



HOUSE OF COMMONS  
CHAMBRE DES COMMUNES  
CANADA

## **Standing Committee on National Defence**

---

NDDN • NUMBER 018 • 2nd SESSION • 41st PARLIAMENT

---

**EVIDENCE**

**Thursday, April 3, 2014**

—  
**Chair**

**The Honourable Peter Kent**



## Standing Committee on National Defence

Thursday, April 3, 2014

• (1100)

[English]

**The Chair (Hon. Peter Kent (Thornhill, CPC)):** All right, colleagues, the hour is here. We welcome Minister Rob Nicholson Minister of National Defence for our committee study today. Pursuant to Standing Order 108(2) the study is of the supplementary estimates (C) 2013-14 vote 5c under National Defence.

Appearing with the minister is Michael Martin, senior associate deputy minister; Major-General Michael Hood, director of staff of the strategic joint staff; Kevin Lindsey, assistant deputy minister, chief financial officer, finance and corporate services; and Rear-Admiral Patrick Finn, chief of staff materiel group.

Also at the witnesses table from the Communication Security Establishment Canada intelligence-gathering policies and practices we have the chief of CSEC, John Forster, whom we will be questioning more closely later in this committee meeting.

Welcome, Minister, if you would please deliver your—

**Mr. Jack Harris (St. John's East, NDP):** Mr. Chair, I have a point of order. I just wanted to clarify that the estimates of course have been passed in the House, as we know, so we're really after the fact potentially asking questions about estimates. One of the principal reasons for this meeting was to have both the minister and Mr. Forster here so we could explore the question of the intelligence activities of government, particularly CSEC. I'm given to understand that we can at this point from the beginning either ask questions about the estimates or about CSEC and its activities in intelligence as well.

**The Chair:** The minister will be with us for 90 minutes. The chief will be with us through to the end of the committee meeting. Questions can be asked on either of those topics.

**Mr. Jack Harris:** On either of those topics, but my understanding is the minister is leaving at 12:30.

That's fine, thanks.

**The Chair:** So with no further delay, Minister Nicholson, your opening remarks ten minutes, sir.

**Hon. Rob Nicholson (Minister of National Defence):** Thank you very much.

I'm here today as was just pointed out to discuss supplementary estimates (C), but first I would like to address a story that ran last night on CTV regarding an invitation officials sent to the families of our fallen soldiers regarding the May 9 National Day of Honour.

The letter was premature, incorrect, and contained false information as event plans have not been finalized. Our government is proud to commemorate our military's mission in Afghanistan and to provide Canadians with an opportunity to reflect on the courage and sacrifice made by our soldiers.

Throughout this mission in Afghanistan our troops demonstrated commitment, dedication, and valour. Sadly, many Canadians made the ultimate sacrifice during this mission and we owe their families a debt of gratitude that can never be repaid. That is why it is the government's position that these expenses will be covered.

Now back to the subject of today's committee business... As you pointed out, Mr. Chair, you've introduced those with me and I am pleased to be here this morning with them.

In a few moments I will also speak to you about the Communication Security Establishment, or CSE, and this is why, as was pointed out, I am joined by John Forster, the chief of CSE.

I understand that some members have a written version of the remarks from my last attempted appearance. I will however go through a number of my remarks to ensure that they are fully and appropriately on record.

[Translation]

Last time I spoke to you, I highlighted the good work of our men and women in uniform. I remain impressed each and every day with the incredible work of our military and the dedicated civilian team supporting them.

• (1105)

[English]

Let's take Afghanistan, for example. Just last month, I had the pleasure to welcome back the last rotation of soldiers deployed to Afghanistan. More than 40,000 Canadian Armed Forces members have served in Afghanistan, and many served more than once. In many ways, it was a war that defined our military in the last 12 years.

With our NATO allies and partners, we helped Afghans reclaim their country from terrorism and provide security for the Afghan population. Today, Afghanistan's security forces stand at approximately 345,000 personnel, and they will take full responsibility for Afghan security at the end of this year.

Mr. Chair, to undertake such a mission abroad for 12 years, our military needed proper equipment, and we gave it to them. Through the Canada First defence strategy, the government made unprecedented investments in military equipment and successfully delivered on many procurement projects.

But at the same time, it's important to challenge ourselves to ensure that our procurement processes are as efficient as they can be. This is why I was pleased to announce a few weeks ago, with my colleague Minister Finley, the new defence procurement strategy. The defence procurement strategy is giving the defence team new tools to improve the way they do procurement. It helps us streamline the procurement process and improve efficiency.

Mr. Chair, in our supplementary estimates, we are requesting \$57.8 million in new appropriations to fund the Aurora modernization and structural life extension project, funds for the force mobility enhancement project, and some transfers to other government departments. Of these funds requested, we are offsetting \$49.5 million with previously appropriated funding, and \$8.1 million with transfers to other government departments. This reduces our total request for new funding to only \$311,000.

Some of these funds will be used, again, as part of the Aurora modernization and life extension program, which will ensure that Canada maintains a world-class airborne surveillance capability while ensuring value for Canadians.

Some of the funds requested will be dedicated to the force mobility enhancement project. This project will provide the army with a flexible multi-purpose capability that will enable them to respond effectively to any mission, now or in the future.

In addition, these estimates will allow the department to work with other federal agencies to leverage resources and enhance the security of Canadians.

Mr. Chair, you will see that the estimates include smaller transfers of \$5.2 million and \$2.7 million to Shared Services Canada in order to reduce duplication and inefficiencies within government institutions and also conduct information technology activities at the Carling campus.

In addition, you will see a funding transfer of \$141,900 to Transport Canada as part of a multi-year commitment to the Canadian safety and security program.

Also, these estimates list a transfer of \$25,000 from National Defence to the National Research Council of Canada in order to conduct surface and groundwater monitoring at two National Research Council sites in Penticton, British Columbia.

[*Translation*]

While the job of the defence team is maintaining the security of this country, this government recognizes that a strong and resilient economy is an important aspect of that security.

That is why, last year, the defence team launched its own internal business process review, called defence renewal.

[*English*]

The defence renewal process is an opportunity to improve the way we manage our people, assets, and resources. While excellence in delivering operations at home and abroad will always be our priority, we must streamline the defence procurement process and leverage Canadian tax dollars that are provided for defence.

Mr. Chair, at the committee's request, I take this opportunity to also address any of the committee members' questions on the Communications Security Establishment. Let me underline the important role that CSE plays in protecting Canada and Canadians. CSE's mandate flows from the National Defence Act and requires CSE to provide the Government of Canada with three key services.

First, CSE collects foreign signals intelligence that supports government decision-making by providing information on the capabilities, activities, or intentions of foreign entities, such as states or terrorist groups.

Second, CSE has a cyber-protection mandate and provides advice, guidance, and services that help secure government systems and networks and the information they contain.

Finally, CSE provides technical and operational assistance upon request to federal law enforcement and security agencies under their respective mandates.

Under both its foreign intelligence and cyber-protection mandates, CSE does not target Canadians anywhere in the world or any person in Canada. Under the agency's assistance mandate, CSE acts under the legal authority of the requesting agency it is assisting and is subject to any limitations to that authority, such as applicable court warrants.

The foreign intelligence activities of CSE are critical to fulfilling the government's commitment to address emerging threats to our sovereignty and economy posed by terrorism and cyber-attacks while ensuring that Canadians' fundamental privacy rights are protected.

Over the years, CSE has provided intelligence to protect Canada and Canadians by supporting Canadian military operations and protecting our forces from threats; uncovering the efforts of foreign-based extremists to attract, radicalize, and train individuals to carry out attacks in Canada and abroad; identifying and helping to defend Canada against the actions of hostile foreign intelligence agencies; providing early warning to thwart foreign cyber-threats to the Government of Canada and to critical information infrastructures and networks; and furthering Canada's national interests in the world by providing context about global events and crises and informing the government's foreign policy.

In fulfilling this important role, CSE operates in full accordance with the law, including the National Defence Act, the Criminal Code, and the Privacy Act. CSE is also subject to legislative measures in place to protect the privacy of Canadians and persons in Canada. Since 1996, a fully independent CSE commissioner—a series of esteemed retired or supernumerary judges—has regularly reviewed CSE activities for compliance with the law. The commissioner and his full-time staff and expert consultants have full access to all CSE personnel, systems, and documents. In more than 17 years, the commissioner has never found CSE to have acted unlawfully. In fact, he has specifically noted CSE's culture of lawful compliance and genuine concern for protecting the privacy of Canadians.

Were the commissioner ever to conclude that the agency is acting outside the law, he would be required to report this immediately to the Attorney General and to me as the minister responsible for CSE. Both the chief of CSE and I take the findings of the commissioner in his reviews very seriously. CSE has implemented past recommendations of the commissioner related to privacy, and the agency is in the process of implementing those from the more recent reviews.

Canadians can continue to count on the efforts of CSE and the government to safeguard the security of Canada from foreign threats while at the same time acting in full accordance with the law and protecting the privacy of Canadians.

Mr. Chair, thank you once again for inviting me. I welcome any questions.

• (1110)

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

We'll proceed now to the opening round of questions, seven-minute segments.

Mr. Chisu, please.

**Mr. Corneliu Chisu (Pickering—Scarborough East, CPC):** Thank you, Mr. Chair.

Thank you very much, Minister and all who are appearing before the committee.

I have a question to you, Minister. I served in Afghanistan. National Defence and the minister, after ten years of darkness, provided us with equipment and with great care in the 12 years of operation in Afghanistan, so I am thanking you all—including the CSE, that provided us with the fusion centre and provided us with great services in fulfilling our mission abroad.

Minister, the Department of National Defence is seeking approximately \$35 million to modernize the Aurora aircraft. Can you explain to us the importance of the Aurora and how this investment is going to affect the capability of our air force?

• (1115)

**Hon. Rob Nicholson:** The Auroras have played a key role in our capability, and certainly Libya was one of the examples of that. These are important surveillance aircraft. I was very pleased to be in Halifax recently.... As you know, Mr. Chair, the estimates have been passed, and so we've proceeded on that basis. A couple of weeks ago, I was in Halifax to make the announcement that we are continuing with the modernization of these important aircraft and

again bringing them up to the greatest possible capability and modernizing them.

I've received very good reports on the role they have played. I mentioned Libya as an example of it, but their importance for strategic surveillance is without question. Again, I was very proud to make that announcement.

The feedback I have received from the armed forces is that these are an important component of our capability. As you pointed out with respect to Afghanistan, our capability is extremely important to making sure that we are able to get the job done that we are called upon to do. That is a commitment, of course, of this government, but one component of it is this modernization program.

Again, I was very pleased and honoured to be able to make that announcement a couple of weeks ago.

**Mr. Corneliu Chisu:** Thank you very much.

Another question that I have for you, Minister, is that in terms of the overall budget of the Department of National Defence the amount requested under supplementary estimates (C) is quite small. Can you please outline the role of the Canada First defence strategy in making budgetary decisions big and small at the Department of National Defence?

I am especially pleased to see that the department is paying attention to the force mobility enhancements project, which is close to my heart as a former combat and construction engineer. That we finally have armoured engineering vehicles and after many years have this capability warms my heart. Can you elaborate on this?

**Hon. Rob Nicholson:** The amount of investment that the government has made in National Defence is unprecedented. Supplementary estimates (C) are not the main repository for the budget of National Defence. As you go through the supplementary estimates process, as you may know and as the chairman would be very aware, there are modifications that take place. So again, we have made unprecedented investment, and rightly so.

As you know, we have just concluded... and I had the opportunity to welcome back the last of our soldiers from Afghanistan. This was a huge operation that we undertook as a nation.

You pointed out quite correctly the Canada First defence strategy. This is something we will be renewing. This has been a part of our outreach and the message we are communicating to the world: that we have a responsibility with respect to Canada's north, the defence of Canada, the defence of North America, and indeed to continuing cooperation with our allies, whether it be through NATO or the outreach that we have made to others. It's a part of who we are, and this is what we are going to continue to do. It's a major operation, and it's an important one. Again, the Canada First defence strategy captures that outlook on behalf of the government.

**Mr. Corneliu Chisu:** Thank you, Minister.

Do I have more time?

**The Chair:** You have 90 seconds, Mr. Chisu.

**Mr. Corneliu Chisu:** Okay. I have a short question about CSE operations.

Of course we Canadians are rightly concerned about the protection of our privacy, but also we are concerned about the protection of our country. I understand that you are doing an excellent job in protecting against threats to Canada, and there are many new threats following the exercise on the world scene of Russia, playing quite aggressively lately.

Can you elaborate on what the CSE is doing for us and what can be expected in the future?

• (1120)

**Hon. Rob Nicholson:** Thank you for those comments that I'm doing an excellent job in this area here. I hope that is being recorded, Mr. Chair.

That being said, you quite correctly point out the role of CSE, and I'm sure there will be more discussions about their role in helping to protect us against cyber-attackers and terrorists. As you quite correctly point out, this is an ongoing threat. Our job and our responsibility is to do what we can within the parameters as set out in the enabling legislation: to assist Canada, to protect Canada, against those kinds of attacks.

I have been very careful in my discussions and my analysis of what's taking place that there are constraints within the laws of this country, and CSE is obligated to operate within those instructions, but again, I can't overemphasize the importance this organization plays in helping to protect Canada and Canadians.

**The Chair:** Thank you, Minister.

Mr. Harris, you have seven minutes, please.

**Mr. Jack Harris:** Thank you, Chair, and thank you, Minister, for joining us along with Mr. Forster and the other representatives of the Department of National Defence.

I have one question about the estimates even though they have already been passed. That's to do with the Aurora project.

Do I understand correctly of the 18 Auroras that were originally purchased, 10 have so far been modernized, there are another four to go, and they will be able to operate the 14 aircraft into 2030 with the new modernization?

**Hon. Rob Nicholson:** Yes, I think that's a very reasonable analysis. You're absolutely correct. The announcement I made was about modernizing those aircraft. Again, these are going to continue to be a vital component of what we do.

**Mr. Jack Harris:** These are used mainly for coastal maritime surveillance.

**Hon. Rob Nicholson:** Certainly. I would say, yes.

**Mr. Jack Harris:** If they were used, they would be added to great effect.

**Hon. Rob Nicholson:** Exactly.

**Mr. Jack Harris:** So they are very useful aircraft.

**Hon. Rob Nicholson:** When you get into these roles, you get analysis of different aspects of our equipment, and what we are

doing. I can say I have had nothing except positive feedback with respect to these aircraft and their value to our armed forces.

So, again, as I pointed out to my colleagues in my opening remarks, I'm very pleased to be able to make that announcement that we're going to continue this modernization process.

**Mr. Jack Harris:** With respect to the operations of the security establishment, let me ask first of all—because I think there are a lot of concerns and questions about what CSEC actually does, much of which is done through authorizations by the Minister of National Defence, whether you have personally been involved in them to date or not, I don't know, but we do know there were two authorizations with respect to what's known as metadata, one in 2005 and one in 2011.

Mr. Forster, you told the Senate committee recently when questioned about the activities involving data collected at a Canadian airport, this was “part of our normal global collection”. In other words, the collection of the data wasn't specifically targeted at that airport.

Is that correct?

**Mr. John Forster (Chief, Communications Security Establishment):** Yes. The metadata we do collect, we collect from the global information infrastructure.

**Mr. Jack Harris:** It wasn't collected specifically at that airport?

**Mr. John Forster:** No, I can confirm the collection of... We used a historical snapshot of metadata. There was no collection done from the airport. It was collected—

**Mr. Jack Harris:** —As part of your normal global collection.

So that same normal global collection would have collected that data whether it had been at the airport, in the downtown of the place where the airport was located, from equipment such as I have in my hand here, my cellphone, and an iPad. All that metadata that's collected is part of what you call your normal global collection. Am I correct?

• (1125)

**Mr. John Forster:** We collect as per the National Defence Act.

**Mr. Jack Harris:** I understand. I have the act. We'll get into the act in a moment.

**Hon. Rob Nicholson:** But it doesn't include any concept of private communication, if that's what you're looking at. But fair enough...

**Mr. Jack Harris:** I'm looking at what are the facts.

**Hon. Rob Nicholson:** Sure, yes.

**Mr. Jack Harris:** Your normal, global collection that was analyzed with respect to that particular airport, that normal global collection includes all communications that occur, not just at airports but everywhere in the country. Is that correct?

**Mr. John Forster:** No. If I could elaborate a little bit...

When you look at the global information infrastructure—the Internet—if I'm sending an email from myself to the chair, for example, that email may get broken up into different pieces, and it may travel different communication routes around the world. When we collect information off the global Internet, Canadian information and metadata, which is not the content, along with foreign, is all intermingled and mixed. When you collect it, you may be collecting foreign, and you have no way of discerning in that context as it's impossible to identify and separate out, so you collect it. We're then required to protect and manage any Canadian metadata, which doesn't include the communications content, separately, and protect the privacy of that information.

**Mr. Jack Harris:** Just so I can be clear here, the data that's collected, you don't know whether it comes from Canadians, persons in Canada or not, but you're authorized to collect metadata from persons in Canada and Canadians, are you not?

**Mr. John Forster:** We're authorized to collect—

**Mr. Jack Harris:** Metadata...

**Mr. John Forster:** —data from the global information infrastructure, which is defined in the act, which includes global communication networks. As I said, data and communications will traverse the globe, depending on where the most efficient, cost-effective...and capacity is. Our Canadian data and foreign data may be intermingled, so when we collect it we're interested in foreign intelligence, so we use that to direct our activities of foreign targets.

**Mr. Jack Harris:** You know, we do hear formulas coming from the government, and you and the minister, that we don't target Canadians, we don't track Canadians, because you're not allowed to directly do that. But you collect that data as part of the data collection that you're doing from what you call the global infrastructure, but that would include information. We've heard metadata described as, for example, this cellphone is talking to that cellphone, or a person is using one of these Internet or GIS-type information systems, that this travels around and you're able to collect it, and you do. Some of it is from Canadians, and some of it is from others. Is that correct?

**Mr. John Forster:** Yes, Canadian and foreign, the metadata, which is not the content, will be intermingled together as it traverses global communication networks.

**Mr. Jack Harris:** So are you saying to me that you then, after collecting all that data, which is an ongoing process, you then separate out the Canadian from the others?

**Mr. John Forster:** Our use of metadata, we use it based on the directions from the minister for three things.

One is to understand global communication networks, so we use it to analyze networks so that when we're searching for a foreign target, it helps us to find where our best chance of success is in identifying targets in a sea of billions of communications.

Two, we use it to make sure that we're actually targeting a foreign communication and not a Canadian communication.

Three, we use metadata to help us detect and identify cyber-attacks against government systems and the information they contain. We can only use metadata either to understand global

networks and analyze them, or to define our foreign targets. We don't use it to identify or target Canadians.

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

That's your time, Mr. Harris.

Mr. Norlock, please.

**Mr. Rick Norlock (Northumberland—Quinte West, CPC):** Thank you very much, Mr. Chair, and through you to our witnesses, thank you for attending today.

I'd like to continue on with the questioning of my friend across the table.

Mr. Forster, if I understood correctly, metadata...when Canadians are listening to this information, of course they read the headlines and they get all upset that maybe there is some personal information that the government's collected on Canadians. I think you rightly identified that Canadians are not targeted, and that the purpose of collection of this data is to, as you put it, understand and analyze so that you can—from that sea of billions of communication methods and addresses that messages are going to, and pieced out to different entities throughout the world—more appropriately and properly identify those foreign information exchanges, shall we call them, that may be targeted against a Canadian target. Would I be correct in what I've just said?

• (1130)

**Mr. John Forster:** That's correct.

**Mr. Rick Norlock:** And your job is to protect this country against people who would use the Internet and other types of technology to infiltrate not only the Government of Canada, including our military. But would I also be correct in identifying those threats to Canadian industry, those industries that protect Canadian jobs and increase Canadian jobs, and that have a high degree of intellectual property that we feel must be protected in order to maintain those jobs and to foster industry throughout Canada?

**Mr. John Forster:** Yes, our role is to help protect Canada from a variety of foreign-based threats. That could include terrorist organizations that are plotting attacks on our allies or Canadian interests overseas, support to the Canadian military in theatre of operations.

Regarding your last point, the organization plays a key role in protecting Canadian networks from cyber-attacks. That would include primarily the Government of Canada and all the information those systems contain, but as well critical infrastructure in Canada. So we collect information on those cyber-threats, cyber-attacks. We can help critical infrastructure providers protect their networks and the tech attacks, which could include the theft of valuable intellectual property, technology, research.

I would like to be clear in terms of our relations with industry. We do not collect and provide intelligence to them for their commercial advantage. We're not in that business at all. Our interactions with them would be solely in terms of helping them protect their networks from espionage and the disruption of their networks. We do that with Public Safety who has the lead role.

**Mr. Rick Norlock:** That's where I was going. So you would go to Public Safety and say, "We have an issue here. Here's what the issue is. You folks do what you have to do to make sure that we protect Canadian jobs in the industry and intellectual property that is domestic in nature."

Would I be correct in saying your organization really doesn't want to know if I'm talking to my grandkids over the Internet, if I'm talking to some family members, if Canadians want to communicate, or the websites Canadians may want to go to? You're not interested in that. What you're interested in is the security of our country and not the individual communications of Canadians with other Canadians or the places they go to visit to get information.

**Mr. John Forster:** That's correct. Our focus, as required under the act, is foreign intelligence and foreign targets to support the intelligence priorities of the government. We're not listening to Canadian conversations with your family and so on. We collect, as I mentioned, information off the Internet but we use it to identify and attract legitimate foreign targets.

**Mr. Rick Norlock:** So tell me how Canadians can be assured that you are doing your job, that you're not interfering with private communications. By that I'm asking if you feel you have to do something, do you run it by, for instance, a judge? Do you make sure that anything you have to do, that if you have to go somewhere or do something...? What are the checks and balances to make sure that Canadians can trust that you're doing your job?

**Hon. Rob Nicholson:** If I might just get in on that and then I'll turn it back to Mr. Forster....

Again, as I pointed out in my initial comments, we have a retired or supernumerary judge who has a look at these. I can tell you that he has done at least six reviews of CSE with respect to whether it's metadata collection, to ensure their compliance with Canadian laws. They are under close scrutiny by the CSE commissioner and those working with him to ensure that they are in compliance with all Canadian laws and that they respect and protect the privacy of Canadians.

I don't know if you had any further comments, Mr. Forster. That is the check that's in place, Mr. Chair.

• (1135)

**Mr. Rick Norlock:** I'm trying to encapsulate this into one little piece of information for Canadians. The piece of information is that you don't target Canadians or Canadian businesses or Canadian entities and if you come across information that some cyber-attack may be targeting a civilian company, a company other than the Government of Canada, that you go to Public Safety and tell them to begin to take action in that regard.

And if it is to deal with the Government of Canada, the military, whom do you contact or notify?

**Mr. John Forster:** In terms of government networks and systems we will look at attacks coming into the government networks. We work with Shared Services Canada then who are providing the basic computer network and services for Canada. We will provide notices and alerts to Shared Services Canada. We will help mitigate those attacks. We will help clean up where there's been need to go in and modify or correct actions that have been taken. We work with government departments on that.

As I mentioned earlier, in terms of military operations we provide direct support to military operations like Afghanistan.

**The Chair:** Thank you.

Ms. Murray, please, for seven minutes.

**Ms. Joyce Murray (Vancouver Quadra, Lib.):** Thank you.

Thank you, Minister Nicholson, for being here to discuss these important issues with the committee members.

To your officials, I want to thank you for reversing the decision on paying for the expenses of families to come to the May 9 commemoration service.

I do have a couple of questions, though, on that because a letter went out last month to all 158 families. You described it as a mistake but clearly this was a plan. Did anyone in your office know about this plan?

**Hon. Rob Nicholson:** Certainly it was not planned by me or my office. We've been very consistent with this. The information to be sent out to these people was one of a save the date, making sure that they had this and the inclusion of a line with respect to them having to pay their own way had absolutely nothing to do with my office and our government position on this hasn't changed as a matter of fact.

**Ms. Joyce Murray:** Thank you.

**Hon. Rob Nicholson:** We will support those and assist those who have suffered these huge losses.

**Ms. Joyce Murray:** Did anyone in your office approve the preliminary plan to hold these commemorations?

**Hon. Rob Nicholson:** Again, this was never the government's policy.

Again, I hope I made it clear in my opening comments that we can and will support those individuals.

**Ms. Joyce Murray:** In the letter it said, "Your attendance will be at your own expense". There were family members who experienced that as being like a slap in the face. Have you or your department apologized to the families for this letter of last month?

**Hon. Rob Nicholson:** It just came to our attention last night. This is part of what we're doing here, to make it clear that's not the government's position, that we will support those individuals, that this is a mistake that was sent out.

Again, it was a question of saving the date, you want people to know, but there will be a considerable, as we pointed out and announced a couple of weeks ago, commemoration as is appropriate.

**Ms. Joyce Murray:** Thank you, Mr. Minister.



I have one last question on that. If that was not your plan or the government's plan, what is planned to be covered? How many family members? What kind of expenses will be covered? Is it hotel, is it travel costs and per diems? Could you share the plan?

**Hon. Rob Nicholson:** Again, at this point in time we're in the planning process and the first step of the planning process was to make the announcement that in fact we would honour Canada's role in Afghanistan and those who played this important role.

Again, it's an evolutionary exercise and we'll get the message out.

**Ms. Joyce Murray:** It's a month away but those details, you aren't able to share them.

**Hon. Rob Nicholson:** We're working on them as we speak, and as I say, getting the message out to save the date was one part of that.

**Ms. Joyce Murray:** Thank you.

On another matter, and this has to do with budget and figures, so this may be in the supplementary estimates but it's at a level of detail that it's not clear if it is in those transfers. An inquiry of the ministry that I've put forward, dated January 29 of this year, elicited the information that the department will be required to pay for commemoration activities for the next six years to the tune of \$27.5 million. That was the total that your department sent back to me.

Is that \$27.5 million for incremental costs associated with Operation Distinction for the years until 2020, a correct total?

**Hon. Rob Nicholson:** Again, without seeing the letter that you have there, this is part of our commemoration of a number of important military moments that we are going to commemorate. We made that very clear, that this is important for us, among other things to, as I say, recognize those who have served in Afghanistan and those who have paid the ultimate price. But, as you know, in addition there are a number of anniversaries that are coming forward with respect to World War I—

• (1140)

**Ms. Joyce Murray:** So it may be higher number?

**Hon. Rob Nicholson:** —and World War II, and, again, it's all part of this.

**Ms. Joyce Murray:** So it may be higher?

**Hon. Rob Nicholson:** Again, we're working through this. We're working with other departments, it's not just national defence. Heritage will play an important role in this—

**Ms. Joyce Murray:** Okay, thank you.

**Hon. Rob Nicholson:** —and we believe this is very important.

**Ms. Joyce Murray:** My understanding is that there's not a specific commemoration budget for this in national defence, this will be coming out of operations and maintenance.

**Hon. Rob Nicholson:** No.

**Ms. Joyce Murray:** If that's correct, I'd like to know what the department would otherwise be using those scarce resources for if it were not to be spending it on commemoration ceremonies.

**Hon. Rob Nicholson:** You may disagree with spending it on commemoration services, but the armed forces will be fully operational, they will be supported, we will continue with our

procurement. But, again, this will also be a part of what we are doing, which is to commemorate those individuals who fought and served in World War I and World War II, and so we will continue along that line.

**Ms. Joyce Murray:** I have been on record saying commemorations are important—

**Hon. Rob Nicholson:** Good, I'm glad.

**Ms. Joyce Murray:** —but not at the expense of ill and injured soldiers and their families.

**Hon. Rob Nicholson:** It certainly is not the case. We will continue to support the ill and injured, we will continue to support our procurement, but this will be one more part of it.

**Ms. Joyce Murray:** Minister, could you answer the question, please? Is this coming out of operations and maintenance budget? If so, what other things would that funding possibly have been spent on? Could it have been spent on programs for ill and injured soldiers and training and maintenance?

**Hon. Rob Nicholson:** Again, the budget for supporting those who are ill and injured is a completely separate budget. It has increased under this government. It has become a priority, and we're going to continue. We're going to continue to hire more people in there. That budget will get larger. Any commemoration for the war in Afghanistan is not coming out of that. I hope that's as clear can be.

**Ms. Joyce Murray:** Thank you for that.

Now we are also advised, through an access to information request, that your director of mental health, Colonel Scott McLeod, a year ago begged for what he considered to be crucial expertise to assist with PTSD, both prevention and treatment, and that's a uniformed licensed psychologist. There has been no response and not a single uniformed licensed psychologist has been hired by the armed forces.

I have to ask: do you consider it more important to commemorate, for example, the War of 1812, than to hire licensed psychologists who are, by your own mental health director, so badly needed? Is that a greater priority for you?

**Hon. Rob Nicholson:** It's not an either/or, Ms. Murray. Again, yes, on the staff there are clinical psychiatrists. For those individuals who have needed psychological help, what we have done—

**Ms. Joyce Murray:** Excuse me, correction, psychologists.

**Hon. Rob Nicholson:** —what we have done is make sure that within the private sector those individuals get that kind of help. It's not just a question. You may not like the War of 1812, but that, too, was extremely important for the history of this country, Mr. Chairman. Again, it's not either/or.

**The Chair:** Thank you, Minister.

Time has expired, Ms. Murray.

Moving on to the second round of questioning, five-minute segments, Ms. Gallant, please.

**Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC):** Thank you, Mr. Chairman.

Through you to the minister, first of all, I hope you pardon the member who just spoke previously. We continuously hear this kind of hypocrisy, on the one hand demanding details of the payments to the families who have lost loved ones during the Afghan conflict to have our Day of Honour versus complaining about money that is spent on commemorating those who have fallen in other conflicts.

First of all, Minister, you stated that among the emerging threats the Canadian Armed Forces is preparing for is cyber-warfare. The world has not yet witnessed the first incidence of cyber-terrorism. Does Canada have its own centre, such as the Americans have—they have a cyber-command—in order to centralize command of operations related to cyberspace, organizing existing cyber-resources and synchronized defence of Canadian military networks at this time?

• (1145)

**Hon. Rob Nicholson:** Mr. Forster, I know, wants to make a comment on that, but you quite correctly pointed out that the threat of cyber-security is huge right now in the world. Our expectation is that these will become a greater challenge, rather than a lesser challenge in the coming years. The defence portfolio plays a key role to protect us from cyber-threats. Mr. Forster I'm sure would like to comment, and I'll give him that opportunity. CSEC does play an important role in protecting Canada and trying to head off some of these activities.

That being said, though, I want you to know that we work with our other allies as well. We're not alone in this. A threat to the United Kingdom is a threat to Canada and a threat to Australia and the United States. These other countries are direct threats, we feel, on this country as well. We're not in this alone, in terms of working to protect ourselves from that, but, again, CSEC does play an important role.

Mr. Forster, if you would like to make any comments....

**Mr. John Forster:** No I think, Minister, you've covered it very well.

**Mrs. Cheryl Gallant:** Minister, our unique, bilateral relationship, the North American aerospace defence command, NORAD, is the envy of other countries. You had just mentioned that we work in conjunction with our allies on cyber-defence. In the same way that we have combined forces for surveillance in defence of North American aerospace and the maritime component, do we have a similar combined defence for cyber-defence?

**Hon. Rob Nicholson:** Again, we share our concerns in this area with our allies, our close allies and we work very closely with them. It's not just the United States. We have others. As you pointed out, one of the important components of the protection of this country is our cooperation with the United States. It's NORAD. It's been in effect since, I believe, 1958, and we've had a very strong relationship of cooperation and protecting Canadian airspace from all types of attacks. Again, that threat as you can imagine, has evolved since the late 1950s but, nonetheless, NORAD itself has evolved in that sense

of protecting us from all the types of threats that can come onto this continent.

You know something, you made a very good point as well that I wanted to pick up on. This is really a model for anyone in the world to see that kind of level of cooperation, that understanding, that kind of commitment between two countries that exists between the United States and Canada. This has been a great success story. Again, when I'm elsewhere at NATO meetings and these cooperative efforts come up, I'm always reminded of how well it works in North America for our defence and our cooperation with the United States. It's been a great success story.

**Mrs. Cheryl Gallant:** Now this may be for either you, Minister, or Mr. Forster.

Is there a continuous input from the private cyber-security companies on viruses, viral incidents or incidents themselves, hacking incidents, to provide the Canadian Armed Forces with real-time situational awareness of what's going on in cyberspace?

**Mr. John Forster:** I think one of the roles that CSE plays...and we're very closely integrated with the Canadian Armed Forces and we have people inside each other's organizations in cyberspace. The minister indicated we share cyber-threat information very closely amongst the Five Eyes allies and provide information to them on cyber-threats to their information networks and computer systems. So, it's a very close partnership we have with our Five Eyes and then, in turn, what we do with Canadian Forces to defend and protect their networks and systems....

• (1150)

**The Chair:** Thank you.

Thank you very much, Mr. Forster.

Mr. Harris.

**Mr. Jack Harris:** Thank you, Chair.

I guess either the minister or Mr. Forster can answer this. You said that the mandate of the CSE, under the National Defence Act, is to acquire and use information from the global information infrastructure, as you pointed out. That's a very broad definition. Of course, what's included in that, is there in the act; it includes anything that deals with electronic communications. Why, if that's all you're doing, do you need the authorizations such as those that were brought in, in 2005 and 2011, to collect metadata?

**Mr. John Forster:** The ones you're referring to are actually ministerial directives, so they were directives brought in to focus and provide additional direction to the agency about how it's going to collect and protect metadata. Metadata has been used by the agency and by second agencies for decades. In 2005, with the growth of the Internet, it was felt that a specific directive from the minister would help inform and direct the agency about how it was to use, what it could use metadata for, and how it was to protect the privacy of Canadians in doing that. Then that directive was updated again in 2011. So, it's not—

**Mr. Jack Harris:** —it's not an authorization on section 273.61.

**Mr. John Forster:** Our ministerial authorizations are used for any collection activities where we might risk the incidental interception of a private communication. So, if I'm targeting a foreign target who's in communication with somebody in Canada—I'm not targeting the Canadian but in targeting a foreign target they may be having an email conversation with someone in Canada. The Minister authorizes any collection activities we have where we risk that incidental interception of a private communication as the act provides for.

**Mr. Jack Harris:** So one is just under the minister's authority to issue directives and those are the 2005 and 2011...and authorizations are something separate for specific interception of private communication?

**Mr. John Forster:** Yes, for activities that risk that incidental interception of a communication, which is where you're talking about the actual content.... Metadata doesn't include the content of the conversation.

**Mr. Jack Harris:** In order for us to know how the privacy of Canadians is protected, we would have to know the contents of the directive, would we not?

**Hon. Rob Nicholson:** Again, these are completely reviewed by the CSE commissioner that any authorization is to ensure that CSE is in complete compliance with Canadian laws, including the protection of privacy.

That being said, all of the activity of CSEC is reviewed by the commissioner and as I pointed out, specifically with respect to metadata and other issues, the commissioner has indicated that the organizations are in complete compliance with Canadian law.

**Mr. Jack Harris:** Sir, we all have the commission's report—

**Hon. Rob Nicholson:** Good.

**Mr. Jack Harris:** —but you indicated in your opening remarks, and you're saying it again, about the protection of privacy. We do know, because the act says so that the whole section of the Criminal Code which refers to privacy of information:

273.69 Part VI of the Criminal Code does not apply in relation to an interception of a communication under the authority of an authorization issued under this Part or in relation to a communication so intercepted.

So the protection of privacy, the wiretap legislation under the Criminal Code, is totally excluded from this and it's totally dependent upon an authorization—

**Hon. Rob Nicholson:** But you then get judicial oversight as to whether the warrant will be issued or not.

**Mr. Jack Harris:** Well, there's no judicial oversight, because the authorization is issued by you as minister, sir, and you're not acting in the capacity of a judge.

**Hon. Rob Nicholson:** With respect to that section of the Criminal Code, you talked about the interception and the...that applies to a wide range of the interceptions that are all under judicial oversight in terms of the applications that are made.

Now with respect to the ministerial directives and authorizations on this, again, it's to be in compliance with Canadian law and that is the basis upon which...there and that is reviewed again by the CSE commissioner.

● (1155)

**Mr. Jack Harris:** The directives themselves, I don't think there's a suggestion here, although others have suggested it elsewhere that there may not be compliance with Canadian law.... What we're attempting to discover here is the level of detail that the CSE collects. For example, it's been also reported that because of obligations made by the CRTC, there has to be a capability to have access to information by companies such as Bell, Rogers, and Telus by government agencies such as CSEC.

Do you have, for example, Mr. Forster, direct access through electronic means from your headquarters to information on the Bell, Rogers, and Telus networks? Is that part of your operational activities?

**Mr. John Forster:** Well, as I mentioned, our target and our focus is foreign intelligence collection.

**Mr. Jack Harris:** I know what you're targeting. I'm asking what access you have?

**Mr. John Forster:** We collect in areas around the global networks where we're going to be most successful in finding our foreign targets. I can't really disclose our methods and capabilities in that collection. Suffice it to say that where there's any risk of incidental instance of private communication, those are authorized by the minister; and then the commissioner reviews all of our collection activities and verifies that they're in compliance with Canadian law and that we have measures in place to protect the privacy of the Canadian—

**The Chair:** Thank you.

Mr. Williamson, please, for five minutes.

**Mr. John Williamson (New Brunswick Southwest, CPC):** Thank you, Chair.

I appreciate everyone coming in today.

I find it interesting how the evolution of this committee has gone on. We focus so much on privacy here at home, we've got other people here who project power and yet not a single question to them. I just think it's interesting the challenges the government has in order to protect Canada and the preoccupation, which I think Canadians rightly share and we've heard that CSE must follow the law which in itself I think is powerful. There's a judicial review.

I'd like to know if you can explain how Canadians can be assured that CSE is accountable to someone at the end of the day, not simply just a judge who will use decisions that the law is enforced and there is some oversight in place that we can have some confidence in.

**Hon. Rob Nicholson:** We all have a stake, of course, in ensuring that there is complete compliance with Canadian law. What CSE can do is very clear, and it's fairly restricted, quite frankly. As I pointed out in an answer to a previous question, if somebody, for example, wants a wiretap or wants to tap into somebody's conversation, they must go before a judge and make an application for that. It is not CSEC or National Defence; it is law enforcement agencies that do this. So you get this oversight, that the courts get an opportunity to have a look at it.

With respect to CSEC, it's very clear that they are not to target Canadians. They are not to intercept the private communications of Canadians, and we expect them to comply with the law. Indeed, it's a ministerial responsibility to direct it in that direction.

That being said, though, as I pointed out, we have had over the last 17-plus years an independent CSEC commissioner who has complete access to all the different activities, all the documents, and that sort of thing. The commissioner is a respected individual who is a former jurist or a supernumerary judge. Those individuals, on a regular basis, have a look, unless they're assisting the RCMP and CSIS under a warrant. There is complete judicial oversight for all these activities, but on their own there are certain prescriptions, unless it's pursuant to an authorization that the RCMP and law enforcement agencies have had.

Going back to your original question—what confidence do we have?—I have confidence in the fact that we have individuals who are looking at this kind of information. You may ask, could more be done? I can tell you that these are the individuals who are protecting us against terrorists and cyber-attackers. It's not information that is all publicly available all the time to everyone, because that's not how we can protect ourselves against these kinds of threats.

I've been satisfied with and confident in the continuation of the process that's in place, which is to have a former judge look at this. I think it has worked well.

• (1200)

**Mr. John Williamson:** Very good. Thank you.

Let's take it down to the ground level. You recently visited CFB Gagetown in New Brunswick.

**Hon. Rob Nicholson:** Yes.

**Mr. John Williamson:** I have just a couple of comments.

I think it's important that you get out to meet the men and women in uniform. Can you talk about that a little bit?

**Hon. Rob Nicholson:** I was amazed at how sophisticated the operation is that's there and how up to date the equipment is that they have available for our men and women in the armed forces, and particularly for those in the air force. It's a large operation, as you know. You're quite familiar with this, I'm sure.

I was very pleased and impressed, quite frankly, and told them that too. I said this is very impressive, the different equipment that you have. I think it works very well. It's something that maybe we don't spend a lot of time congratulating ourselves on. Whether through commemorations for our service in the war or otherwise, nobody has a better record than Canada of doing the right thing throughout the world. To see all the men and women at that base and all the work they are doing there was very impressive.

Thank you for asking me about that.

**The Chair:** Thank you.

Mr. Harris, I understand you'll be splitting your time.

**Mr. Jack Harris:** I'll split my time with Ms. Michaud for the last minute and a half.

**The Chair:** Thank you.

**Mr. Jack Harris:** Mr. Minister, in the United States, as a result of public concerns about the collection of metadata and the knowledge that it contains information as to what devices are talking to other devices and for how long, where they are, and all of this other information, President Obama has moved to take the data that is collected and have it only accessed under a warrant issued by a court. So the data is collected for security reasons and available for use, but in order to assure the public of privacy and proper use, a court order must be obtained to go after a particular set of data or particular individuals.

Why would it be inappropriate for Canada to do the same thing?

**Hon. Rob Nicholson:** I think the tools are in place in Canada for this system to work well and to keep us protected. I hear this sometimes, and I certainly heard it when I was justice minister: the Americans are doing this in this particular state, so why aren't you doing it?

I always say to those who say these things that we have our own systems in this country and we will develop our own protections and guidelines. While I appreciate that, I do have discussions with my American, British, Australian, and other counterparts. I'm always very interested to hear what they are doing in this particular area. But I'm pleased with the system that we have developed here in Canada. It's a made-in-Canada solution.

**Mr. Jack Harris:** True, but the solution is—

**Hon. Rob Nicholson:** Sometimes it's like comparing apples and oranges when you think of some other countries—

**Mr. Jack Harris:** It's a made-in-Canada solution. The made-in-Canada solution is a directive issued by the minister containing these provisions but no one knows what's in it except the minister and CSEC, and perhaps the commissioner.

How can we have confidence if we don't even know the contents of the directive and what measures are in place to ensure the privacy and protection of Canadians?

**Hon. Rob Nicholson:** It's the same comfort in many ways that you have when very sensitive disc documents are disclosed in courts. You would know this from your background, to a certain extent, I'm sure, in terms of the applications that are made to court on highly sensitive security areas. We have confidence in this country that with judicial oversight and input Canadians are protected throughout the processes. Again, you'll point to an individual who is a supernumerary judge or a retired jurist. I think people have confidence in the Canadian judicial system and the individuals who are in it. That's the confidence that they can take with them when they have a look at this.

That's my view of it.

**The Chair:** Ms. Michaud.

**Hon. Rob Nicholson:** That being said, though, I don't underestimate it. We do watch it and look very carefully. Indeed, when I get together with my colleagues from our other allies, I'm constantly asking them about what they are doing and the different threats that they are doing. That said, I'm very pleased with the made-in-Canada product that we've come up with.

**The Chair:** Madam Michaud, you have just under two minutes.

•(1205)

[*Translation*]

**Ms. Éline Michaud (Portneuf—Jacques-Cartier, NDP):** Thank you.

Since I have very little time, I would ask that you kindly keep your answers brief. I'll try to go quickly as I would like to discuss a number of issues with you.

Mr. Forster, you touched on the matter of information about Canadians being shared with the Five Eyes allies. Some information is shared.

Could you provide some details on how our Five Eyes partners could use intelligence collected on Canadians and on what limits currently exist as far as their access to that intelligence goes? I would really appreciate it if you could be concise.

[*English*]

**Hon. Rob Nicholson:** I'm going to ask Mr. Forster to try to give you a brief answer.

**Mr. John Forster:** Thank you.

As an intelligence agency, it's very important that we share intelligence with our closest allies, which we do. However, in sharing any intelligence we still must comply with Canadian laws, our act, the Privacy Act, and the charter in doing that. We have to put in place measures to protect the privacy of Canadians. For example, if we're writing an intelligence report, we would not make any reference to the identity of a Canadian in that report when that—

[*Translation*]

**Ms. Éline Michaud:** Let's say metadata on Canadians is shared with our Five Eyes partners. Right now, are there any limits on how they can use that information? What information can they extrapolate? That is what's troubling.

Our organizations abide by the law. But can we guarantee how metadata our organizations provide to our partners will be used? That, in part, is what troubles me.

[*English*]

**Mr. John Forster:** Even if we were sharing metadata we still must take steps to make sure that any information that would lead to the identity of a Canadian in that data is minimized and reduced so that it's not possible to identify them.

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

Mr. Bezan.

**Mr. James Bezan (Selkirk—Interlake, CPC):** Thank you, Mr. Chair.

I want to thank the minister and the officials for coming in and spending time with us today, especially since we had to reschedule this.

It is important that we have this discussion on CSEC and also on the supplementary estimates (C), even though the supplementary estimates (C) have already been passed. There is a lot of good stuff that was in those supplementary estimates (C). This is in addition to what we've already done in providing new equipment on the Canadian Armed Forces, with new heavy-lift tactical equipment,

with C-17s, new Hercules, and new Chinook helicopters for troop movement. We now have the new Leopard tank series. We're enhancing that battle group with these new armoured engineering vehicles.

Can we talk a little bit about what exactly those vehicles do and how they function within the context of the battle group? Are these newly acquired assets or are we doing some modifications to the existing fleet?

**Hon. Rob Nicholson:** Well, as you know very well, Mr. Bezan—and thank you for your role as our parliamentary secretary—it's all part of our overall process, which is to make sure that there is capability within our armed forces.

I don't have to describe to you what it was once upon a time, if you go back over 10 years ago, and how challenging it was. We had allies who were very good to give us a lift if we needed to get somewhere, and I think they were very accommodating. But one of the important changes we have made is to make sure that our armed forces have capability in all areas for which they will be called upon to assist.

I was very pleased—when we were called upon to assist, for instance, the Philippines a couple of months ago—to be down at the base at Trenton and to see that we were completely capable and had all the equipment necessary to move members of the Canadian Armed Forces and equipment and people and assistance and were able to do it.

I am very grateful for any other country that has helped us over the years or that gave us a lift somewhere, or that type of thing, but I am very pleased that we have this. We learned in Afghanistan that we have to be capable on all different fronts to meet these challenges, and so we are continuously having a look at what our needs are and what we have to do to make sure we maintain that certain level of capability.

I answered questions earlier in the meeting with respect to the Aurora. This is all part of it. By updating it, we're making sure that we have the latest technology, the latest capability. I think we owe this to the people of this country. We certainly owe it to the men and women in our armed forces to do everything we can to make sure that they have up-to-date equipment, that it works, and that they have the equipment that's consistent with the priorities of this country.

I outlined in some small detail the Canada First defence strategy and our role in protecting Canadian sovereignty and Canada's interests, our cooperation for North American security, and in addition, our cooperation with our traditional allies.

But as your question in general points out, this is all part of what we have to do to make sure that this country continues to pull its weight. And indeed, we punch over our weight, as you know, in the last 100 years when it comes to assisting other parts of the world to help themselves. This is something of which we can be very proud, but it is something to which we have to be very committed.

•(1210)

**Mr. James Bezan:** Thank you, Minister.

When you were talking in your opening comments, you were saying that CSEC has to respect Canadian law. We've said many times that CSEC cannot do indirectly what it is prohibited from doing directly.

We talked about allies; we're a member of the Five Eyes surveillance community. Can we talk about how we make sure, when working with the Five Eyes, that we're not violating the rights and privileges and the privacy of Canadians?

**Hon. Rob Nicholson:** I'll repeat Mr. Forster's comments, that in fact we are very careful. When we have these discussions with our Five Eyes partners, we obviously are focusing on the common threats that we have, which come from any part of the world. But as the chief has pointed out, the organization has to be respectful of all aspects of Canadian laws and protection of Canadian privacy, compliance with the National Defence Act, compliance with the charter, compliance with all Canadian legislation.

This marks the relationship. We have this, and I believe that our other partners understand that. But again, we all have a stake in trying to protect ourselves against cyber-attacks and terrorist activity, and that's exactly what we do.

**The Chair:** Thank you, Minister.

Mr. Harris.

**Mr. Jack Harris:** Thank you.

Minister, I know you're going soon, so I do have a question that is policy related.

We talk about CSEC being required to obey Canadian law. Of course we all have to respect Canadian law, whether we're individuals or institutions or members of Parliament or whatever, so that's not really the point here.

But I'm sure you're aware that the privacy commissioner, in a report to Parliament called "Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance", suggested and argues that the law must be updated to reflect the increased surveillance capabilities, including requiring CSEC to disclose statistics about their assistance to other agencies; that greater clarity must be presented to the National Defence Act in terms of the definitions of what is required so that people can understand what's going on; and that there ought to be an expanded parliamentary oversight and strengthening of the accountability regime to better reflect the state of national security operations.

We're talking about major changes since this legislation has been made. We've seen the budget going from \$50 million a year to something in the order of \$500 million or more per year.

A lot of people are reflecting on what the privacy commissioner has said, and are concerned about the capabilities of your organization, Mr. Forster.

What is your reaction, Mr. Minister, to these recommendations, and are you prepared to consider making changes that are going to update the act to make it more transparent as to what is going on so that people have a better understanding and better protection of their privacy?

**Hon. Rob Nicholson:** My view of it is that the system we have in place today works.

Again, having the opportunity to analyze this and as you quite correctly pointed out, this whole area of concern of terrorist activities has changed a fair amount since 1996 and has certainly increased.... That being said, though, the processes that have been put in place, I am satisfied, are working very well.

Again, if the CSEC commissioner was coming out with reports that were showing the gaps or that there were violations of the law or that there was a culture of disrespect for Canadian privacy, if there were any of those things over the last 17 years, I'm sure I would probably change my mind. But what I do get from this respected individual is that in fact there is a culture of respect and that there are processes in place to protect the privacy of Canadians. So again, when suggestions are made by the CSEC commissioner, these are taken seriously by the organization.

So in answer to your question, I'm satisfied that the regime that's in place now works and I believe it should continue, Mr. Chair. Again, you can't point to everything and say how well everything works, that it has a record of success, but I believe this is an area we can.

• (1215)

**Mr. Jack Harris:** These processes you're talking about in place to protect the privacy of Canadians, these are contained in a directive that is not public. So we don't know what those processes are that you suggest you're satisfied with. You're telling us that you're satisfied, but how can we be satisfied?

**Hon. Rob Nicholson:** Well again, the organization has to be in compliance with a whole host of Canadian pieces of legislation, including a constitutional document, the charter. Again, that is exactly what is reviewed on a regular basis by the CSEC commissioner and those working with him. It's not a question of my investigating this organization, it's a question of having an independent individual having a look at it. They can give me all the assurances of what they are doing but when I can have a look and see somebody we respect and we trust having a look at this, it does give me the confidence that they are in compliance with all Canadian laws.

**The Chair:** Thank you, Minister.

Ms. Gallant.

**Mrs. Cheryl Gallant:** Thank you, Mr. Chairman.

We understand that DND and the Canadian Armed Forces will be tenants in Nortel's former Carling Avenue campus.

Would you please tell us how the consolidation of these different departments, organizations in the national capital region will be of benefit to our country?

**Hon. Rob Nicholson:** I think the benefit will be that, having had National Defence in several dozen different locations all over this community and this area, consolidating and reducing the number of footprints at National Defence will be a huge benefit. In terms of administrative costs—I was quite impressed when I saw this—the move will have net savings to the Government of Canada of more than \$750 million in addition to \$160 million in cost avoidance over 25 years.

Again, if you disperse your activities over several dozen different facilities and are paying for that in administrative costs, etc., and are now consolidating it so that not all of National Defence will be in the one location but much of it will be, there are savings to Canada—and a much more efficient way to do business, frankly. You can imagine that having operations in all different types of locations can in and of itself be inefficient. That being said, this is a great improvement and one that I'm pleased to see.

**Mrs. Cheryl Gallant:** So will the new money that's being transferred in these estimates to Shared Services Canada to fund this Carling Campus project actually generate savings?

**Hon. Rob Nicholson:** In the long term we have to take steps to make the move from the 40 different locations that National Defence is in now, and there are some preliminary steps that have to be taken working with other government agencies, but I'm satisfied that in the long term this will result in considerable savings for the taxpayers of this country and I believe it will contribute to better operations within DND.

• (1220)

**Mrs. Cheryl Gallant:** In terms of allocations towards exercises—as you know, the military has to be at the ready at all times—can you tell us about what is in the estimates and how it pertains to keeping our forces ready?

**Hon. Rob Nicholson:** I can tell you how pleased I was to participate in the Army Run a few months ago, and certainly this has been a part of the tradition within the Canadian Armed Forces.... I've told members of the air force that I remember that at my school we had the RCAF 5BX plan. This was an exercise program, and the chairman might remember it as well. This was a great program, and this is what we were told. It's good that the members of our armed forces want to maintain fitness levels and that they were extending that and encouraging us as young children to get involved with it.

We'll get whatever information we can to you on the exact breakdown of this, but I've been very pleased to see over the years, and the Army Run is just a good example, the bringing of people together and demonstrating that commitment to a level of fitness.

I'll see what we can do about coming up with more details for you.

**Mrs. Cheryl Gallant:** Thank you, Minister.

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

We have time. We will hit your departure time, sir, with two more five-minute rounds.

Mr. Harris.

**Mr. Jack Harris:** Thank you, Mr. Chair.

There are provisions in the act for ministerial authorizations, as we discussed, under section 273.65, some of them for intercepting

“private communications in relation to an activity... or activities” that are identified in the order, including, within Canada, with respect to protecting computer systems and networks.

Could you give us the history of the use of these authorizations? How many of these have there been, say, in the last five years?

**Mr. John Forster:** I wouldn't have the number with me. Last year there were, I believe, four or five authorizations. They are related to the class of activities that risk incidental interception, as when you're targeting a foreign target who may be in conversation with somebody in Canada. That's when you need an authorization, and it has to meet a number of criteria in the act that are spelled out there, such as that it has to be a foreign target and that you couldn't reasonably obtain the information in another way, and it has to have foreign intelligence value. The minister has to be satisfied that those conditions are met, and then the commissioner reviews those authorizations and assesses whether our activities have complied with them.

He also reviews, as you'll note in his report last year, all of the private communications—so that involves a Canadian on one end—to make sure they were used in compliance with those conditions.

**Mr. Jack Harris:** When you say it has to be authorized by the minister and is reviewed by the commissioner, it's not reviewed by the commissioner before the authorization is acted upon.

**Mr. John Forster:** No, he reviews—

**Mr. Jack Harris:** This is part of his activity after the fact.

**Mr. John Forster:** Yes, sir. He reviews—

**Mr. Jack Harris:** Then the four to five last year, would that be typical? Would that be four or five a year or would there be...I'm asking about the last five years, so are we talking about that being typical?

**Mr. John Forster:** No, I think we've reduced and consolidated them, but to be honest, I don't have the numbers with me over the last five years.

**Mr. Jack Harris:** Were there fewer last year than in the previous four years?

**Mr. John Forster:** Yes, sir, and as I said, any private communications that were retained and used by us—the number is quite small—the commissioner reviewed each and every one of those to make sure they were in compliance with our act and with the authorization by the minister.

**Mr. Jack Harris:** There's a specific authorization as well, under subsection (3), of that type of authorization to intercept private communications with respect to protecting the computer systems or networks of the Government of Canada from “mischief, unauthorized use or interference”.

Are there authorizations in place under that section as well?

**Mr. John Forster:** There would be an authorization for cyber-defence activity that risks the interception of a private communication.

**Mr. Jack Harris:** It doesn't say "risk" here. It says, "authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization", and that includes Canadians.

•(1225)

**Mr. John Forster:** If we were getting an email into the federal department that contained malware or was spear-phishing in the hope that somebody would click on it, open, download malware to infect government computers, that authorization allows us to intercept that but only for cyber-defence purposes and protecting the government networks.

**Mr. Jack Harris:** Would that be used then to follow up and try to prosecute somebody who was trying to do damage to Canadian computer systems? Is that part of the role?

**Mr. John Forster:** If we wrote a report on it and the RCMP or CSIS wanted to follow up, they'd have to come...we wouldn't disclose that information. They would have to come and justify why they're entitled to it under the act and those are reviewed case by case, and the commissioner reviews a sample of those every year as well.

**Mr. Jack Harris:** So you see it as a defensive mechanism and not

**Mr. John Forster:** For that authorization, it's strictly for—

**Mr. Jack Harris:** Not a law enforcement one.

**Mr. John Forster:** —right, it's strictly for defending computer networks.

**Mr. Jack Harris:** And in terms of your—

**The Chair:** You can have a very brief question, please.

**Mr. Jack Harris:** In terms of the involvement in providing technical and operational assistance to federal law enforcement and security, that would include the RCMP, CSIS—anybody else? CBSA perhaps?

**Mr. John Forster:** It's law enforcement and security, so it tends to be mostly RCMP and CSIS. It may also include CBSA, but those would be the primary ones.

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

Mr. Bezan, go ahead.

**Mr. James Bezan:** Thank you, Mr. Chair.

To follow up on Mr. Harris, he was talking about the budget for CSEC. How does that compare to our allies in the Five Eyes, and how much they spend? Does anyone have that information handy?

**Hon. Rob Nicholson:** The amount the United States spends is huge. I wouldn't be able to exaggerate in terms of how difficult it is, but again, the security arrangement between the five countries of New Zealand, Australia, Great Britain, the United States, and Canada has worked very well, and I think it's a good investment for Canada to work closely with our allies for our protection against terrorism, cyber-hackers, international kidnappers, child pornographers, and others. So the sharing of information among the five has worked well.

But you're quite correct. There are very huge budgets both in the United States and the United Kingdom on these areas, but everybody

has a stake in it. When I've discussed this with my New Zealand counterparts, they are worried about these issues as well because many times these five countries are among the targets of people who get into this kind of activity. So this is a relationship that has worked well to Canada's benefit, quite frankly, and being able to work with them and cooperate with them is for our benefit. I mentioned earlier our work on NORAD. This is something that works well for Canada. It's in Canada's interest to protect the airspace over North America. We all have a stake in that, but as I said, you can't have a strike against any of those five countries, and indeed many other countries throughout the world...so we all have a stake in that.

I apologize. I thought, Cheryl, you were talking about physical exercise here, but thank you very much. So you heard about all my... everything, yes. Obviously, the military exercises are a vital component of what we do in our operations and they too are included. Most of them, quite frankly, are in the main estimates here, but again, I appreciate that.

Thank you.

**Mr. James Bezan:** Good. Just as a follow-up, one of the concerns I keep hearing from the other side is the issue of oversight on the metadata and on making sure the privacy of Canadians is protected.

In addition, we talk about the supernumerary judge we have as the commissioner, who is doing a great job for 16-plus years now, with reports coming in always showing that CSEC is in compliance with our laws. Are there any other officers who have oversight over CSEC, such as the Auditor General or Privacy Commissioner?

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

**Mr. John Forster:** We're subject to the same parliamentary agents as any other department, so the Auditor General, Privacy Commissioner, etc. As well, within CSE we have our own audit evaluation function that does internal reviews, evaluations, and audits similar to other departments. We also have an audit committee of people external to the government that reviews those reports.

•(1230)

**Mr. James Bezan:** Has the Auditor General or the Privacy Commissioner ever raised any red flags?

**Mr. John Forster:** The Auditor General had the last audit we were involved in. We tend to be captured as part of broader audits—for example, cyber-protection in the government. The last one he did on us was related to security in contracting. They looked at the new building and the security provisions we had in place and were satisfied with those.

**Mr. James Bezan:** That's perfect. Thank you.

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

Minister, thank you very much for spending time with us today. We have met our time commitment to you, and as you make your departure we will suspend for two minutes. We'll resume with Ms. Murray for the remaining time to the top of the hour.



•(1230) \_\_\_\_\_ (Pause) \_\_\_\_\_

•(1230)

**The Chair:** Colleagues, in the interest of best use of time, we will continue now, in five-minute segments, until the top of the hour.

We will begin with Ms. Murray.

**Ms. Joyce Murray:** Thank you.

Mr. Forster, I have some questions about CSEC. I would love to have put them to the minister, but since you're here, thank you for being here.

The essence of what I've been hearing about the CSEC and metadata conversation has been that the minister trusts the commissioner, so the committee and the public should trust the minister, and that there's no concern.

Regarding the two key issues of metadata and the law, we're told that the metadata is no problem because the communications aren't opened and the law is being respected. However, the privacy commissioners are telling us the opposite. Ann Cavoukian from Ontario, for example, is saying that metadata is far more dangerous in disclosing the private lives of individuals than opening an email is. Metadata is a dangerous thing in terms of personal privacy.

The national Privacy Commissioner, Chantal Bernier, is telling us that the act is out of date, that the National Defence Act does not reflect changes that have happened in the capabilities of the national security agencies to invade the privacy of individuals, and that the law should be strengthened with a greater accountability regime to reflect the current scale of national security operations. This is the exact opposite of all of the reassuring words we were being given.

Could you tell me briefly, because I have another line of questioning, what concrete steps, if any, are being taken to amend the National Defence Act so that it actually addresses the dangers that metadata can pose to individual privacy and reflects that today's modern capabilities are different from when the Defence Act was last amended?

•(1235)

**Mr. John Forster:** Just quickly, then, I don't think we would ever say metadata does not have an important privacy interest—

**Ms. Joyce Murray:** Excuse me. Not to be rude, but I want to ask that question. That's all I have time for.

What concrete steps are being taken to put in place the recommendations, if any, of the Privacy Commissioner?

**Mr. John Forster:** Thank you, sorry.

We've met with Chantal Bernier, interim Privacy Commissioner. We've given her a briefing. We're reviewing her recommendations. The government is reviewing the legislation in the context of past commissioners' recommendations for changes to the act, and that will be for the government to—

**Ms. Joyce Murray:** Okay. So under review, no concrete steps at this point. Thank you.

Mr. Lindsey, since you're here I have a question about the estimates that I'm hoping you can answer. At a Senate committee on

national finance on March 19 of last year, you testified that the net decrease in authorities for National Defence in the 2013-14 main estimates was from:

...the sunseting of Canada First Defence Strategy budgetary authorities of \$832 million....

And you noted that the department will seek a reinstatement of the CFDS funding:

...once Treasury Board approves our investment plan.

You also noted:

We would seek that authority through supplementary estimates in 2013-14.

Did Treasury Board approve your investment plan that would allow that funding that lapsed to be reinstated?

**Mr. Kevin Lindsey (Assistant Deputy Minister, Chief Financial Officer, Finance and Corporate Services, Department of National Defence):** Mr. Chair, Treasury Board has not yet approved that investment plan. That said, an additional \$400 million in CFDS funding was approved for the 2013-14 fiscal year. I believe I spoke to that increase in funding before this committee in the context of supplementary estimates (B).

**Ms. Joyce Murray:** Thank you for that answer.

So \$832 million, which was a part of CFDS's authorities and plans, was sunsetted or allowed to lapse. You did not receive authority for the investment plan, but you did get \$400 million. What was that used for?

**Mr. Kevin Lindsey:** This is really testing my memory, with all due respect, Mr. Chair.

I did testify and give the distribution of that \$400 million. Again, I believe it was in the context of my testimony here for supplementary estimates (B). I do not have that distribution with me today, nor is my memory of it firm enough that I dare give you an answer today. But we could follow up.

**Ms. Joyce Murray:** Okay.

**Mr. Kevin Lindsey:** Or refer to the earlier testimony.

**The Chair:** Thank you, Ms. Murray. Time has expired.

Mr. Williamson, please.

**Mr. John Williamson:** Thank you, Chair.

Just as a point of note, while I take the privacy concerns of Canadians extremely seriously and think it's vital that we remain on guard and always vigilant when it comes to that privacy, I do want to highlight the difference between our organization and the NSA to follow up on Mr. Bezan's point.

In the U.S. the NSA budget is over \$50 billion. It's not just 10 times our budget, it is over 100 times our budget—just to highlight the capabilities. I feel sometimes people see what's happening in the United States and automatically assume the same thing is happening in this country, given some of the reports. I think it is important to highlight the difference in capability.

On that question, Mr. Forster, do you feel you have the resources to do your job adequately, to safeguard and protect the country as you're mandated to do or your group's mandated to do?

• (1240)

**Mr. John Forster:** I believe so, yes. Since 9/11 and with the advent of cyber-threats that have increased dramatically over the past several years, the organization has about doubled in size in the last 12 years. We have outgrown our current facility and are moving into a more state-of-the-art facility that will allow us to fulfill our mandate given to us by government and collect the intelligence that the government needs.

**Mr. John Williamson:** Thank you.

Rear-Admiral Patrick Finn, I'd like to.... Finally, you're thinking, you get to talk about some hardware. How are things going with the shipbuilding on the east coast? I'm a member from New Brunswick. This project is vitally important to our economic interests. I know it's important to the defence of the country. I'm curious to know how you feel the procurement strategy is going and if there have been any hang-ups or any updates you can offer us today.

**Rear-Admiral Patrick Finn (Chief of Staff, Materiel Group, Department of National Defence):** As you can appreciate, the shipbuilding strategy has many projects that underpin it and, in fact, a few projects that precede it are very large enablers. For example, the modernization of the Canadian patrol frigates, a very important ship to the navy, is well under way. The shipyard in Halifax has delivered a number of those ships, which are out on sea trial. This year is a very important one for us as we do some of the high-end trials, culminating in the first ship coming back into the fleet fully modernized at the end of the year. The shipyard has also delivered the last of the midshore patrol vessels for the coast guard, another key enabler. Right now in Halifax, a brand new state-of-the-art shipyard is on the ascendency.

A lot of work has gone in, specific to our other projects unfolding on the east coast. We are well on our way to completing the design of the Arctic offshore patrol ship, and certainly completing that design before we start construction is a very large enabler to success. We anticipate being in contract later this year and to start construction of the first ship next year. On its heels will come, as I like to describe it, building through the Arctic offshore patrol ships into the next generation of surface combatants. That long-term approach is serving us very well so far.

**Mr. John Williamson:** That's very good.

How about on the west coast, can you update us? I think that's more coast guard, if I'm not mistaken, but are you able to provide an oversight on that as well?

**RADM Patrick Finn:** It's principally coast guard. Again, we're working—and one of the things about the strategy is that it has brought the users of federal fleets working much more closely together for the Canadian Armed Forces. It's also where the joint support ships will be constructed, so we are engaging there as well. Another shipyard has recently—as of yesterday, I've got some photos of their new crane, their new facilities, and everything they're building out there to be a real top-end shipyard. They'll be building through some smaller coast guard vessels and then into the joint support ship and other ones like it. That is also moving forward.

**Mr. John Williamson:** Thank you.

Thank you, Chair.

**The Chair:** Thank you.

Mr. Harris, will you be splitting your time?

**Mr. Jack Harris:** I will splitting my time with Ms. Michaud.

Mr. Forster, I would like to explore the relationship between CSEC and the law enforcement agencies. The act says that you were to provide technical and operational assistance to these agencies. How many occasions in a year would you have to engage in the specific operations with other agencies?

**Mr. John Forster:** I'm sorry, Mr. Chair, I don't have that number with me, but if we can release that and provide it to you, we would be happy to do so.

**Mr. Jack Harris:** Can you give us a number for the last several years, the last three or four years, so we can get an idea of what the scale of operations are?

I think in your testimony you said that you operate under their—

**Mr. John Forster:** Oh sorry, Mr. Chair, if I may, I do have a bit of a number for you that I could give you actually, sorry, just looking at my notes. Between 2009 and 2012, there was a total of about 294 assistance requests. The average is about 70 to 80 per year.

**Mr. Jack Harris:** In those averaging 70 to 80, you're technically an operational assistant. Would you be operating under their wiretap warrant, for example?

**Mr. John Forster:** Yes, where we're providing assistance to law enforcement or security, we operate under their authority. If CSIS wants assistance in collecting information on a Canadian in Canada, they must go to court, they get a warrant, and then we're just providing technical help for them to do that under their lawful authority, which they have to demonstrate they have.

• (1245)

**Mr. Jack Harris:** Is that because you have the superior technology or you have the backdoor—

**Mr. John Forster:** We would have capabilities.

**Mr. Jack Harris:** —you have the backdoor access to these networks that Bell and Telus have?

**Mr. John Forster:** No, I wouldn't say that.

**Mr. Jack Harris:** You wouldn't say that, but it's not true?

**Mr. John Forster:** No, we would have the technical assistance—

**Mr. Jack Harris:** You would not say it because it's not true or you wouldn't say it because you're not going to tell us?

**Mr. John Forster:** No, sir, we would provide technical assistance to them. It could range from computer assistance to collection to other aspects they would need for their investigation, and it would be done lawfully under their authority and their warrant.

**Mr. Jack Harris:** You're acting under their warrants, but you could actually do the technical accessing of the private information.

**Mr. John Forster:** Only if they've gone to court and got a warrant

**Mr. Jack Harris:** No, we're already in court now, we've got a warrant, and they're coming to you for assistance.

**Mr. John Forster:** It's their operation, their authority, and we would provide some technical assistance.

**Mr. Jack Harris:** Okay, but the nature of that technical assistance is what I'm interested in. What I'm asking you is whether you are able to use your technical capabilities, to actually intercept private communications on the existing networks of Bell Canada or Telus or Rogers or any of these networks. Is that the case?

**Mr. John Forster:** No, we would have to do that only through them, through their assistance, with the telecommunications companies. They would approach this.

**Mr. Jack Harris:** So you don't actually collect the information on their behalf through your systems?

**Mr. John Forster:** It depends what the particular case is.

**Mr. Jack Harris:** So you do?

**Mr. John Forster:** I said it depends what...you'd need to give me a specific, sir.

**Mr. Jack Harris:** Well, we were talking about an intercept warrant, which requires the interception of private communications. You would actually do the work with your equipment, is that the case?

**Mr. John Forster:** No, it may be helping them with forensics on a piece of computer equipment that the RCMP has obtained under warrant. It could be a range of technical assistance.

**Mr. Jack Harris:** Are you saying, no, you don't actually do the interceptions yourself under their warrants?

**Mr. John Forster:** Again, if they have the lawful authority, they would go to a telecommunications company and say, "We have a court order to access this information." They may need our assistance with encryption. They may need our assistance with forensics on a computer drive. It could be a range of technical assistance.

**Mr. Jack Harris:** But they don't use your access to those services?

**Mr. John Forster:** They use our technical assistance; that's all I can tell you at this point.

**Mr. Jack Harris:** Thank you, Mr. Chair.

Ms. Michaud.

**The Chair:** Barely 30 seconds....

[*Translation*]

**Ms. Éline Michaud:** I'll be very quick.

My question is for the Department of National Defence officials.

Coming back quickly to supplementary estimates (C), I saw that DND was transferring \$25,000 to the National Research Council of Canada for the assessment, management and remediation of federal contaminated sites. Could you please provide to the committee, in writing, the details on how that money is being used?

In my riding, Portneuf—Jacques-Cartier, there are TCE-contaminated sites in Shannon caused by the Valcartier military base. Although federal money is earmarked for the cleanup, there is very little of it and it isn't accessible quickly enough.

So I'd like to have the details on how that \$25,000 is being used and see whether it includes the cleanup in Shannon.

[*English*]

**The Chair:** A very brief answer, please.

[*Translation*]

**Ms. Éline Michaud:** Actually, since the witnesses won't have enough time to give me the details now, I'd just like the answer in writing.

[*English*]

**The Chair:** So yes or no?

[*Translation*]

**Mr. Kevin Lindsey:** We can provide the answer in writing, of course.

I would, however, like to make one thing clear. The transfer in supplementary estimates (C) is for \$25,000, not \$25 million.

**Ms. Éline Michaud:** That's the same information I have. I apologize if there was a mistake in the interpretation.

[*English*]

**The Chair:** Thank you.

Mr. Norlock, please.

**Mr. Rick Norlock:** Thank you very much, Mr. Chair.

Through you, once again, to the witnesses, for appearing today.

Unfortunately, Mr. Forster, I'm going to have to be asking you some questions. I would just love to ask General Hood some questions, but I think we need to clear up a few things.

Most of these questions are as a result of a CBC story that aired, that I believe you responded to when you appeared before the senate defence committee. You said it wasn't an accurate story in that you said it was not an operation at the...I think you referred to Pearson Airport, and that it was the construction of a model. I think in that testimony you said that basically you were sending around some parameters in that model and that you wanted to compare it to a previous model, from 2005, I think you said, or 2006.

• (1250)

**Mr. John Forster:** No, that doesn't apply. It was the date the first ministerial direction was signed by a minister around metadata.

**Mr. Rick Norlock:** So it was seeing where you're standing with the ability to collect this metadata, which is not an operation. Because it was reported as an operation, am I correct?

**Mr. John Forster:** Yes, I think the report implied that we had accessed the computer networks of an airport to collect the information. I think what we clarified was we were using an historical sample of metadata from our global collection that was used to build an analytical model that helped us find foreign targets. I think the commissioner issued a statement as well on his website saying that he had come in, looked at that case, and found.... I believe his words were that the activity did not include:

"... 'mass surveillance' or tracking of Canadians or persons in Canada; no CSEC activity was directed at Canadians or persons in Canada."

**Mr. Rick Norlock:** So you were in compliance with the law. You were in compliance with the reason the facility exists. You exist to protect Canadians from foreign intervention, from people who want to do us harm. Because of an inaccurate story, we get a whole lot of misinformation out there and people questioning...again, a whole bunch of people concerned with privacy. Everybody was fired up. But in the, I think, 18 years of your existence...?

**Mr. John Forster:** It's in 16 years of the commissioner's existence, not to go back to the Second World War.

**Mr. Rick Norlock:** In 16 years of the commissioner's existence at no time was it ever found that your agency went above and beyond those operational requirements...the accumulation of data and the protection of Canada. At no time have you superseded.

I guess my question to you would be, if any loyal Canadian employee you have under your command or under your system were to circumvent, would there be checks and balances to make sure the commissioner would eventually look at any concern? I guess that would be the correct question. And the commissioner would have reported that in his annual report.

**Mr. John Forster:** Not in his annual report. He's required by law to immediately notify both the Minister of National Defence and the Attorney General of Canada if he feels the agency has acted outside the law.

In addition, if our employees suspect there is any unlawful activity going on in the agency, we have an internal ethics officer they can report to, or they can go directly to the commissioner who performs that role if one of our employees felt we had gone outside the law.

**Mr. Rick Norlock:** Thank you very much.

I'd like to quickly clarify once again for Canadians, because most of us around this table understand what metadata is. So to be very clear, the evidence that came out from the Senate committee is, why do you collect metadata?

Could you very briefly tell us why you do metadata as opposed to...because it's a specific piece of information in the global context of what you do?

**Mr. John Forster:** Metadata is the data around a communication that allows it to be rooted and managed through global communication networks. That's not to say there aren't important privacy interests in that data that we are required to manage and protect in accordance with Canadian law.

We use metadata to understand global networks, so when we're trying to find a foreign target in a sea of billions and billions of communications, we can then know where to look to find our target.

We also use metadata to be able to distinguish Canadian from foreign communications so we're not targeting. So it actually helps us avoid targeting Canadians and focus on our foreign targets. So it must be used for foreign intelligence purposes.

● (1255)

**The Chair:** Thank you.

Ms. Murray.

**Ms. Joyce Murray:** I'm interested in this explanation you have just given, Mr. Forster, because one of the key concerns the Ontario Privacy Commissioner Ann Cavoukian has is in creating a framework for how to pursue targets that may be foreign terrorists. You're utilizing the metadata, and because Canada does not have a density of those targets, it means the kind of framework is going to, in effect, cast a very wide net.

Her concern expressed in a personal communication with me...that means many people could be targeted. Because it's such a wide net, a lot of people could be caught in that net who are not a security concern. So that could be very much a risk to our democracy. People start to be concerned about what website they use, or what activities they do, or who they talk to because they may be caught in this very broad net that is based on metadata collection and analysis and considered potential targets of CSEC's activities.

Could you give me your response to that concern?

**Mr. John Forster:** Sure. Thank you. I'd be happy to.

Again, although we collect metadata, it's very much limited in its use to our existing mandate, which is foreign intelligence collection and cyber-defence. The restrictions we have around that is to understand global networks to find foreign targets. We're not using it to target Canadians or anyone in Canada for our intelligence-gathering activities unless we're assisting CSIS and RCMP under a court warrant. Otherwise our activities are aimed at foreign targets outside Canada to collect intelligence against priorities established by the government.

We have to have measures in place to protect the privacy of that information. That's what the commissioner reviews carefully and reports on. He has done six reviews over the years by three different commissioners of metadata and found those activities to be lawful.

**Ms. Joyce Murray:** I made a comment about that earlier. Something can be lawful because the law just fails to address it because something is so new, and when the law was written it was not an issue. I find it not very reassuring to be told that this is lawful when our tools for analysis and horsepower for analysis that we've never had before were not imagined when the law was written.

You are able to identify Canadian targets if you have a ministerial authorization.

**Mr. John Forster:** No, not at all. The ministerial authorization is there if we're pursuing a foreign target outside Canada, somebody in another country.

When we're collecting intelligence on that target we have no way of knowing if that person may be in communication with someone in Canada, so the authorization says if you're pursuing a foreign target and they are talking to someone in Canada, if the minister authorizes it according to the criteria in the act, you may collect that one-ended communication. We are not allowed to collect Canadian-to-Canadian communication or two-ended. That's forbidden.

**Ms. Joyce Murray:** Then you can connect that end of the communication, and we've had intelligence security experts say that these authorizations are like blank cheques, that there are some very broad authorizations, which we're not privy in this group to know exactly how broad, but it's been described to me by an academic whose life study is this issue that it's essentially a blank cheque. There's a blank cheque that allows you to track back to Canadians the foreign metadata you collect, and so I think the concern stands that this could be a pretty—because we don't have a great quantity of actual, real examples of terrorist activity in our country...to put an algorithm in place to analyze this data is creating a wide net, and potentially going to put a lot of people on a list.

● (1300)

**The Chair:** That's your time, Ms. Murray.

With barely two minutes left till the top of the clock, Ms. Gallant.

**Mrs. Cheryl Gallant:** Thank you, Mr. Chairman.

Mr. Forster, there seems to be a lot of anxiety about the use of new metadata. Certainly no Canadian likes the idea of government snooping in their personal business, but, in reality, meta tags, metadata is used by Google, the social media, and even commercial retailers to track their potential and previous customers' whereabouts.

Would you care to explain to this committee how the metadata is used for commercial aspects? Perhaps we should be more concerned about that than the organization that is trying to protect Canadians.

**Mr. John Forster:** Certainly private commercial companies use metadata, so when I click onto my CBC website in the morning, it's providing me with the Ottawa weather and the Ottawa news because it knows I'm in Ottawa, so it's providing that information to me. If I'm a retailer, as you said, it's providing information that I might be interested in.

The federal Privacy Commissioner has written a number of reports on that, and that's an area they follow quite closely in terms of the use of that information by commercial, for-profit companies.

Just to reiterate and reassure again, our collection of metadata—it's impossible for us, when we're collecting it on the global infrastructure, to disaggregate Canadian from foreign, so we collect, then we use it to target foreign people. We don't use it to build targets of Canadians. We can only target Canadians if we're assisting CSIS or the RCMP under a warrant. Otherwise our mandate and our law is focused on foreign intelligence collection and the metadata we use is to help us understand those networks and to find that target in a sea of billions of communications.

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

Thank you, Ms. Gallant.

Thank you, Mr. Martin, Mr. Lindsey, General, Admiral.

The meeting is adjourned.

---





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

---

### SPEAKER'S PERMISSION

---

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

---

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

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

---

### PERMISSION DU PRÉSIDENT

---

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

---

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