we certainly view that as a positive step.

**Mr. Andrew Saxton:** Thank you.

My final question is for the deputy minister. Can you elaborate on this new memorandum of understanding for us, please?

**Mr. Louis Ranger:** I indicated earlier that one of the issues was of privacy of information, and we are now building in a new questionnaire and a new application form, a pretty extensive section, where we would have very explicit consent from the applicant so the information can be used.

Another issue is obvious—a resource issue. I'll give you numbers: 40,000 to 45,000 applications a year. In my department alone we have 48 people reviewing that full-time, not counting resources from the RCMP. As we discuss the heavier workload and as we request the RCMP to make better use of all the databases, there are resource implications, and we have come to an agreement on how we will help support the resource issue. The RCMP has also contributed to that solution, so it's a joint effort. But I must say, this has come a long way in helping us establish a very stable working relationship, and it's a five-year agreement.

**Mr. Andrew Saxton:** Thank you very much.

No further questions, Mr. Chair.

**The Chair:** Thank you very much, Mr. Saxton.

Madame Zarac, four minutes.

[*Translation*]

**Mrs. Lise Zarac (LaSalle—Émard, Lib.):** Thank you, Mr. Chairman.

My question is for Ms. Fraser. You mentioned the achievements to date. You also raised the fact that implementation is very dependent on finances. I am concerned about that.

Shouldn't funding for an area as important as that of national security be a priority? I would like to hear your comments on that. What is being done in order to obtain the funding that is necessary to implement those important projects?

**Ms. Sheila Fraser:** I believe that the issue of funding is mainly related to computerized exchanges of information, where implementation is limited. The report indicates that completing a project depends on funding.

Choosing our priorities depends on several factors including the fiscal framework, other priorities and availability of other priorities within the department.

I don't have any more information on the current situation. One of the government's realities is that funding is voted in only for one year at a time. Therefore, there is always uncertainty for projects that are spread out over several years.

**Mrs. Lise Zarac:** We're talking about problems that have existed since 2004, as you pointed out. There has been a lack of funding and not just for this year.

Were you talking about the secret communications interoperability project?

**Ms. Sheila Fraser:** Yes. That's it.

**Mrs. Lise Zarac:** You mentioned that it's underfunded. Who's responsible for implementing that project?

**Ms. Sheila Fraser:** Ms. Hurtubise's department. She could perhaps give you more information.

**Mrs. Lise Zarac:** It's very important if we're talking about information exchanges.

• (1630)

**Mrs. Suzanne Hurtubise:** That's right. A few years ago, we were given a mandate to develop a system that allows for secret communications. We succeeded, with the assistance of several other departments and organizations, including the Communications Security Establishment Canada that we mentioned earlier, in developing and testing such a system. It was tested and now we can use it. We know that it is operational because we established a pilot project. The system is now ready to be implemented, if so desired.

The first stage has been completed, and everything has been done from a technical point of view. Users have tested it. Everything is ready including the memorandum of understanding. We are in the middle of discussions with several other departments in order to determine whether or not there is a will to continue and go ahead with this project.

I absolutely agree with you. This project and this system are extremely important in order to allow secret communications.

**Mrs. Lise Zarac:** I'm surprised to hear you say “if there's a will”. Why wouldn't there be?

**Mrs. Suzanne Hurtubise:** My goal wasn't to imply that there is no will. I simply want to say, as the Auditor General mentioned, that choices have to be made in order to fund various projects. Now that the pilot project is finished and that the system has been properly tested and deemed operational, we have to determine how to implement it.

**Mrs. Lise Zarac:** Have there been any forecasts of the implementation costs?

**Mrs. Suzanne Hurtubise:** I did ask that question as a matter of fact, but no one could tell me what the cost would be. I was told that it would depend on the extent of the system and the number of departments that want to use it. The more users there are, the less the cost. That is the stage which we are at.

**Mrs. Lise Zarac:** Thank you, Madam.

[*English*]

**The Chair:** Mr. Kramp, you have four minutes.

**Mr. Daryl Kramp (Prince Edward—Hastings, CPC):** Thank you, Chair, and welcome to our guests.

Like Mr. Christopherson and Mr. Murphy here, I sat on public accounts after the 2004 report, and quite frankly, we were more than alarmed. It was frightening to see just how insecure we were and the ridiculous silo mentality that existed back then between our agencies and the tremendous lack of communication. It certainly did not serve the Canadian public well, and I can tell you, I'm really encouraged to see the movement forward.

There are difficulties yet and some things to overcome, but whether it's ITAC or the Government Operations Centre now, or whether it's all the MOUs that are moving forward, it's tremendously encouraging. It just gives great credence to the value of that original report. I think we now have not a bit of a wake-up call here yet, but the job is not done. As Madame Morin quickly stated, one of the biggest difficulties we have is that every time we have a problem today, it will be a new problem tomorrow. So we're steadily adapting and modifying to the challenges we have.

What I'm really interested in is just how effective and coordinated our communications are between all these organizations in two components. One is the actual willingness, or the MOUs—in other words, basically, policy. The other one is the technology.

In the past, we had a tremendous breakdown where one system couldn't even communicate effectively with another. What is our technological capacity right now? Are we up to snuff, or are we years behind where we need to be to use our technology effectively?

Who would like to handle that?

**Mrs. Suzanne Hurtubise:** Thank you very much for your question.

I should probably say that I'm not a technology expert. There are technology experts. But I won't speak to the policy for now; I'll just speak to technology.

You're quite right, technology is critical. How we communicate—just in answering your colleague's question—points to the need to be able to communicate at a secret level. We have not had a system in government to do that. We now have pilot-tested a program that is certified as operational and functioning. It is available for rollout if we want that. That's very important.

We also have, on the other hand, some very strong world-standard telecommunications capacity within the government to address some of the issues around cybersecurity, for example, and to address some questions of counter-terrorism.

The other most effective tool of communications is for everybody to be on the same wavelength and for everybody to have the same priorities and to move forward together on that.

So we are working very hard on the technological front. I think there's still a lot to be done, but we have already achieved a fair bit.

• (1635)

**Mr. Daryl Kramp:** I'm concerned as well about the number of MOUs signed, whether between CSIS and the RCMP or Transport Canada. That's paper. Are they being implemented? That's what we need to know. Are they being followed through? Is the intent there and is the composition of the MOUs being enacted, not just in theory but in principle? I'd like to know.

Maybe you can tell us, Madam Fraser, whether you're suggesting that there is complete adherence to these MOUs, or are they basically just paying lip service to them?

**Ms. Sheila Fraser:** Thank you, Chair.

Obviously, we noted an issue with the MOU between Transport Canada and the RCMP. We've heard that a new MOU has been signed, and it would appear that this has been resolved.

I think it's important to understand that these MOUs are really critical, for a number of reasons. Departments just can't share information freely, so they have to have those memoranda in place to clarify what information can be shared, how it's protected, and all the rest of it. One of the big issues that came up in this report was the whole issue of privacy. It was raised several times. It is a really fundamental issue that has to be addressed going forward on the whole intelligence information-sharing issue.

We do note in the report—it was mentioned earlier—that the MOU between the RCMP and CSIS was updated. We didn't note any particular problems with information-sharing there, but we didn't go through an analysis of each one to see how well they were working.

**Mr. Daryl Kramp:** Thank you.

**The Chair:** *Monsieur Pomerleau, quatre minutes.*

[*Translation*]

**Mr. Roger Pomerleau (Drummond, BQ):** Thank you very much, Mr. Chairman.

I wish to thank the witnesses for appearing before us here today.

Mr. Ranger, as you know, when you decide to run as a member of Parliament for a political party, you sign a document authorizing the party to conduct a police investigation on you. This is openly admitted. However, you're saying that you still don't have that type of document, that you're thinking about putting one in place.

**Mr. Louis Ranger:** That will be done very quickly. We're currently designing the new application forms. A very long section was added, where the applicant consents to disclosure of their history of the past five years, including information on their spouse. It goes even further by authorizing the RCMP to hold information for a certain number of years and to share it with other police forces, for example. This will unblock an awful lot of...

**Mr. Roger Pomerleau:** Even with such a form, you're saying that one of the problems is the quantity of information to be processed. You receive over 40,000 applications a year. A few years ago, the Bloc Québécois had the longitudinal labour force file dismantled. It had existed under the Liberals and 37 million Canadians were listed in it. I wanted to know what that file contained and I asked for my personal file. I gave my name and my social insurance number. Five days later, I received quite a voluminous file.

I have a lot of trouble understanding that with a name, an address and a social insurance number, the RCMP is incapable of obtaining something more quickly than what you seem to be claiming. Does it take a long time to obtain information on someone?

**Mr. Louis Ranger:** According to the standards we have set, it takes 30 days for a new applicant. For someone renewing a pass, it takes 10 days.

**Mr. Roger Pomerleau:** All right.

Mr. Killam, the Library of Parliament gave us briefing notes before this meeting. In them we can read what follows:

An RCMP analysis found that there were more than 60 airport employees with criminal links at Canada's largest airports, and many organized crime groups were found working within or using these airports.

I was completely stunned to read this. Is this accurate?

My colleague, who collects all the paper she can find, has an article from the Canadian Press dated September 25, 2006. It talks about a report that was prepared by Mr. Jean-Pierre Fortin, of the Customs and Immigration Union, in which he says that the Customs Officers Union is worried about airport security, because customs officers are being pressured by unknown persons to not visit certain planes and not carry out certain inspections. This even led to Mr. Cannon demanding an investigation. A few months later, Mr. Cannon said that all the investigations had revealed that Montreal airports were perfectly safe.

There's a lot of contradictory information. I get the impression that the situation in our ports and airports is the same. You are not reassuring us; you have not demonstrated that organized crime has not infiltrated these places. What are your thoughts on this?

•(1640)

[English]

**D/Commr Tim Killam:** I think you speak to a project that our criminal intelligence folks did just recently with regard to class 1 airports, the large airports in Canada.

We looked for any gaps in security for our purposes, to be able to know where we would target our investigations with regard to organized crime. It verified that there were 58 organized crime groups working within or using the eight class 1 airports across Canada. And we found a number of workers within secure areas who had some association or had close association with organized crime.

This was shared with Transport Canada, and this was also one of the catalysts to making sure we get over the large legal hurdles with regard to sharing information between Transport Canada and the RCMP. We could ensure that we looked at all our databases and were able to take the right information from Transport Canada to do our search with regard to that person and their suitability. That's why my previous statement was, I believe, with the agreement we have and what we're working on right now—we are looking at all the databases we have access to—the airports and the marine ports are and will be safer, for those who want to apply and work in those areas.

**The Chair:** Thank you, Monsieur Pomerleau.

Mr. Shipley, four minutes.

**Mr. Bev Shipley (Lambton—Kent—Middlesex, CPC):** Thank you very much, Mr. Chair, and to our guests for being here.

I'd like to go to Ms. Hurtubise, and I would also like to hear from the RCMP and Transport Canada to help me understand.

Ms. Hurtubise, in your presentation you talked about the coordination since 2004 with the Government Operations Centre. Can you help me as to how that links with the memorandums of understanding that have been developed, and how that will complement some of the security issues that had not been addressed before, which seem to now be moving ahead at a satisfactory rate?

**Mrs. Suzanne Hurtubise:** Yes, thank you.

The Government Operations Centre does not get involved in policy arrangements between any agencies, so it would not be involved per se in the MOU between the RCMP and Transport Canada. Its role is operational and it's one of information and coordination. It is there to coordinate and provide information among all the operations centres in government and also to coordinate with provinces, where the case may be, and sometimes even with local municipalities.

I could give you an example of the recent floods in Manitoba. Many people were involved in that. The Government Operations Centre was producing regular reports, at one time four times a day, and eventually it was a little bit less. We were liaising with the Manitoba government and providing them with all the information we had. We were ensuring that the Canadian Forces were aware of the situation in case they might be asked to provide support.

So it's very much to ensure coordination of all the Government of Canada activities, inform all the various players in the Government of Canada so that everyone has the same information, and add that extra dimension to the provincial and municipal dimensions, if necessary.

You may recall a major explosion in Toronto about a year and a half ago. There was a concern that search and rescue equipment in Toronto might not be sufficient. Through the Ontario Operations Centre and the Toronto area police forces, a request came in to the Government Operations Centre, and we lined up search and rescue equipment from another Canadian city that could have been brought in, if necessary.

So it's very much coordination of various government operations across the board. In that way we are better equipped to deal with any issue.

•(1645)

**Mr. Bev Shipley:** And you raise an interesting point, because today focuses a lot on airports and points of entry. But those of us who have been involved in municipal work over the years know that everything from weather-related emergencies to train derailments to aircraft crashes—it isn't always the large jets, but we do have those happen.... We have an incredible respect, I can tell you, for the Government Operations Centre in terms of dealing with emergencies that happen to everyday people. Set aside that these do not involve terrorists, these are not threats to our society; they are events that happen whether they're natural or just by accident. I want to pass that on as part of what we sometimes overlook, quite honestly, the good things that are happening out there.

**Mrs. Suzanne Hurtubise:** Yes.

**Mr. Bev Shipley:** As we go through some of those debriefings post-event, the lessons learned—that's a new term I guess I've learned down here—are lessons to be learned, and they need to be implemented. I just wanted to pass that on.

Ms. Dansereau, you talked about filling positions, and I want to follow up on Mr. Christopherson's comments. On the filling of positions and the number of vacancies, you always have these vacancies. Is the process behind because they're trying to save dollars, because it's hard to find qualified people, or because it's a complex issue and security is one of the main issues to be dealt with?

**Ms. Guylaine Dansereau:** It's not about saving money. We created permanent positions in order to attract and retain qualified employees. The training is not available outside, so we do the training on site. It requires further training and staffing actions to keep our employees and train them. So it's a lengthy process to retain and staff positions.

It's also very complex. It requires a stringent screening process to have qualified criminal analysts to do the job.

**Mr. Bev Shipley:** You have the money to do it.

**Ms. Guylaine Dansereau:** Yes.

**Mr. Bev Shipley:** Thank you.

**The Chair:** Mr. Christopherson, you have four minutes.

**Mr. David Christopherson:** Thank you very much, Mr. Chair.

I'll attempt to get three issues on the floor as quickly as I can. We'll see if it works.

I want to continue where I left off before on decision-making and draw our witnesses' attention to page 11, item 1.19:

Our 2004 audit reviewed the management of security intelligence, finding that overall direction came from five high-level government committees within the intelligence community, and that decision making was by consensus. When agencies could not reach consensus, decisions could be delayed.

I draw to your attention items 1.27 and 1.28, as the Auditor General did. You'll recall that when I asked her if this was still a concern, her answer was yes. So I'd like to hear a response to that.

Secondly, on the day this audit was tabled, in the news release, the Auditor General said in the fourth paragraph:

The audit also found, however, that security and intelligence agencies are still not subject to a level of independent review that corresponds to their intrusion into people's lives.

I'd like to hear some comment on that.

My last comment is on the watch list—they're called lookouts in this report—on page 27, item 1.72, and on page 29, item 1.81 where it says:

Processes to ensure the quality of lookouts have improved in certain areas; however, there is a gap in ensuring the quality of lookout information provided to CBSA by other agencies.

If you flip the page over, that comes up as an issue first shown in the 2004 audit, and it's still unsatisfactory.

Those are the three areas.

Don't all jump in at once.

• (1650)

**Ms. Marie-Lucie Morin:** Thank you for that. I think I will tackle the first question.

Look, what I would say is that the issues with respect to security and intelligence are by their very nature complex. It does perhaps sound like a simple thing to say, but it is just a reality. My experience is that we are able to prioritize issues and we are able to provide timely advice to the government on priority issues.

I have been a national security advisor for six months but have been associated with this community for many more years, and I have seen a high degree of progress in the celerity, the speed, with which we're able to treat issues. We have better mechanisms now to face events when they occur, whether it is the standing up of the operations centre or, as somebody else mentioned today, the ITAC, the Integrated Threat Assessment Centre. So I do feel that we are well equipped, in fact, to meet the challenges as they come our way.

That being said, can we make more progress? Yes, we can make more progress. But I do not believe that the structure as we have it today is actually an impediment to our providing the right policy advice in a timely fashion. My position is a position of coordination. I sometimes have to accelerate work, to make sure that agencies and departments speed up the work, but I have to say that I am satisfied that they are stepping up to the plate.

So again, in conclusion, not to belabour the point, it is not perfect, but I think it is a lot better than it has been.

Thank you.

**Mrs. Suzanne Hurtubise:** On your second question, sir, I don't have the precise quote you noted, but it was about independent review being proportional to the intrusion, I think, of the activities in people's lives, or words to that effect.

I can say, and I believe the Auditor General recognized this in her report, that a lot of work has been done, a lot of analysis, and a lot of options have been developed. We agree completely with the principle set out that the level of review should be proportional.

We also agree, and I believe—

**Mr. David Christopherson:** Sorry, it was actually about the independence of that review, not proportionality.

**Mrs. Suzanne Hurtubise:** Yes, external review, some call it. An independent review is what others call it. Yes, absolutely, sir.

I would point out, as I believe the Auditor General did as well earlier, that, for example, CSIS already has extensive independent or external review, however you cast it, through SIRC, the Security Intelligence Review Committee. But we have done a lot of work since the O'Connor report came out on this, and ministers have appeared before various parliamentary committees on this issue.

A lot of work has been done. We have developed a lot of options. We have set out a number of principles. In addition to the proportionality one, there's the fact that the operational effectiveness of agencies is also critical. We have done a lot of work specifically with respect to review and oversight of the RCMP, but we have also done work with respect to the need to have review for operations that involve more than one agency. That's very important.

I will conclude by saying that we are now awaiting the report of the Air India inquiry, and then the government will decide how it wants to implement those recommendations.

•(1655)

**The Chair:** Thank you, Mr. Christopherson. Thank you, Madam Hurtubise.

Mr. Weston, four minutes.

[*Translation*]

**Mr. John Weston (West Vancouver—Sunshine Coast—Sea to Sky Country, CPC):** Thank you all for being here today.

[*English*]

I have to say you have been very forthcoming with your answers. I thought, Madam Morin, you might say that if you answered the question, you'd have to kill us, but you haven't said that yet.

In terms of the international field, you've said in different ways how complicated things have become. How good are we at integrating information from the field from abroad? And related to that—maybe this is for other members of the panel—how good are we at integrating best practices from other countries? What is the international dimension? It seems in a complicated world much of what is relevant here is happening in Islamabad, for instance.

**Ms. Marie-Lucie Morin:** Thank you.

I believe we are actually doing a very good job on both counts. We do receive a lot of information from varied sources. By the way, today we have to look at the integration of information that is also readily available in open sources. There is a view that the only information that is helpful, from a security and intelligence point of view, is that which is provided, I would say, by our sister agencies or departments overseas. In fact, the business of analyzing all elements that go into providing recommendations to the government on national security entails the analysis of every possible source of information. This is done in various departments across government, but it is coming together in an integrated way.

I have mentioned the creation, for example, of the ITAC, which has really brought us into the 21st century in terms of being able to pull together this material in a timely and helpful fashion. Of course, in the business of security and intelligence, the amount of information grows exponentially. This is the case as well in the so-called civilian world. So it is a challenge that we need to constantly reflect upon, as to how we are going to be able to continue to really analyze all the information that comes our way.

In terms of best practices, I already mentioned that we have particularly close ties to other Westminster-style governments, but we also have very close relationships with other allied countries, partner countries. Of course, it is important for us to take stock of how they are conducting this kind of business, because you are right

in saying that there are best practices elsewhere that we need to be able to import if we think it would be desirable.

This being said, I want to share with you that Canada is often cited as a best practice as well. So inasmuch as we look to the outside, the outside world also looks to us for best practices. When I said earlier that I believe we are first class, I do believe that. I receive a lot of delegations from overseas who want to come and talk to us about how we conduct our business. So there is very much give and take, including from what I would call a machinery-of-government point of view that goes on in this community.

Thank you.

•(1700)

**Mr. John Weston:** Merci.

**The Chair:** Before we go to Ms. Ratansi, I have a question I'd like to put to the Deputy Commissioner of the RCMP here, on the whole issue of civilian oversight.

As you know, the RCMP had a fairly lengthy hearing before this particular committee about a year and a half or two years ago. Very troubling allegations came about. We have the Robert Dziekanski situation going on in Vancouver now. There have been a number of inquiries, and it's been troubling for members of Parliament to watch this. Bear in mind that most of us came here with a lot of respect and admiration for not only the RCMP but the people who wear the uniform, but it certainly has been a very trying couple of years.

One of the issues that I see as fundamentally deficient in the overall organization is this lack of any meaningful civil oversight. We have the complaints commission, but even the commissioner himself gets up before a parliamentary committee and indicates very clearly that the legislation is woefully and totally inadequate. This has been called for, really, by various commissions within government and outside of government, and I think the RCMP will be well served with a more comprehensive regime of civil oversight. That was recommended two years ago by the Brown commission, but as of yet, nothing has been done on that issue.

Do you see any developments coming, and where do you see this whole issue going?

Perhaps Madam Morin might want to chirp in on this issue, too, because I think this is clearly an area where there is a deficiency in the whole operation of the Royal Canadian Mounted Police.

**D/Commr Tim Killam:** The RCMP welcomes oversight mechanisms. We have gone through a very rough last couple of years. There is a lot of work being done, and I know my colleague Madame Hurtubise can speak to that. Frankly, I think we're very close to being there.

**The Chair:** Would you prefer to comment, Madame?

**Mrs. Suzanne Hurtubise:** A lot of work has been done. I think there's a recognition of a need to enhance and modernize the CPC. We need to provide it with additional powers. The RCMP is very open to that. We look forward to seeing the recommendations of the Air India inquiry.

**The Chair:** Can you tell us when we might see a regime change?



**Mrs. Suzanne Hurtubise:** That would be for the government to decide. But all the analysis, the options, have been set out, and the government recently said that it was awaiting the Air India recommendations.

**The Chair:** Ms. Ratansi.

**Ms. Yasmin Ratansi:** Madame Morin, you were asked whether we are more secure today than in 2001. You were very candid in your response. You said that the terrorism issue is very complex and that perhaps we are more coordinated. Whether we are totally prepared, we don't know.

In the global context, we have countries that are being destabilized even as we speak. We have outside interference in sovereign states. We know nothing about the culture or traditions of some areas. We are taking our eye from the ball. We are concentrating on some groups, but we do not know that others are percolating. I do not know whether we are secure. You were talking about challenges, about information-sharing and the need for government to balance it with transparency. Could you explain the concept of transparency with respect to Abdelrazik, who is a Canadian citizen sitting in the Canadian embassy compound in Sudan? Can anybody give me any guarantees that there will not be another inquiry?

**Ms. Marie-Lucie Morin:** I was candid in saying that the world presents a great number of challenges, but I hope I was also clear that I believe we have made huge progress in being more prepared if we have to face security incidents. I firmly believe that we are.

We are able to gather a lot of information and intelligence with respect to what happens around the world. We have embassies around the world. We have a fairly clear picture of what goes on from a geopolitical point of view. This allows us to look at the threatened environment and to learn what it means for North America, for Canada. I believe we have good mechanisms for providing this kind of landscape to the government. We can assure Canadians that we are cognizant of what happens in the greater world. As for Mr. Abdelrazik, I believe this issue is in front of the courts. Because of this, I would refrain from making any further comments on the matter.

• (1705)

**Ms. Yasmin Ratansi:** Fair enough.

Madame Hurtubise, a question was asked regarding the secret-level communication system implementation. The Auditor General said that because it was over budget it might not move forward. I'm not putting words in the Auditor General's mouth. Is there enough budget now? Is it going to be implemented? A system of this kind might have prevented the Air India disaster

**Mrs. Suzanne Hurtubise:** With respect to the secure communications project that you're referring to, I can certainly say that we were given sufficient budget, about \$34 million, to create it, devise it, and implement it as a pilot, which we have done—to develop the technical specifications, to develop the protocols for use, to test it, to make sure it could then be rolled out. That has been done. Parliament voted sufficient funds for us to do that, and that phase is now complete.

I don't believe we referred to it explicitly, but the next phase now is whether or not it gets implemented, and how it gets implemented. For it to be implemented, additional funds will be required,

absolutely. But we certainly had the funds to do the pilot we were responsible for.

**The Chair:** Thank you, Ms. Ratansi.

Mr. Young, for four minutes.

**Mr. Terence Young (Oakville, CPC):** Thank you, Madam Hurtubise.

I'd like to learn a little more about the Government Operations Centre. Is it just an ongoing administrative centre or does it serve us in emergencies? Does it make Canadians safer from terrorism and extremism? Is it that kind of operations centre, or is it just a communications hub?

**Mrs. Suzanne Hurtubise:** It is basically a communications and coordination hub. It does, however, receive input from a variety of sources to coordinate and provide information. So if we were dealing with a particular incident, if there were important intelligence information, it might get that from ITAC, the Integrated Threat Assessment Centre, for example. It might receive information and be in regular contact with the RCMP, if it's an ongoing incident and the RCMP is involved. We might also be dealing with local police forces or local first responders as well, to transfer and provide as much information as we have.

So it is not a creator of information or intelligence; it coordinates and transmits it. But it does operate 24/7. Obviously, when there's an incident, we bring in additional people.

• (1710)

**Mr. Terence Young:** So you would support ITAC if there were an apparent emergency?

**Mrs. Suzanne Hurtubise:** We would support any government department or agency, not just in the security community. We would support, for example, the Public Health Agency in the latest H1N1 outbreak. We would support any government department in any of its activities in any way they need.

**Mr. Terence Young:** Thank you.

Mr. Grégoire, there's a five-point plan that the Minister of Public Safety and Security and the Minister of Transportation put together, and part of that plan is to improve the screening at airports. You mentioned biometrics.

Can you tell us a little bit about how biometrics work, how it works on the front line, how the employees are screened to work at airports?

**Mr. Marc Grégoire:** Yes, absolutely.

First, the government provided money to increase the physical screening of workers. CATSA screens a number of people today. The government provided money for more workers to be screened, and I mean physically screened, not the background check.

Then we have the restricted area identity card, which is the biometric card. The concept of this card is that the biometrics of the person, that is the fingerprints, digital information, as well as the iris scan, are embedded in a little chip on the card. When the employee wants to enter the restricted area, they have to swipe their card through a magnetic reader that then compares the biometrics on the card with the biometrics of the person. It also compares them with a database of valid security clearances.

**Mr. Terence Young:** Where does that data come from for that database? Is that an international database?

**Mr. Marc Grégoire:** Well, CATSA manages the system on a national basis. We manage the validity of security clearances. CATSA checks with us, Transport Canada, once a day for the validity of the clearance. So, for instance, if the RCMP gave us information about somebody whose card we should suspend, that would be in the database immediately. It would be transmitted back by CATSA to the airport, and when the employee tried to open the door, it wouldn't work.

**Mr. Terence Young:** I get it. Thank you.

I had a question for Madam Morin. I want to find out a little bit more about how your office works, if I may. Is it like a secretariat? Where do you get security information? What are the sources? How is it provided, and is it provided on a 24-hour basis?

**Ms. Marie-Lucie Morin:** My office is located, as you know, in the Privy Council Office. I have mentioned my role of coordination from a security and intelligence point of view. If you want to call it a secretariat, essentially what I do is provide this coordinating role, if I may borrow the analogy, at the top of the pyramid. In other words, the security and intelligence apparatus comes through me in terms of the advice I need to provide to the Prime Minister and the government on specific issues.

Again, I think it is important to remind us all that in our Westminster style of government, the various departments and agencies have their own vertical accountability to ministers. My role exists, in fact, in the U.K. and in Australia, but it is not to be confused, as it is at times, with the same role that exists in the United States at a political cabinet level; I am obviously a public servant, and my role is one of coordination of the community.

**The Chair:** Thank you very much, Mr. Young.

The committee has a couple of items of business we want to look after, so I'm going to suspend this part of the meeting, but it will still be public.

Before we do that, though, on behalf of all members of the committee and all members of Parliament, I want to thank all the witnesses for their appearance here today. Our country of Canada is an advanced democracy where the fundamental right and the fundamental obligation of the country is to protect its citizens, but we have the competing interests of privacy and intrusion into the rights of citizens. These concepts have to be balanced, and we certainly want to thank you for all your efforts in doing that. I want to thank you for your appearance here today, and I want to thank the Office of the Auditor General for their report.

Before I go on to the next part of the meeting, do any members have any closing remarks or comments that they want to make?

Before I do that, I want to ask you, Madam Auditor General, if you could stay around for the next part too, because I believe there may be a question on the supplementary estimates (A).

Are there any closing comments?

• (1715)

**Ms. Sheila Fraser:** Chair, I'd like to thank the committee for their interest in our report on what I think is a very important issue. We are very pleased to note that the government has made satisfactory progress on many complex issues since our last audits.

**The Chair:** Is there anyone else? Mr. Ranger or Madame Hurlbise, would you like to comment?

Go ahead, Madame Morin, please.

**Ms. Marie-Lucie Morin:** May I use my privilege of coordination to thank you all on behalf of the community? I hope that we have been able to answer most of your questions, and we thank you for your interest.

**The Chair:** Thank you very much.

We're going right to the next item of business, colleagues. The next item I'd like to deal with—and I'm going to ask the Auditor General to stay—is the review of the minutes of the steering committee meeting held earlier today. Those minutes have been circulated.

The first paragraph just deals with the possible scheduling of a hearing on June 16. You also have the schedule circulated with the report, and at the meeting on June 4 we're going to allow a 10-minute session to be with the parliamentary delegation from Serbia.

**Mr. David Christopherson:** Could you do them one at a time? I'd like to talk about them.

**The Chair:** I'm just going over it before we open it up. I'm just going to highlight it.

Then we're going to bring in a couple of the academics in the fall. That's item 4. The next item is the supplementary estimates (A), which I'm going to ask perhaps the Auditor General or the analyst to explain. The last one is that the departmental action plan and progress reports received by the committee be published on the committee's website, subject to the approval of the committee.

I would like an explanation. I think it's appropriate that the committee receive an explanation on the supplementary estimates (A).

**Mr. David Christopherson:** Why don't we go in order, with number one?

**The Chair:** We can deal with them all. Do you want to deal with one first? Okay, go ahead.

**Mr. David Christopherson:** Yes, I do, Chair.

I just wanted to ask, having been there when we made the recommendation regarding the issue of the crown corporations—I don't know if my colleagues on the steering committee made any notes—I was looking for two, and I was thinking we could do that in one day. I don't know if there is any reference there, and I'm just worried it's going to fall off the table and disappear, because we're now picking which ones we're going to do.

**The Chair:** No, that will be done, Mr. Christopherson, but it will be done in the fall. The only slot we have is June 16, and we decided we would have a hearing, or we would deal with this issue on June 16.

**Mr. David Christopherson:** The first part of your answer is cool. There was nothing here, and I just thought the next report would come, and this would be forgotten as an issue there.

**The Chair:** There is no scheduling done yet for September. That will be at the next steering committee.

**Mr. David Christopherson:** Thank you. I appreciate that.

**The Chair:** Did you want to explain the supplementary estimates, or do you want the analyst to do it? I just want a 30-second explanation on the record.

**Ms. Sheila Fraser:** I'd be glad to, and perhaps the analyst can add something if my answer is not complete.

We mentioned, I believe, when we came for our report on plans and priorities, that we had established what is called a national professional practices group with the provincial auditors general. So my office will be providing to them technical advice, training on accounting standards, and analysis of exposure drafts, and helping them with some of their accounting or auditing issues.

We are charging the provincial auditors for this, and we asked for and obtained from the Treasury Board approval for what is called "re-spending authority," because otherwise we would not be able to keep those moneys coming in. They would go into the consolidated revenue fund, and then we would have to ask for a supplementary estimate to get them back. Because we were very uncertain about how much money could be involved, we asked for re-spending authority, so it simply means when we charge, the office can keep that money and use it for our own expenditures.

• (1720)

**The Chair:** Are there any questions on that issue, or on any other issue on the minutes?

Mr. Christopherson.

**Mr. David Christopherson:** Yes, I have a question on another issue.

I draw Mr. Kramp to number five. At the steering committee today we had a discussion about whether it was subject to the approval of the committee. Initially, your concern, well-placed, was that if we're going to tinker with anything before it goes forward, we need to give approval, but at the end of the discussion it was clear that the reports, the action plans, are all being generated by the departments, and therefore there really was no need for us to say anything.

I only raised it because if we're going to provide for that process, why build in a step that's not needed? That document is not ours. It's generated by the department. It's an action plan. It's a request from people in the community across the country, who themselves, on the website, want to monitor what plans are in place, and we're facilitating that. So I would just suggest that we don't need that step, given that, again, Mr. Kramp, it's not a document we're touching. It's generated in government, through our clerk and chair, and then it goes onto the website, and everything else we do has to come back here.

**The Chair:** So you would like to see the elimination of the words—

**Mr. David Christopherson:** I would amend it to remove the "subject to approval of the committee." I think it's redundant.

**Ms. Yasmin Ratansi:** Mr. Chair, I think it was Ms. Faille's point that we put a disclaimer. So if it's understood that a disclaimer will be put stating that this is the action plan of the department and has nothing to do with us.... Thanks.

**The Chair:** Okay. Is there any discussion?

First of all, is there agreement on the amendment?

(Amendment agreed to)

**The Chair:** Is there agreement on the minutes as amended?

(Motion agreed to)

**The Chair:** Okay. The motion is carried.

The last item is the motion of Mr. Saxton. Let me say at the outset that I reviewed this and had some chats with the clerk. We'll circulate it.

Let me make a few comments. I've reviewed it with the clerk and I would be inclined to rule it out of order. I'm willing to hear any arguments, but there may be a way around this.

First of all, it's in the negative. It's argumentative. It's talking about breaking the law. I would suggest—and maybe Mr. Saxton can amend it—that a motion really should just be a statement. If he were to keep the first eight words, "That, notwithstanding the motion adopted", and then go right to his last sentence and put a specific time there, the motion would be very simple, and I think we could move on to debate the merits of the motion rather than getting into who broke the law.

**Mr. Andrew Saxton:** Mr. Chair, first of all, there was no intent to be argumentative in the motion. It was intended to be factual and to relay what actually took place, but if you found it to be argumentative, then I would be amenable to making some changes.

What you are proposing, then, is the first eight words, "That, notwithstanding the motion adopted on May 12, 2009", and then taking up where...?

**The Chair:** You could continue on with the sentence, stating: "That, notwithstanding the motion adopted on May 12, 2009, in relation to the deposit of audio cassettes requested at the meeting of March 24, 2009, the Department of Public Works and Government Services be given", and then I would encourage you to put a time instead of it being open-ended.

• (1725)

**Mr. Andrew Saxton:** The difficulty with putting a time is that the purpose of this motion is to give them the ability to respect their obligations under the Privacy Act. I don't think putting a time would be appropriate, because what if they have not satisfied the Privacy Act by a certain date? We have to leave it somewhat open, to the point where they have the time necessary to respect the obligation under the Privacy Act.

**The Chair:** If you insist on the time needed, what your motion would read, just to be absolutely fair, is: "That, notwithstanding the motion adopted on May 12, 2009, in relation to the deposit of audio cassettes requested at the meeting of March 24, 2009, the Department of Public Works and Government Services be given the time needed to respect its obligations under the Privacy Act".

That would be the amended motion. Is that okay with you, Mr. Saxton?

**Mr. Andrew Saxton:** That sounds exceptional.

**The Chair:** Now, it's a little late in the day, so we'll go to Mr. Saxton, and then perhaps four or five interventions, and then I'll put the question.

Mr. Saxton, for one minute.

**Mr. Andrew Saxton:** First of all, Mr. Chair, I think it's very important that this committee respect the Privacy Act. I do have a copy of the Privacy Act here. It states: "Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section". There are 12 subsections that relate to circumstances under which information could be relayed. This particular request doesn't fall under any one of those 12.

I just want to point out that we don't have a problem agreeing to the provision of the tapes. That's not the issue here. The issue here is the usurping, for lack of a better word, of the Privacy Act. We feel that we need to abide by the Privacy Act and not force a department to do otherwise. That is the purpose of this motion.

**The Chair:** Thank you very much.

Before I go to the next intervenor, I do want to point out to the committee that our legal counsel was of the opposite view.

**Mr. David Christopherson:** On a point of order, Mr. Chair, I want a ruling. Is this not contrary to a decision we've already made?

**The Chair:** It's not contrary; it's allowing sufficient time.

**Mr. David Christopherson:** On the pivotal point of whether the privacy issue was going to legitimately prevent us, we dealt with that, and you're alluding to that procedure now.

**The Chair:** Yes, that's right.

**Mr. David Christopherson:** It passed, right or wrong.

Now there's a motion being put before us that goes in the exact opposite direction, and I'm asking for a ruling from you. Is this not tantamount to a double jeopardy? You vote on one matter one week, and then you roll back the next week and put in the same motion that goes in the opposite direction. I'm just asking for your ruling on whether that's in order.

**The Chair:** It's up to the committee. I'm a servant of the committee.

If you go to the first few words of the motion, "That, notwithstanding the motion adopted on May 12, 2009," you're quite correct that, if we adopt this motion, we are taking a 180-degree turn.

Madame Faillie.

**Mr. David Christopherson:** Are there not procedures for that, though, as to who can introduce a motion when it's the exact opposite of where we've already been?

**The Chair:** The committee is the master of its own....

Madame Faillie.

[*Translation*]

**Ms. Meili Faillie:** We were told that the tapes would be provided. Is this motion null and void?

[*English*]

**The Chair:** Let me say at the outset that I find this disturbing. I listened to what the lawyer said. I have researched this point, and it's my opinion that the Privacy Act and interests of privacy have no bearing on this issue at all, none whatsoever. But somebody over at Public Works thinks otherwise.

They haven't filed the tapes. They've reduced them to CDs. We have about 12 of them. We got them about two hours ago. The information we're getting from Public Works is that we're going to get the rest of them prior to the end of the week. We don't know if they've been altered or are unaltered. If they haven't been altered, then of course they've met their obligations under the previous motion, and they will be recorded and circulated to all members of this committee shortly.

That's where it stands, but we don't know if they've altered them or not.

• (1730)

**Mr. David Christopherson:** There are 18 minutes missing.

**The Chair:** There could be.

**Ms. Yasmin Ratansi:** Mr. Chair, if we have the tapes, this motion becomes redundant. I do not know why we're going to circular motions.

**The Chair:** We have a situation right now where the Department of Public Works and Government Services is in violation of an order of this committee. We asked them to provide them by May 12. They didn't do it. They did it this afternoon at 3:30. So they're in violation of a motion of this committee, and they are continuing to be in violation because they say they won't get it in until Friday. And again, we don't know whether they've been altered.

We'll entertain three more interventions.

Had you finished, Madame Faillie?

[*Translation*]

**Ms. Meili Faillie:** I don't want the floor, but I'm opposed to this motion.

[*English*]

**The Chair:** We have two or three more interventions. Is there anybody else who wants to speak?

Mr. Young, Mr. Kramp, and then I'll put the question.

**Mr. Terence Young:** As I said about the motion the last time, the previous motion, I was very uncomfortable with it and wouldn't be supporting it.

I was very uncomfortable. I didn't want to be a part of it.

For the same reason, I'm supporting this motion. In my view, the Privacy Act is pretty clear.

Thank you.

**The Chair:** Mr. Kramp.

**Mr. Daryl Kramp:** That argument as well, Chair, and I absolutely did not want to put us in a position where I'm going to suggest this committee go contrary to the Privacy Act. We have a legal argument that suggests it's not on that particular point. But you're suggesting, Chair, that you had a private conversation with legal officials who advised you of one thing. Well, that could be, but certainly if that's the case, that's one set of lawyers. Chair, you've been a lawyer yourself. You recognize sometimes lawyers have different opinions. I can certainly assure you we probably haven't heard from the lawyers from Public Works, because they might have a different take on this.

I think the point being made is that the government members on this side, and certainly I as an individual member, are not party to moving forward with a motion—I did not vote for it in the past and would not vote for it now—to suggest that we would just automatically go and ignore the Privacy Act, regardless of the situation.

I think it's moot, in a way, the simple reason being that they apparently have 12 of the 18; the rest are coming within the week. Well, wonderful, but I don't think we need to go down that road. If for some particular reason the tapes aren't what we wanted and/or the tapes weren't produced, then we would go through the route and ensure we would have access to them, but I don't believe that's the problem.

**The Chair:** Mr. Weston.

**Mr. John Weston:** On a point of order, Mr. Chair, I think what Ms. Ratansi was raising was really a point of order as well. Is this a moot issue? If we find that either we or the ministry is in breach of a law, then we shouldn't be reviewing those tapes that we have received. I would say that even though some of them have been delivered and more may be on the way, we ought to thoroughly investigate that before either we or the ministry commits an offence we would all regret.

**The Chair:** Well, just to go back to Mr. Kramp's point, the legal issue I was talking about was with Mr. Tardi, who appeared here, and he's given us his testimony and opinion on the issue.

Mr. Christopherson.

**Mr. David Christopherson:** I won't be long. When Madame Faillie first raised this, no one really knew exactly what road the honourable member was going to go down, but she's a respected member of this committee. She's never done anything that suggested actions that wouldn't be supported by all of us, so we said yes—and we usually do unless we have a reason not to. Then it kind of proceeded, and there was a little resistance. Then Madame Faillie brought it back again. She's very tenacious. She brought it back

again. Most of us, again, weren't focused on this; it wasn't a priority, but it was a concern she was following on behalf of some concerns that had been raised to her. So then we pushed a little more, and then finally we're told, "No, we can't give you that."

If you recall, it would cost too much money to do all the transcripts, and suddenly it just started to look as if there were blockades put in front for some reason, out of nowhere. So we pushed past that and said, "Look, just give us the tapes, then." We accept that we don't want to spend a lot of money, but we have a member who wants a piece of information that's relevant to an issue in front of us and we're going to support her in that.

Then we get into this stuff about, well, they can't give it to us now because there are privacy concerns. Okay, well, the last thing any of us wants to do is infringe on the rights of a Canadian citizen. What would be the logical step? We call in the parliamentary law clerk's office. Now, I'm not going to go into details of the advice we got, but I think it's fair, and suffice it to say that what he suggested to us was because he had meetings with their lawyers. At some point you have to pick a lawyer you're going to follow. He came to us, after having consulted with the others, and gave us a rationale as to why he didn't think the arguments stood the test.

I'm not a lawyer, so I'm not even going to enter the fray, but I have to decide who I'm going to follow. At the end of the day, the majority of the committee decided, based on the legal advice of the parliamentary law clerk's office, that we were entitled to all that information and there were no privacy issues per se.

Now we get this kind of letter, just ignoring our decision and saying, "We're going to do this, anyway." I have to tell you, as one member peripheral to this issue, more and more I'm starting to wonder what you are hiding. What is the big deal that this department is prepared to block a legitimate decision of this committee to receive information? This stuff about privacy, there's nothing there beyond the members of the government saying it. We have all the information I think we need to stand by the decision we made.

Chair, we may be into a situation where they're in contempt of this committee. It's one thing to call you or to call the clerk and say, "We still have ongoing problems; we have to do something", but to send us a letter that just basically says, "We really don't care what you've decided, we have made this decision, and therefore we will decide what information we're going to spoon-feed you. We're not necessarily going to give you all the information you asked for." Suddenly we're getting a major federal case out of one member simply asking for information and the majority of us backing her up.

• (1735)

**The Chair:** I'm going to spend 30 seconds reading what I consider to be the law on this issue, and it really goes right to the supremacy of Parliament:

Parliament, and by extension its committees, has the constitutional right to initiate inquiries, to call witnesses, and to demand papers and records. This right is not limited by any ordinary statute, including the Access to Information Act and the Privacy Act.

Although the House has not placed any restriction on the power to send for papers and records, it may [that's the House] not be appropriate to insist on the production of papers in all cases. ....considerations of public policy, including national security, foreign relations, and so forth, enter into the decision as to when it is appropriate to order to production of such documents.

Where a committee meets with a refusal to provide a document it deems essential to its work, the committee may pass a motion ordering its production.

That has been well known. It's in Marleau and Montpetit. It's in the other books dealing with parliamentary procedure.

I think we've said enough. I'm prepared to put the question right now on the motion as amended.

Mr. Saxton has called for a recorded vote. I will turn that over to the clerk.

●(1740)

**The Clerk of the Committee (Ms. Joann Garbig):** There is an equality of voices. It is a tie.

The chair votes nay.

(Motion as amended negatived: nays 6; yeas 5)

**The Chair:** I remind all members that Thursday afternoon we will be dealing with four reports. I won't be here. Mr. Kramp will be chairing the meeting.

The meeting is adjourned.

---









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

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

**Also available on the Parliament of Canada Web Site at the following address:  
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :  
<http://www.parl.gc.ca>**

---

**The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.**

**Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.**