House of Commons
CANADA

Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness

SNSN • NUMBER 011 • 1st SESSION • 38th PARLIAMENT

EVIDENCE

Wednesday, May 4, 2005

Chair

Mr. Paul Zed

Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness

Wednesday, May 4, 2005

● (1535)

[*English*]

The Chair (Mr. Paul Zed (Saint John, Lib.)): Good afternoon, colleagues. I call this meeting to order.

As you know, I've been away on a bit of a vacation, and I want to say I'm very happy to be back. I understand that during this time the subcommittee has had several meetings and, as part of our review of anti-terrorism, Minister Cotler has been here and Minister McLellan. The subcommittee has also heard from FINTRAC and has received a briefing on security certificates.

[*Translation*]

Mr. Serge Ménard (Marc-Aurèle-Fortin, BQ): Given the kind of holidays you take, I must say that we were concerned about you and that we are extremely happy to see you smiling, healthy and ready to take on the considerable workload that awaits us.

[*English*]

The Chair: Thank you very much, Serge. I also want to thank all of you for the good wishes I've received and personally thank our vice-chair, Kevin Sorenson, for the great job he's done chairing these meetings on my behalf. I want to thank you all for the collaborative approach we're taking in our committee.

Speaking of work, we have much to do this afternoon. This is a special four-hour meeting. I want to welcome the first witnesses we're going to be hearing from. We'll be hearing from the Office of the Superintendent of Financial Institutions from now until just beyond 5:30, and we'll be meeting in camera after that to discuss some committee business. Our meeting today will also obviously be interrupted by votes, after which we will hear from the Communications Security Establishment, and we'll adjourn at 7:30.

So without any further ado, I'd like to welcome our first witnesses, Julie Dickson, Brian Long, and Alain Prévost. Do you have an opening statement?

Mrs. Julie Dickson (Assistant Superintendent, Regulation Sector, Office of the Superintendent of Financial Institutions Canada): Yes, thank you.

I would like to thank the subcommittee for this opportunity for the Office of the Superintendent of Financial Institutions to provide information as part of your review of the Anti-terrorism Act.

I would like to introduce my colleagues. Brian Long is a director in the compliance division, and he is specifically responsible for anti-terrorist listings and anti-money-laundering assessments at OSFI. Alain Prévost is OSFI's general counsel.

OSFI is the primary regulator of all federally incorporated financial institutions in Canada, as well as federally administered private pension plans. The first key element of OSFI's legislative mandate is to supervise institutions and pension plans to determine whether they are in sound financial condition and meeting minimum plan funding requirements respectively. Also, we have to ensure that they are complying with their governing law and supervisory requirements. Second, we are to promptly advise institutions and plans in the event that there are material deficiencies and take, or require management boards or plan administrators to take, necessary corrective actions expeditiously. Third, we advance and administer a regulatory framework that promotes the adoption of policies and procedures designed to control and manage risk. Finally, we monitor and evaluate system-wide or sectoral issues that may have a negative impact on financial institutions.

Our legislation also requires that we have due regard to the need to allow financial institutions to compete effectively and take reasonable risks. It recognizes that management, boards of directors, and pension plan administrators are ultimately responsible and financial institutions and pension plans can fail.

With respect to the Anti-terrorism Act, OSFI plays a small but important role in Canada's ability to identify and freeze potential terrorist assets. As you know, the Anti-terrorism Act made amendments to the Criminal Code that, together with United Nations suppression of terrorism regulations, permit the federal government to maintain lists of names of persons or entities where there are reasonable grounds to believe they are involved with terrorist activities. So I will refer to these two pieces of legislation together as the act and regulations.

OSFI's role related to these terrorist lists is twofold. First, due to our ongoing relationships with federal financial institutions, as well as provincial regulators, we maintain an updated list on our website of all names and aliases of potential terrorists that have been identified under the act and regulations. OSFI is not involved in determining the names on the list, but we act as a convenient intermediary to assist both federal and provincial financial institutions to meet their obligations under the act and regulations. Financial institutions are expected and obliged to scrutinize these lists of terrorist names to determine if they have customer accounts in the names of any person or entity on that list. Should this occur, they must freeze any assets held and report the details immediately to the RCMP, CSIS, and FINTRAC.

Second, as provided under the act and regulations, OSFI receives monthly reports from federally regulated financial institutions indicating whether they have identified assets belonging to persons or entities on the list. If they have not identified any such assets, they are required to file a nil report to us. Provincial and financial institutions file similar reports with their respective regulators. This process is designed to ensure that financial institutions are carefully reviewing customer lists on a continuous basis and reporting the results to the regulatory authorities.

As you know, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act requires many financial entities, including federally regulated deposit-taking and life insurance companies, to take the steps necessary to deter and detect money laundering and terrorist financing. These requirements, taken together with the searching and reporting obligations under the act and regulations, have resulted in financial institutions committing significant time and resources to the fight against money laundering and terrorist financing.

● (1540)

Financial institutions must be vigilant in fulfilling these obligations, not only to combat money laundering and terrorist financing, but also to protect reputations. Because of the importance we place on these matters, OSFI has a program in place to assess the ability of our financial institutions to comply with their obligations. Where necessary, we make recommendations for improvements to their anti-money-laundering and anti-terrorist-financing controls, and we follow up on their implementation.

Since June of last year, we have been sharing with FINTRAC information related to policies and procedures that financial institutions adopt to ensure their compliance with the record-keeping, reporting, client identification, and compliance regime requirements of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. As a result of our memorandum of understanding with FINTRAC, we have been able to direct our anti-money-laundering and anti-terrorist-financing efforts to two areas that are of concern to both of our agencies, thus making our work more targeted and more effective. For example, FINTRAC's analysis of reports filed with it can give rise to concerns about the systems that are used to generate those reports. OSFI's work can then be targeted to these systems and we can make recommendations for changes and improvements.

Overall, we are satisfied that the financial institutions that we regulate and supervise take their anti-money-laundering and anti-terrorist-financing obligations seriously and are committed to discharging their obligations in a timely and effective manner.

This completes my remarks, and we'd be very happy to answer your questions.

● (1545)

The Chair: Thank you very much.

Mr. Sorenson, did you want to start?

Mr. Kevin Sorenson (Crowfoot, CPC): Thank you again for coming here.

I remember the last time you were here you guys were sitting in the back and waiting patiently. We never did get an opportunity to hear you, so we apologize on behalf of the committee. FINTRAC was here that day and we got onto a certain line of questioning. If I remember, there was a vote or something that came up and we were unable to hear you. I'm glad you are here today. I look forward to the line of questioning.

As I go through this, some of the questions I was going to ask I think should perhaps be better asked again of FINTRAC. Let me make sure I have this right. You have compiled a list of entities and you are the liaison with our financial institutions. Our financial institutions have to keep records of transactions they have every month. If all of a sudden, at the end of the month, they believe they maybe have had a transaction that has dealt with some type of terrorist entity, they then have to report to you. You have no way of disciplining any financial institutions. You would then report it to the RCMP or report it to FINTRAC and they would basically go through the records with the financial institutions. Is that correct?

Mrs. Julie Dickson: First of all, we don't compile the lists of terrorist names. We receive that information from the government and we put it on our website, in part to provide one-stop shopping to financial institutions so they don't have to go to a lot of government websites to get these names. So it assists them in doing their searches.

We want them to do continuous searching. We don't want them to just search what might have happened one day of the month. We want them to be doing this all the time. We do want a report sent to us every month. That is a requirement, but also, if they have to send in a report that says “nil”, it provides you with some comfort that someone actually did do all the work because they wouldn't send a report in that says “nil” if they had not done the work.

The details of any amounts that might have been uncovered aren't given to us. Those details are sent by the financial institution to law enforcement agencies. We are more concerned about whether the financial institutions have the processes in place to search their records and identify whether there are any relevant accounts. All bank regulators in the world worry about money laundering and terrorist financing. So bank regulators also have guidelines telling financial institutions that they must have procedures in place, they must know their clients, they must ensure that there are training programs in their institutions, and they must ensure that there is an audit internally of whether their procedures work. If we found a financial institution that was completely ignoring that, we do have powers under our act that we can use, but typically it doesn't get to that. We have a meeting with the financial institution, and as soon as a board or a CEO or senior management learns that there are weaknesses, they get addressed pretty quickly.

Mr. Kevin Sorenson: Other than the banks and the life insurance companies and those types of institutions, what other types of institutions are there, and what happens if they miss a report? What happens if they don't submit a report for that month? Are they allowed so many reports missed and then you bring about the disciplinary action?

● (1550)

Mrs. Julie Dickson: Institutions comply.

Mr. Kevin Sorenson: Everyone has always complied?

Mrs. Julie Dickson: I think it is about 99%. It's pretty high.

Mr. Brian Long (Director, Compliance Division, Office of the Superintendent of Financial Institutions Canada): It's quite high. We do a follow-up for those that may be a little bit tardy, but we track that monthly.

Mr. Kevin Sorenson: And the different types of institutions? Chartered banks, lending institutions, life insurance.... What else?

Mrs. Julie Dickson: Yes, we're responsible for the banks, life insurance companies, property and casualty insurance companies, trust companies, loan companies. There are credit unions, but they are not our responsibility. They are regulated provincially.

Mr. Kevin Sorenson: We got somehow, last meeting, into the question of auctions, auction companies—you know, clearing houses. They're a great way of laundering money—bringing in valuables and exchanging them for currency.

Are auction companies on that list as well, some types of auction clearing houses?

Mrs. Julie Dickson: No, they're not our responsibility, but to the extent that banks have auction houses as clients, banks would have to know who they were dealing with. We do have anti-money-laundering guidelines on our website, and if you read them you can see references to high cash value businesses. Banks are dealing with those types of businesses. They have to be extra cautious in dealing with them to ensure they know they are legitimate.

Mr. Kevin Sorenson: Now, I own an auction company, although it's not that active right now, and as far as I know, the bank has never asked to see our books to see what type of auction sales we've done. I guess in our communities—rural Alberta—they realize that it's maybe not the type of auction that would do that. But how closely are they monitored with regard to that type of activity?

Mrs. Julie Dickson: I think our assessment would be that Canadian banks are very good at identifying their customers and knowing who they deal with. Obviously, a lot of these requirements came into play within the last 10 or 15 years, so it's much easier today, I think, with a new client, for a bank to start being quite rigorous in determining who they're dealing with. If you've been dealing with someone for many years, it's a little more difficult to phone them up and ask the types of questions you would ask when someone is establishing a new relationship. We spend a lot of time looking at what's going on internationally and the types of expectations that exist for banks internationally, and we would say that our banks are very high on the list in terms of—

Mr. Kevin Sorenson: How many people work for you? When was the start-up date for your organization, and over the last period of time, how are you being resourced?

Mrs. Julie Dickson: OSFI has about 450 people. It was created in 1987, but that was a merger of the Inspector General of Banks and the Department of Insurance. Half of our people are involved in on-site assessment of financial institutions. The other half would be involved in rule-making, setting guidelines, looking at all transactions that institutions do, etc. In the anti-money-laundering, anti-terrorist financing area we've just increased the resources we have. We have a special unit, which now has about seven people in it devoted only to assessing financial institutions. We've already covered 90% of the system easily, because in Canada, once you've covered the large institutions, you've covered the vast majority of the system.

The Chair: Can you just get to a last question, because your time is running out?

● (1555)

Mr. Kevin Sorenson: Part of that personnel question concerns the types of people who make up your group. Are most of them forensic auditors, are they accountants, are they ex-banking people?

Mrs. Julie Dickson: It would be a combination of people. We would have people who are experts in assessing bank compliance systems, accountants, people experienced as bank supervisors. Our job at OSFI is really to ensure that the processes are in place at financial institutions. They're not the investigators that you would find at the RCMP or CSIS to follow up on details that institutions provide to them.

The Chair: Thank you.

Monsieur Ménard, s'il vous plaît.

[*Translation*]

Mr. Serge Ménard: If I understand correctly, you receive a list of persons or organizations targeted by the legislation from cabinet, is that correct? Once you have received the list, does cabinet sometimes withdraw names?

[*English*]

Mrs. Julie Dickson: When we get the names, we put them on our website, and financial institutions start to search all their accounts to see if they have any that match those names.

[*Translation*]

Mr. Serge Ménard: Has it happened that names have been withdrawn from the list? Did you understand my question?

[*English*]

Mrs. Julie Dickson: Yes.

Mr. Brian Long: Some names have been withdrawn from the list over the years. The cases I recall have all been as a result of changes to United Nations resolutions, another one through an amendment to the UNSTR by Canada.

[*Translation*]

Mr. Serge Ménard: If someone claims to have been unfairly registered on this list, what recourse do they have to have their name withdrawn from it?

[*English*]

Mrs. Julie Dickson: I think you would have to ask the people who create the list.

Mr. Brian Long: Right now you would have to go to, I believe, the Solicitor General and ask for that recommendation to be made to Public Safety and Emergency Preparedness Canada, and they would have to go through a formal process to have the name removed.

[*Translation*]

Mr. Serge Ménard: Apart from those two instances, where it seems that the regulations were changed or that there were other precise reasons, has it happened in the normal course of your business that one or two names have been withdrawn?

[*English*]

Mr. Brian Long: I am aware that there have been some changes to the list as a result of some cleanup by the UN Security Council of some technical types of names, certain aliases, and a very large portion of that happened, I believe, last November.

[*Translation*]

Mr. Serge Ménard: All right.

I understand the reasons that you give, but have names ever been withdrawn because they were unfairly registered on this list?

[*English*]

Mr. Brian Long: Not to my knowledge.

[*Translation*]

Mr. Serge Ménard: Never.

For all intents and purposes, when a person's name is on this list, that person can no longer use their bank account, nor withdraw any money from that account.

[*English*]

Mr. Brian Long: I think it's important to recognize that when a name goes on the list, there has to be more than just the name. A lot of information we request concerns specific identifiers, so that when our institutions get a match between a person's name and a name on the list, they have to do a little more due diligence to rule out that this person on the list and their customer are one and the same. In many cases we refer to these as false positives.

[*Translation*]

Mr. Serge Ménard: That is not what I am asking you.

Here is my question: In practice, when persons with money in a bank account find their name on this list, they can no longer withdraw their money. Is that correct?

● (1600)

[*English*]

Mr. Brian Long: That's correct.

[*Translation*]

Mr. Serge Ménard: Therefore, in practical terms, the money is confiscated. Is it not? It is in the bank, but the person can no longer withdraw it.

[*English*]

Mrs. Julie Dickson: In fact, the money is frozen. The person would not have use of that money, that is true.

[*Translation*]

Mr. Serge Ménard: Has it ever happened to someone, without it having been proven?

I will give you an example illustrated by certain significant events that have taken place recently, particularly the tsunami. Let us take the case of an organization that does not collect money for terrorists but for child education in Sri Lanka, in the part of the country not controlled by the government. In this case, the organization, which was wrongly identified as being one collecting funds for terrorists, and which claimed this was not the case, but rather that they were collecting for child education, would see all of the funds it had collected confiscated.

Mr. Alain Prévost (General Counsel, Legal Services Division, Office of the Superintendent of Financial Institutions Canada): May I say something?

Mr. Serge Ménard: Yes.

Mr. Alain Prévost: You talk about confiscation. The funds are frozen. The person no longer has access, but does not lose his ownership rights, if he can prove...

As my colleague Brian was saying, there are processes, under the Criminal Code, that allow the person to challenge such a decision. They can apply to the Solicitor General to have their name withdrawn from the list.

Mr. Serge Ménard: Fine. To your knowledge, this has never happened.

Mr. Alain Prévost: Perhaps you have a case in mind. There was a fellow in Ottawa who...

Mr. Serge Ménard: No, I had no case in mind.

Mr. Alain Prévost: All right.

There was a case where a person who was registered on the list had their name withdrawn. To my knowledge, it is the only case, except for the changes we alluded to.

Mr. Serge Ménard: All right.

You state that the money is frozen. What happens to it?

[*English*]

Mrs. Julie Dickson: We don't do anything with the money; it's frozen.

[*Translation*]

Mr. Serge Ménard: How long is the money frozen for? Forever?

[*English*]

Mrs. Julie Dickson: If you read the regulations, they simply say it's frozen.

[*Translation*]

Mr. Serge Ménard: There is a provision of the Bank Act that provides, I believe, for funds in accounts that have not been used for five years to be sent to unclaimed bank balances. Up until now, I have been given to understand that you have not had any accounts that have been frozen for five years. Is that right?

What happens after five years? Do you intend to send this money to unclaimed bank balances?

[*English*]

Mrs. Julie Dickson: It's true, there is a provision in the act that says if it's not claimed, it has to go to the Bank of Canada, I believe. After that I think people still have the right to make a case that that is their money, they have a right to it, and they are honest people. At this point I assume those two sections are co-existing, and we haven't reached the point where we would have a case where that has happened.

[*Translation*]

The Chair: You may ask a final question.

Mr. Serge Ménard: We had people here from FINTRAC. It seems to me that there is an overlap between what FINTRAC does and what you do. Can you tell me what distinguishes your work, in practice? I understand that this affects insurance and the safety of pension plans, etc.

What is your role as far as people whose names appear on the antiterrorist list are concerned, whose equity has been frozen?

[*English*]

Mrs. Julie Dickson: We have an MOU with FINTRAC, in part to ensure that we are not both doing the same thing. Our roles are very different. For a number of years we've had an interest in anti-money-laundering, and we've had guidance out since 1990, I believe. So we've always required that institutions know their client and so on. FINTRAC's job is to analyse data financial institutions are required to provide, data we don't get. This would be data on actual suspicious transactions that they have identified and so on. We and FINTRAC work together, so that we avoid a situation where both are in the same institution doing the same thing, looking, for example, at their ability to monitor what's going on and to provide reports on suspicious transactions.

● (1605)

[*Translation*]

The Chair: Thank you.

Mr. Comartin, you have the floor.

[*English*]

Mr. Joe Comartin (Windsor—Tecumseh, NDP): Thank you, Mr. Chair. Thank you for being here.

I want to pursue that last line of questioning, because I had a similar inquiry, and we've had it from the researcher as well. We have an unnecessary overlap. Could FINTRAC take over full responsibility, given that they're doing most of the assessing of the files, and simply report to you on those occasions where they find institutions that are not properly meeting the requirements?

Mrs. Julie Dickson: I would say two things. First, the way we operate now, there is no overlap. We are doing different things as a result of that memorandum of understanding.

Mr. Joe Comartin: I understand that, but I think I'm speaking on behalf of my colleagues when I say we're always concerned, because we've seen around the globe numerous occasions where, in respect of fighting terrorists and dealing with intelligence issues, you end up with multiple agencies. I guess the classic example has been in the United States; when Ridge went in and took over as Homeland Security, he had 80 different agencies to deal with. So is it not possible for FINTRAC to be performing all this and only reporting to you when they find the bank or the insurance company that's not performing according to your regulations and bank regulations? Could they not be doing all of that? They would get the lists from the government and from the UN, and not have you there as—I think you used the term—intermediary or go-between.

Mrs. Julie Dickson: Certainly with the list, anyone could do that. We just had been asked to do it, and it made sense for us to do it, but anyone could do that. There are different models in the world; you might find some bank regulators and some countries doing less and having an agency like FINTRAC do more, and then there are some bank regulators to do even more, because it would be a statutory requirement that they do anti-money-laundering. From our perspective, we are already on site at the financial institutions, because we have to go on site to look at all of their procedures. We look at their board, we look at their senior management, we look at their credit policies, their internal audit. So we were a natural party to continue to do what we were already doing on the anti-money-laundering side, so that FINTRAC could focus on something we were not doing, which is actually analysing data on suspicious transactions, reporting electronic funds transfer, etc.

Mr. Joe Comartin: So you had no particular experience within your framework to deal specifically with that analysis function.

Mrs. Julie Dickson: No.

Mr. Joe Comartin: We may be going back and reinventing the wheel, but could you have developed that expertise, or perhaps more specifically, is it not possible for FINTRAC simply to become a division of yours, doing that analysis?

Mrs. Julie Dickson: From our perspective, it's always a question of focus. OSFI's mandate came into place in 1995 or so, and for now we have a big enough job to do as it is. We have 450 institutions, and all of the prudential aspects of their operations are our responsibility. This would be quite a diversion, and it is a different skill, I think, searching through millions of data points to try to find out whether there's a terrorist or a money launderer in there.

So it is very different work. There are different models out there, as I said, but I don't think that's something where we could leverage our expertise quickly enough.

● (1610)

Mr. Joe Comartin: Thank you, Mr. Chair.

The Chair: Thank you.

Mr. Wappel.

Mr. Tom Wappel (Scarborough Southwest, Lib.): Thank you, Mr. Chairman.

Good afternoon. I want to go back to square one. In your presentation, you said that you maintain an updated list on your website of "all names and aliases of potential terrorists that have been identified under the act and regulations". The act you're referring to, of course, is the Criminal Code, and the regulations you're referring to are the UN suppression of terrorism regulations.

Just tell us again, where under the act do you get the list?

Mr. Brian Long: Under the act, as regulations are being made under the Criminal Code, we would get the names from Public Safety and Emergency Preparedness Canada officials. So we get a heads-up approximately a week before the names are put out by...or under Governor in Council so that we can get prepared for the inclusion on that particular list of those names that were subject to the Criminal Code.

Mr. Tom Wappel: Thank you. And where do you get the names for the regulations?

Mr. Brian Long: We get them from two sources. If it's a specific amendment to the regulation, from a Governor in Council amendment, we would get them from Foreign Affairs Canada officials there. If it turns out it's one that's been made by the UN Security Council, we would normally get a heads-up from our colleagues at Foreign Affairs that a name was going to be put up by the UN Security Council, and then we would follow their website. They have a list on their website that they update. We get it as soon as possible so that we can get it into the public domain in Canada as well.

Mr. Tom Wappel: I don't want to put too fine a point on this, but to quote from Ms. Dickson's presentation, you include "all names and aliases of potential terrorists". Are there any human beings, as opposed to groups, currently listed under the Criminal Code list of entities?

Mr. Brian Long: Not to my knowledge.

Mr. Tom Wappel: So we're talking about groups.

Mr. Brian Long: Under the Criminal Code, all the lists are of groups, I believe.

Mr. Tom Wappel: Now, the definition of "entity" means a person, so it could be a person; a group, so we've got some groups; trust, partnership, or fund, or an unincorporated association or organization.

Do you have any comments as to why an incorporated entity is not listed in the definition?

Mr. Alain Prévost: I must admit that we were not involved in this part of the legislation. In my own personal opinion, I suspect they wanted the definition to be as broad as possible so that they could include any type of organization that could conduct terrorist activities.

Mr. Tom Wappel: I fully agree, but then why not include a corporation in the definition of entity?

Mr. Alain Prévost: Oh, I'm sorry, I missed your question. In the Interpretation Act, "person" is used to mean either an actual person or a corporation. So by drafting convention, person includes both.

Mr. Tom Wappel: Very good. And that's under the Interpretation Act?

Mr. Alain Prévost: Yes.

Mr. Tom Wappel: All right. But at present, as far as I know, there are no corporations on the Criminal Code list. Is that right?

Mr. Alain Prévost: Not to my knowledge.

Mr. Tom Wappel: You mentioned an MOU with FINTRAC. Could we have a couple of copies of that, please?

Mrs. Julie Dickson: Yes, okay.

Mr. Tom Wappel: Do you have anything to do with the criteria established as to what entities go on which list, or are you simply a conduit to the banking and financial institutions?

Mrs. Julie Dickson: We just post the names.

Mr. Tom Wappel: All right.

According to your evidence, if the banks find something they notify the RCMP, CSIS, and FINTRAC, but not you. Is that correct?

● (1615)

Mr. Brian Long: That's correct.

Mr. Tom Wappel: So your involvement ends with ensuring that the banks are examining or checking their clientele lists against the two lists you're involved with?

Mrs. Julie Dickson: Yes.

Mr. Tom Wappel: Again, going back to that line of questioning, since FINTRAC is automatically advised by an institution if there's a problem.... I'm having a little trouble with this overlap and why FINTRAC can't do what you're doing vis-à-vis the anti-terrorism provisions.

Mrs. Julie Dickson: I don't think I said that FINTRAC could not go into a financial institution and ask questions and try to determine whether those institutions have procedures in place, and so on, to get reporting. The issue was that because we were already in the institution, asking a lot of questions pursuant to our safety and soundness mandate, it made a lot of sense for us to pick up on that and to have FINTRAC focus on what we couldn't do.

Mr. Tom Wappel: Okay.

Let's go back to this freezing of the assets. Has it happened?

Mrs. Julie Dickson: Yes.

Mr. Tom Wappel: Can you just help us with the procedure? You've already told us that you're not aware of any person whose assets have been frozen, but the assets of a group are frozen at a particular bank. What happens? Is that group notified that the assets are frozen?

Mr. Alain Prévost: There is no specific notification requirement.

If I may just add, as was mentioned previously, we do the reporting both under the Criminal Code and the United Nations suppression of terrorism regulations. There are individuals listed under the regulations, not under the Criminal Code. So in the case of an individual, his or her account would be frozen by the operation of law; there is no notification process involved. I assume that when they go to the bank to get their money, they will be told, no, you cannot have it—and it's the same for a corporation or group.

Mr. Tom Wappel: So if there is no notification procedure under the Criminal Code, do you have any idea why that is? Don't you find that peculiar? If a person or entity's bank account is frozen, would it not make some sense to advise them their bank account is frozen?

Mr. Alain Prévost: If I may add, once cabinet has determined that a person or group has to be listed, it is all public and published in the Canada Gazette. So I assume that people are presumed to know that their names have been added to the list. But you're quite right that there is no formal notification process.

Mr. Tom Wappel: So the account is then frozen and the owner of the account is not notified that the account is frozen. Are there any procedures in any law that provide for what is to happen to that frozen money, other than what Mr. Ménard mentioned about it eventually going to the Bank of Canada?

Mr. Alain Prévost: Under the Criminal Code and the provisions added by the anti-terrorism legislation, there are some processes that the Attorney General of Canada may apply to a court, on request, to have the money seized or forfeited, but only under the new provisions added by Bill C-36.

Mr. Tom Wappel: But that's only available to the Attorney General, not to the owner of the account, right? Or is it available to both? If the owner of the account wants the money, what does he or she do?

Mr. Alain Prévost: I guess the recourse would be to challenge the listing. There is a process.

Mr. Tom Wappel: There's a process for that.

The Chair: Last question.

● (1620)

Mr. Tom Wappel: Thank you.

Is it accurate to say that if nobody does anything for the five-year period, then the money goes to the Bank of Canada?

Mr. Alain Prévost: I believe it's 10 years.

Mr. Tom Wappel: Well, whatever the statutory limit is.

Mr. Alain Prévost: Again, it's just a matter of the money being shifted to the Bank of Canada. As Ms. Dickson indicated, the people who claim that money, instead of going to their own banks, would go to the Bank of Canada to get the money back, assuming they have been delisted by that time.

Mr. Tom Wappel: All right.

Thank you very much, Mr. Chair.

The Chair: Mr. Cullen, and then Mr. MacKay.

Hon. Roy Cullen (Etobicoke North, Lib.): Thank you, Mr. Chairman. Thank you, Ms. Dickson, Mr. Long, and Mr. Prévost.

If I put it into my own words—maybe you can tell me if I've got it wrong—OSFI has a responsibility to safeguard the soundness and safety of Canada's financial system, which consists of a number of different financial institutions and different types.... Is that a fair reflection?

I want to come to that in the context of terrorists. Are there ways in which terrorists could undermine the safety and soundness of Canada's financial system? I'm thinking not just about money laundering. Obviously, if there was too much money laundered through Canada's financial system—I don't know how you define that—that would seem to me to create some soundness and safety issues.

Maybe you could comment, Mr. Long, when I come back to you. What is our assessment of the extent of money laundering that we believe is going through the financial system, and when do we get to a point where it could endanger the safety and soundness of the system?

I'd like to talk more generally about whether there are ways that terrorists could subvert and undermine the integrity of the financial system in Canada beyond just money laundering. There have been a lot of cyber-hackers. I think I've read that it is a target for terrorists. If they can undermine the financial system of a country, they can create a lot of havoc. I wonder if you could comment on that. Are there threats? What are they? And what is OSFI doing to respond to those threats?

Mrs. Julie Dickson: I can start that off.

I think every financial institution in the world realizes that the world is a different place today than it used to be. Tremendous amounts of money and time are being spent to think about the safety and soundness of the sector. A lot of time is being spent now, for example, on business continuity planning, because after the 9/11 attacks there were a lot of post-mortems done on what could have been improved in the financial services sector, even in agencies like OSFI. I think everyone learned a few things after that. Internationally, there continue to be discussions on best practices to deal with crises that may happen.

In terms of hackers and things like that, institutions continue to spend a lot of money trying to deal with them, because I think they recognize that with the business they are in and the move towards Internet-based banking, etc., they need to spend the money. I think they are probably in the forefront in that industry in trying to protect themselves. We don't have to be in there telling them to do that. They've got business reasons to do that. That is good news in a sense.

Hon. Roy Cullen: I know we don't want to give terrorists a lot of ideas, but presumably someone at OSFI has done some risk assessment. OSFI looks at the system in a holistic sense, so that while the banks have proprietary interests, it surely is OSFI's responsibility to make sure the whole system, in a holistic way, is protected as best it can be against terrorist attacks.

Have you done that kind of analysis and risk assessment and developed that into a response or some type of a preparedness plan?

Mrs. Julie Dickson: OSFI, like any organization, would have a plan. Internationally, we participate in the financial action task force, and part of the work of the task force is to look at threats, ways of money laundering, and ways of terrorist financing.

Our participation in the FATF ensures that we are involved and are aware of emerging issues there. For example, the FATF would have a list of things it thinks people should now start to focus on, and that would include wire transfers, charitable organizations—

● (1625)

Hon. Roy Cullen: But the FATF is focused mostly on money laundering, is it not?

Mrs. Julie Dickson: And terrorist financing as well.

Hon. Roy Cullen: But money laundering that's associated with terrorist financing.

Mrs. Julie Dickson: Yes.

Hon. Roy Cullen: The only point I'm making is, I would hope that OSFI steps back and looks at these kinds of threats in a holistic way and has some responses that might be appropriate.

That leads me into this. Mr. Long, it's always a problem, but can we make an assessment of the extent of money that's laundered through our Canadian financial system, when that becomes a threat to, let's say, the soundness of our system?

Mr. Brian Long: That's a very good question. Unfortunately, we don't have those sorts of statistics yet. I know the RCMP, in previous years, have put some estimate on money laundering that's going through the system, but accurate assessments are just not possible at this stage.

It's the same with the terrorist.... As you recall from FINTRAC's testimony, they found something like $70 million, I believe, for 2004-05. They think that may potentially double now for suspicious transactions. Once they do the analysis, if it came through, I think that number would drop significantly. It really is difficult to put a number to it, because you're dealing with crime. As long as there's crime in your country, you're going to see some money laundering so they can bring it back into the system.

Hon. Roy Cullen: I suppose there's a question of measurement of how much money laundering, but is there a measurement technique that would say when it reaches this proportion of transactions we've got a major problem?

Mr. Brian Long: Not to my knowledge. Really, I think that would come out through law enforcement's assessment of the actual cases they see and that sort of thing.

At this stage, we're just looking at deterring and detecting, particularly on the deterrence side, to try to stop our institutions from being used for money laundering.

The Chair: I'm sorry, I just want to let you know we have a bell for a procedural vote.

One short last question, and then Mr. MacKay, and then we're going to suspend.

Hon. Roy Cullen: I wanted to ask about.... There has been some concern in the past. If we look at offshore financial institutions and—I don't want to generalize—let's call them weaker regulatory regimes and how that could threaten the stability of the financial systems of the world, not to be too dramatic about it, is there still work going on there, and where are we at? Is that still a concern with insurance companies, reinsurance, offshore institutions of a variety of types?

Mrs. Julie Dickson: There is a list of jurisdictions that aren't cooperating. That's a list you can find on the FATF website.

Because we are a consolidated supervisor, we would look at banks' activities, no matter where they are. We would indicate that if you are operating in a country where anti-money-laundering detection has been identified as an issue and where work needs to be done, our guidance would suggest that you must be extra vigilant in those areas. We will also visit some of those countries if our institutions have major operations, for example, to make sure they are applying their anti-money laundering policies throughout the entire organization.

Hon. Roy Cullen: I wasn't only thinking about money laundering, but the effects on—

The Chair: Thank you, Mr. Cullen.

Mr. MacKay.

Mr. Peter MacKay (Central Nova, CPC): Thank you, Mr. Chair, and thank you all for your presence.

I apologize for the generality of this question, but I guess I'm trying to get a clear mandate that you follow. It's the gathering and analysis of information that is provided solely to you from these financial institutions. Is that correct?

Mrs. Julie Dickson: With respect to the list of terrorist names, we simply get a sheet from each institution at the end of every month. Typically, it says, “Nothing Found. Nil.”

● (1630)

Mr. Peter MacKay: But you don't have any input into what's on that sheet; you simply analyse what you get back in return.

Mr. Brian Long: We get this sheet. Our role is as a conduit. We don't even get the individual names, if there happens to be more than one. All we do is get an aggregate number. We do no analysis of that. Our mandate is simply to ensure that it's being done and processed. What we expect our institutions to do, if there happens to be what we call a positive hit and assets are frozen, is contact the RCMP as quickly as possible and CSIS, as well as FINTRAC, so that law enforcement and intelligence are involved as soon as possible. They will do the analysis and follow-up with the institutions.

Mr. Peter MacKay: I appreciate that use of the word “conduit”. So you don't verify the listing process, nor do you actually verify the receipt of the information that comes back from the financial institutions.

Mr. Brian Long: No.

Mr. Peter MacKay: So by extension, you can't speak to the veracity at either end of that process, either the provision to the banks of the listing or what comes back in return. Correct?

Mr. Brian Long: That's right.

Mr. Peter MacKay: This question may be a penetrating statement of the obvious, but the issue of those who could escape detection by virtue of not being caught in this process, I guess, like a credit union at the provincial level.... Let me flip it around the other way. Can I ask you this? If you're the terrorists—maybe this is the simpler way—how do you avoid detection? Where do you go to hide your money?

Mrs. Julie Dickson: If your name is on the list, you can't really go anywhere.

Mr. Peter MacKay: But what if you're not on this list?

Mrs. Julie Dickson: If you're not on the list, I think you're captured by suspicious transaction reporting and that sort of thing.

Mr. Peter MacKay: But if we're looking to close the filter here, as just one that comes to mind, a provincial credit union doesn't appear to be caught in this process anywhere.

Mrs. Julie Dickson: It's regulated, though; it's covered.

Mr. Peter MacKay: It's covered?

Mrs. Julie Dickson: Yes.

Mr. Brian Long: We don't administer the regulations, we're subject to them, like the institutions they report to us. All federal institutions report to OSFI, and provincial institutions report to their respective regulators.

Mr. Peter MacKay: I see, at the provincial level. So there is a similar body provincially.

Mr. Brian Long: Exactly.

Mr. Peter MacKay: Do you from time to time, at the federal and provincial levels, share information?

Mr. Brian Long: We get information from some of the provinces with regard to the filings. We collate that, for purposes of making sure, and we cross-reference with RCMP on occasion, just to make sure our numbers are similar to their numbers.

Mr. Peter MacKay: I guess my concern—I think Mr. Cullen was going in this direction too—is the perception that we could be having these various silos doing rather specific tasks, but that the information wouldn't sometimes be shared, or that there are still some areas in which cracks could appear.

Mr. Brian Long: Certainly, the provincial companies, as well as federal, if they have a positive hit, have an obligation to share it with the RCMP, CSIS, and FINTRAC.

Mr. Peter MacKay: Then my final question would be this. This is voluntary on the part of the financial institutions themselves. Where is the enforcement mechanism? Not to say that they wilfully disobey and refuse to provide this information, but how do we ensure the integrity of the information and ensure the thoroughness of their checks? They're required to do so, but who's doing the follow-up to say, you're doing it thoroughly, you're doing it properly, you're doing it on time, you're doing it in a way we have determined to be the standard? Who does that?

Mrs. Julie Dickson: We're certainly playing a role. Brian and his team, for example, would be going into institutions. You can easily identify if an institution is an outlier.

● (1635)

Mr. Peter MacKay: An outlier?

Mrs. Julie Dickson: For example, if we are talking about suspicious transaction reporting, FINTRAC will tell us if one institution doesn't seem to be reporting the same kinds of transactions that another institution is reporting, and that is very useful information we can follow up on. Part of our role is to take action if a financial institution is not reporting in the way you think they should be reporting. We actually will go on site to look at account opening procedures to ensure that they're actually doing what they say they are doing. So there is some follow-up to ensure that the expectations that are out there are actually being met.

Mr. Peter MacKay: You're telling me that you do check the mechanisms or procedures that they're following. I guess it's an issue of how do you look for something if you know it's not there, as we're dealing with very sophisticated individuals. It's analogous to guarding the ports, if I could make that analogy, as port officials are sometimes paid a considerable amount of money not to be at a certain location at a certain time so that they're not participating, but noticeably absent, allowing criminality to occur.

Again, it's not that I would finger any particular institution or any person in those institutions, but how do we ensure that this type of activity doesn't go on, where an individual working in a bank simply does not report? Where are the teeth or enforcement?

Mrs. Julie Dickson: There are a lot of checks and balances in a financial institution.

Mr. Peter MacKay: Okay—

The Chair: I'm sorry to jump in, but your colleague wanted a short, piggybacked question.

But first, colleagues, we'll come back after the vote at 6:15 or 6:20.

Mr. Tom Wappel: But it's only 20 minutes to 5 right now?

The Chair: I realize that, but there's a vote, and then there's another set of votes, so there's no point in coming back.

Mr. Tom Wappel: Are we anticipating that another set of votes is going to occur right after this vote?

The Chair: Yes, at 5:45, so there's no point in coming all the way back and going on.... I'm in your hands, colleagues, but by the time you get to the 15...you're not going to be able to make it.

Mr. Kevin Sorenson: In that case, there are two things. Does your group have any recommendations that could make Bill C-36 better, as we review it? Is there anything out there that you believe could make it better or that should be brought forward?

My other question goes to Mr. Ménard's question on the freezing of assets. If all of a sudden someone has an account with $1 million in it, and they aren't notified, what happens if they come to the bank to make another deposit—but not to withdraw money or have a cheque go through? What happens if they put in another $1 million? Is that money taken?

Mr. Alain Prévost: I could perhaps quickly answer the second question.

The Chair: I'm sorry, but would you mind providing us with a written answer to that question?

After talking with the researcher, I'd be interested in getting a little bit more clarification on when the funds get transferred to the Bank of Canada. How long do they stay there, or do they stay there in perpetuity? How much money is there currently on deposit at the Bank of Canada?

Mr. Kevin Sorenson: Nothing has been turned over to the Bank of Canada yet, has it?

Mrs. Julie Dickson: If you don't use your account—

The Chair: It does get turned over to the Bank of Canada.

A voice: Eventually.

The Chair: They said there were moneys there, but I'd like to know how much.

No? Okay, that answered our question.

I'm sorry, colleagues, but we're suspending because we have to go to a vote.

● (1640)

_____ (Pause) _____

● (1909)

The Chair: I would like to welcome the Communications Security Establishment, and Keith Coulter, Barbara Gibbons, John Ossowski, and David Akman. Welcome

We're going to go right to your presentation. We're mindful of your time and are sorry about things being a little delayed, but we were voting. So thank you.

Please proceed, Mr. Coulter.

[*Translation*]

Mr. Keith Coulter (Chief, Communications Security Establishment): Mr. Chairman, members of Parliament, thank you for inviting me to appear before you today as chief of the Communications Security Establishment. I welcome this opportunity to talk to you about the impact the Antiterrorism Act has had on CSE.

● (1910)

With respect to its protection mandate, CSE's ability to protect electronic information and systems was being similarly eroded. In the new cyber-environment, CSE needed to monitor activity on the government of Canada's networks, and to sample messages that have characteristics associated with viruses and other malicious codes. Yet the Criminal Code prohibition against intercepting private communications also prevented CSE from undertaking these essential protection activities. As a result, the essential tools of information protection were rapidly moving beyond CSE's reach as well.

● (1915)

[*English*]

Nothing could have highlighted more clearly the limits of CSE's authorities than the events of September 11, 2001. In the aftermath of these events, the CSE provisions in the Anti-terrorism Act were designed to ensure that CSE's authorities reflected both the requirements of the new security environment and the realities of modern communications, as well as the obligation to protect the privacy of Canadians. Specifically, steps were taken to exempt CSE from part VI of the Criminal Code where CSE could demonstrate that it needed this to fulfil its mandate. The act thus created a mechanism, an authorization by the Minster of National Defence, that allowed CSE to get back into the game.

I want to be very clear here about how this works. Under the legislation, CSE is prohibited from directing its activities against Canadians or anyone else located within the 12-mile limit that defines Canadian territory. CSE is also prohibited from directing its activities at Canadians abroad, defined in the act as Canadians or permanent residents. However, under ministerial authority, when directing its activities at foreign entities abroad, CSE can now conduct operations even if doing so risks intercepting private communications. When this occurs, the act allows CSE to use and retain these communications if a very strict set of conditions is met; otherwise, upon recognition, they are deleted. Similarly, CSE may obtain a ministerial authorization to carry out essential IT security activities that run the risk of intercepting private communications. In practice, with respect to both foreign intelligence and IT security, CSE requests ministerial authorization to ensure legal protection against what otherwise would be a Criminal Code offence of intercepting private communications that may be incidentally acquired by CSE in the course of carrying out specific collection and protection activities. It is important to understand here that such activities, or class of activities, to use the legislative phrase, are only permitted once the minister is satisfied, following an in-depth review by the Department of Justice, that the specific legislative conditions have been met.

Since CSE's legislation was passed, ministerial authorizations have allowed us to significantly increase our ability to provide high-value foreign intelligence. Obviously, I can not go into detail about CSE's foreign intelligence successes in a public forum. I can say, however, that intelligence provided by CSE has been directly responsible for helping to protect Canadian troops in Afghanistan from terrorist attack. I can also say that CSE has provided intelligence on foreign terrorist targets used to protect the safety and interest of Canadians and our closest allies. This was intelligence CSE would not have been able to acquire without the Anti-terrorism Act. Similarly, CSE's IT security program has used ministerial authorization to ensure that the Government of Canada's computer systems and networks are better protected from cyber-attack.

Let me now turn to the critically important measures CSE has in place to protect the privacy of Canadians. Before approving a ministerial authorization, the minister must be satisfied that, among other things, satisfactory measures are in place to protect the privacy of Canadians. In this regard, CSE has in place comprehensive procedures to ensure that its activities respect the charter right to privacy in letter and in spirit. This obligation is taken very seriously by all CSE employees, who receive extensive direction and training in this area. In addition, CSE has instituted new procedures for activities conducted under ministerial authorization to ensure that CSE's activities are always directed at foreign entities abroad and that any intercepted private communications are used or retained only if they are essential to international affairs, defence, or security. CSE also works closely with an on-site legal team assigned from the Department of Justice to ensure that its practices and procedures satisfy all legislative requirements.

● (1920)

In addition, the role of the CSE commissioner, former Chief Justice of the Supreme Court of Canada, the Right Honourable Antonio Lamer, who operates independently, was formalized in the Anti-terrorism Act. The commissioner has a mandate to review CSE's activities to ensure they are lawful. He has unfettered access to CSE personnel information and documentation.

The commissioner is required by the act to report to the Minister of National Defence annually on his review of CSE's activities. The minister then tables this report in Parliament. The commissioner also provides classified reports to the minister on a regular basis. These focus on specific programs or issues.

Allow me to note here that since the office was established in 1996, the commissioner has consistently confirmed that all CSE activities reviewed were lawful. In addition, I note that since the Anti-terrorism Act was enacted, the Office of the Privacy Commissioner has examined CSE's activities conducted under its new mandate; no issues of concern were identified.

[*Translation*]

In short, I believe the authorities granted to CSE under the Antiterrorism Act provide the right foundations for the organization's activities while protecting the privacy of Canadians.

The act responded to an urgent need to update CSE's authorities, allowing the organization to address new threats and to keep pace with the rapidly changing communications environment.

[*English*]

These new authorities are now absolutely essential to CSE's operations, its ability to successfully overcome formidable technical obstacles, and ultimately its ability to contribute to Canada's security and other national interests. Indeed, in the current strategic and technological environment, CSE could not function effectively without them.

Three and a half years ago, the Minister of National Defence and I explained to Parliament what CSE needed to help protect the security of Canadians. Parliament had the more difficult task of ensuring the right balance between protecting the privacy rights of Canadians and protecting the nation's security. In the end, it provided CSE with the critical authorities it needed to be effective in the new strategic and technical environment.

It is my hope that Parliament will continue to support this authority structure so that CSE can continue to help address the very serious security challenges facing our country.

Thank you. I'd be happy to respond to your questions.

The Chair: Thank you, Mr. Coulter, and thank you, colleagues, for putting up with our being a little bit tardy today.

Tonight we'll start with Mr. MacKay.

Members have been sending me notes and asking me, so I think we will try to finish with this panel of witnesses, and probably that will be the work or the business for this evening.

Mr. MacKay, go ahead, please.

Mr. Peter MacKay: Thank you, Mr. Chair, and I want to thank all of you for being here and for your patience this evening.

I want to go first to the mandate of the commissioner, Mr. Justice Lamer. Is it my understanding that the commissioner can review these ministerial authorizations and then report back to the Minister of Defence? Is that the line of authority?

Mr. Keith Coulter: He does report back to the minister. There are two ways he does that: an annual report, which is made public, and very specific reports on specific operational things. In addition to that, under this legislation he has a responsibility to report not only to the Minister of National Defence but to the Attorney General any issues he has with respect to lawfulness.

● (1925)

Mr. Peter MacKay: That was my next question. In terms of the authority, then, of the commissioner, does he have the ability to demand the withdrawal of a ministerial authorization? Who outranks who, I guess, in that relationship?

Mr. Keith Coulter: It's the minister who would withdraw the ministerial authorization—

Mr. Peter MacKay: Can the commissioner request it?

Mr. Keith Coulter: The commissioner's responsibility is to report on the lawfulness of CSE's activities. If he had difficulty with a specific ministerial authorization and we thought we were operating outside the law—we haven't had this happen—I think within a heartbeat the minister would withdraw that ministerial authorization and we'd have to present the facts. We'd undoubtedly have a very thorough investigation to determine what had happened.

The commissioner has a philosophy that he outlined in his last annual report, and it includes a proactive element, in terms of how he thinks about his mandate. There's the kind of "looking in the rear-view mirror, was it lawful, was everything conducted lawfully" kind of approach that he's responsible for. But in addition to that, he feels he needs to report to the minister on anything he feels is a weakness in a procedure, or could develop into a legal program in a very dynamic environment where the technologies are changing and everything—and he does that. He makes a lot of recommendations, many of which we implement, in order to stay ahead of any possible problems.

So it's not just reporting on an infraction; it's reporting on how we're performing and his view on whether that's going to keep us in the legal parameters or not. That's done on an ongoing basis.

Mr. Peter MacKay: Sure, and I understand they are there to essentially complement each other, but if there were an adversarial issue.... I guess my question again is, if the commissioner is of the belief that something is outside the law, when it comes to this ministerial authorization, what recourse is there, and how would that be resolved? Are you saying it would be resolved internally?

Mr. Keith Coulter: I believe if the commissioner reported us to be out of the bounds of the law, he and his staff would portray reality, and we'd be in a world of hurt. It hasn't happened, because we're constantly working with the Department of Justice on every possible legal interpretation as we move ahead.

Mr. Peter MacKay: But if we boil it down, warrants are sometimes struck. I realize this is a different type of process, but if we're using that type of analogy there are occasions when the authorization is inappropriate, new evidence comes to light, or information turns out to be false.

I guess I'm just trying to establish what happens when that process breaks down and the commissioner is in conflict with the minister.

Mr. Keith Coulter: First of all, I think we would react in a huge way to that. We'd shut down the program and fix whatever the problem was. But in addition to that, the commissioner would report about our lawfulness behaviour in his public report. I think that would be information that Parliament and parliamentarians would have. Without getting into specific operational details, which he would describe to the minister, there would be a general infraction kind of portrayal in the public domain, and that would be a big setback for CSE.

That's why we play the game the way we do, with the Department of Justice, very rigorous procedures, and everything. We know we would lose the trust of parliamentarians and the Canadian public if we ever got to that point.

Mr. Peter MacKay: Sure. My understanding of this process of ministerial authorizations around the interception of private communications is that power is vested in the Minister of Defence. Why does the minister have the ability to authorize the interception of private communications—simply because they are coming from outside of Canada? That seems to be the criteria. Why isn't a warrant required, as is the case for interception of private communications inside Canada? Do you understand?

● (1930)

Mr. Keith Coulter: Yes, I understand the question.

Mr. Peter MacKay: That seems to be the big difference.

Mr. Keith Coulter: And that's the crux of the legislation, because it's about enabling CSE through this ministerial authorization process.

In the kind of business that CSE is in, intercepting communications in faraway places in the world has always been the executive prerogative of governments.

For example, just a wee bit before CSE's time, our predecessor organization, during the Second World War over in Europe, intercepted German communications. These were foreign-to-foreign communications. That's our bread-and-butter business. I can't imagine the Canadian army commander—all these images are on TV right now—swinging through Europe, having to go back to a Canadian court to intercept the communications of a German panzer division. This has always been the executive prerogative. All our allies work that way.

The trouble we had when we faced our set of circumstances following 9/11 was that we had this absolute prohibition against acquiring private communications. We were trying to intercept the communications of foreign entities abroad, but this absolute prohibition made it impossible for us to do that, because we had to, before the interception, guarantee that it would be a foreign-to-foreign communication.

In the modern communication landscape, that bar had been set too high. We couldn't get a 100% guarantee that you had foreign-to-foreign communication in any haystack or on the electronic highway. So we couldn't even touch the highways and haystacks, and we were essentially winding down out of the business.

In addition to that, if we had a terrorist target abroad and it had a communication into Canada, we wanted to be able to acquire that. If there was an al-Qaeda target in a faraway place and they were communicating into a city in Canada, that was a communication we sought the authority, from Parliament, to acquire, use, and retain, and that's what it gave us.

Mr. Peter MacKay: And are the majority of the requests—I presume they come from CSIS—and the targeted individuals or groups predominantly in the area of anti-terrorism, as far as the intercepts? Is that correct?

Mr. Keith Coulter: Right now, if you look at the reporting as one metric on this, over 75% of our business is in the security domain, and that's a little broader than terrorism. That's proliferation as well. It is counter-intelligence as well. It's cyber-threats as well.

And these days it is hugely a support to military operations—I referred to panzer divisions and intercepting communications in Europe during the Second World War—because we have troops deployed abroad and we're very involved in helping to intercept communications so they can paint the picture of what the local threats are to them.

Mr. Peter MacKay: Okay.

And what are the requests, just to finish that question?

Mr. Keith Coulter: Of the requests we get—for security—a lot come from CSIS and a lot come from the defence department. And Foreign Affairs is always a big client, and it plays on the security agenda as well. Those are the highest-demand clients.

The Chair: Thank you, Mr. MacKay.

Mr. Comartin, please.

Mr. Joe Comartin: Mr. Coulter, the CSE was obviously substantially smaller before September 11, 2001. Could you give us a ballpark figure, percentage-wise, of how large it has grown since then? How many staff did you have at that point? What was your budget before that period of time and what is it now?

Mr. Keith Coulter: Our growth has been over 50% in population, and our budget.... Barb, you've got the numbers with you.

Could I ask Barb Gibbons to respond?

Ms. Barbara Gibbons (Deputy Chief, Corporate Services, Communications Security Establishment): I'll start with the budget first. Our budget, before 9/11, was $140 million. Budget 2001 actually gave us an increase of 25% over that. Then budget 2004 gave us another 25% increase over and above that. As of 2007-08, ongoing, our budget will be at $220 million, in the dollars of those years. So there have been considerable increases. We're looking at a 57% increase in our budget. As far as the people go, the resources, before 9/11, we were under 1,000 people—about 950. With budget 2001 funds, we actually grew by about 35%, so we got an increase of 350 people. Budget 2004 gave us an increase of another 350—another 25%—so that by 2007-08, we're looking at a population of about 1,650, which is a 65% increase over where we were pre-9/11.

● (1935)

Mr. Joe Comartin: In terms of interceptions, can you tell us how many you were doing pre-9/11 and how many you're doing in the current period of time?

Mr. Keith Coulter: We don't talk publicly about the volume of our business. We needed this authority to be able to launch a couple of new collection programs—things that are done technically that we would not have been able to do technically without this new authority. Our collection is increasing, but neither ourselves nor our international partners talk publicly about how many terabits of information we collect and that kind of thing, because it reveals information that you just can't make public in a business like we're in.

Mr. Joe Comartin: In terms of the authorizations by the minister for interceptions that may include private conversations, how many of those have there been since the changes came about?

Mr. Keith Coulter: The volume of that is very, very low, and if you look at, broadly, the work we've done since 9/11 under our new authority and the number of reports we've issued based on private communications defined in the Criminal Code, the number is very low. It's in the dozens, but beyond that, I don't think I should specify publicly what it is. I said to Parliament, when we sought the legislation, we were projecting what this new authority would mean and we didn't really know. I said it would be extremely low volume, in my view, and very high value, and that has indeed proved to be the case. This is very low volume; we're surgical. We're going for foreign communications; almost all of it is foreign to foreign. There's the odd private communication, and when it's security-related and yields high intelligence value, we now have the authority to share that with the relevant Government of Canada agency so that the right thing can be done.

Mr. Joe Comartin: How large is the staff of former Chief Justice Lamer's agency?

Mr. Keith Coulter: It's a small but effective staff.

John could you answer that? John works directly with them.

Mr. John Ossowski (Director General, Policy and Communications, Communications Security Establishment): I think in total there are six reviewers. There's an executive director and some admin support, so I think in total there are about eight staff. One of the reviewing staff is a contract person. Most of them are people who have worked with the SIRC review process or the inspector general for CSIS.

Mr. Joe Comartin: A number of them came out of the CSIS staff originally, didn't they?

Mr. Keith Coulter: I should say here that we're auditable, and because of the way we work, we're fairly easy to get to know. You don't need huge numbers to come. They have unfettered access; they can come in and look at any program, get briefings, see what the facts are, and call for the information they need quite easily. It's not a hard business. It's not as difficult in the high-technology kind of intelligence we do as it might be in an agency that has people all over the country and that kind of thing. We're Ottawa-based.

● (1940)

Mr. Joe Comartin: With the current inquiry that's going on under Justice O'Connor, has CSE been involved at all in any of the investigatory work that inquiry has done?

Mr. Keith Coulter: Yes, we are fully cooperating with the inquiry. Beyond that I wouldn't comment, but I do, whenever anybody brings up this issue, like to make the point that Mr. Arar is a Canadian. We do not target Canadians, so we did not target this individual.

Mr. Joe Comartin: You're not able to tell us the nature of the investigation the O'Connor inquiry has conducted with regard to your agency?

Mr. Keith Coulter: No, I'm not at liberty to talk about it. The government position is that as long as the inquiry is going on, we don't engage on that issue.

Mr. Joe Comartin: Those are all the questions I have.

The Chair: Thank you, Mr. Comartin.

Mr. Wappel, please.

Mr. Tom Wappel: Thank you, Chairman.

Good evening.

As you know, this committee is charged with reviewing the Anti-terrorism Act, so my first question to you is, do you have any recommendations for us for changes to part V.1 of the act, positive changes, drafting resolutions, or anything like that? Is there anything you'd like us to take a look at?

Mr. Keith Coulter: Knowing that the legislation would be reviewed in this manner, before the process started, we did a very comprehensive review from an internal perspective of the act, as to whether we thought there were any gaps that needed to be addressed. The conclusion of that work was that at this time we do not have anything we need added, and we certainly can't afford to have anything subtracted. The basic thing we went for was this ministerial authorization, the ability to risk the interception of private communication, to be protected from that, in order to be effective. We got that, we're happy with it and the way it's working, and we don't have a gap we can identify at this time.

That said, our business is very complicated technically, and the way technologies evolve, the words can end up not working any more. At some future point we might be back to say we need some amendments to the legislation, but at this point, having done this very comprehensive review, we're not bringing a proposal forward.

Mr. Tom Wappel: I have just a couple of drafting questions then.

Could I refer you to paragraph 273.64(2)(a), "shall not be directed at Canadians or any person in Canada".

Mr. Keith Coulter: Correct.

Mr. Tom Wappel: Is there any reason why you had the words "at Canadians" in there?

Mr. Keith Coulter: Yes. If anybody in Canada is within that 12-mile limit—

Mr. Tom Wappel: I'll get to that in a minute.

Mr. Keith Coulter: But we're dealing with Canadians abroad defined as citizens or landed immigrants. So this is a prohibition against targeting you as a Canadian travelling abroad.

Mr. Tom Wappel: So shouldn't it read, "shall not be directed at Canadians anywhere or any person in Canada"? Isn't that what it means?

Mr. Keith Coulter: It could say that, but that's the meaning of it; that's the way we're reading it and implementing it.

● (1945)

Mr. Tom Wappel: Why "any person in Canada"? What if Osama bin Laden found himself in the Rocky Mountains?

Mr. Keith Coulter: It would not only be my hope, it would be my expectation that a sister agency would take care of this man and bring him to justice.

Mr. Tom Wappel: Which sister agency would that be?

Mr. Keith Coulter: CSIS.

Mr. Tom Wappel: You would not be able to assist in that work?

Mr. Keith Coulter: We could. Paragraph 273.64(1)(c) says we can "provide technical and operational assistance" to CSIS. So if they wanted assistance, we would be able to technically or operationally assist them. But this would be done under their authority, their rules, their mandate. We would be in a supporting role.

Mr. Tom Wappel: Paragraphs 273.64(1)(a) and (b) are exempted under subsection 273.64(2), but not paragraph 273.64(1)(c)?

Mr. Keith Coulter: Correct.

Mr. Tom Wappel: Take a look at subsection 273.63(1). I'm just not sure what this means: "The Governor in Council may appoint a supernumerary judge or a retired judge". Must the commissioner be a supernumerary judge or a retired judge?

Mr. Keith Coulter: By this legislation, yes.

Mr. Tom Wappel: Does it say that? "May" is not a mandatory word.

Mr. David Akman (Director and General Counsel, Legal Services, Communications Security Establishment): When we drafted it, our intent was that we would have to have a judge, whether a supernumerary or a retired one. This was because his mandate is to review the activities of CSE to ensure they comply with the law.

Mr. Tom Wappel: In that case, why not use the word "shall?"

Mr. David Akman: That question came up during the clause-by-clause. It could have said "may" or "shall". The question was, what happens if there's no commissioner in place? It would be folly for the government not to have a review body in place for CSE. It's a drafting style, and it could have gone either way.

Mr. Tom Wappel: I'm sorry, I didn't understand. How would there be a gap?

Mr. David Akman: I didn't say there would be a gap. I said you could read in the word "shall", but it says "may". At the time this was going through clause-by-clause, the question was raised whether the government, with the "may" in there, would appoint a commissioner. The answer was that it would be a folly if it didn't, because CSE would need a review body. While it says "may", it was expected that the government "shall", as you're suggesting.

Mr. Tom Wappel: Didn't anybody suggest at the time that the wording could be simply, "The Governor in Council may appoint a Commissioner who shall be a supernumerary judge or a retired judge"?

Mr. David Akman: I don't think that wording was ever brought forward. It could have been, but it wasn't.

Mr. Tom Wappel: That's amazing. I'll bring it forward now then.

Where do you get the 12-mile limit?

Mr. Keith Coulter: Our territorial limit goes out 12 miles past the coast of British Columbia. Legally, those are Canadian territorial waters and are defined by law as Canadian territory.

Mr. Tom Wappel: That's not defined in part V.1?

Mr. Keith Coulter: No, but it says "in Canada", which legally means within the 12-mile limit, not the 200-mile limit. Canadian territory is legally defined under international law to be the coastline plus 12 miles.

Mr. Tom Wappel: There's no way we can extend it to the exclusive economic zone?

Mr. Keith Coulter: Those are international waters for legal purposes. It's an economic zone that's recognized legally. But we could do an interception beyond the 12-mile limit.

Mr. Tom Wappel: You were talking about the collaboration between you and others. Is everything okay between you and CSIS? Do you collaborate with the RCMP and the Canadian Forces?

Mr. Keith Coulter: Is everything okay?

Everything's not perfect. We've been working at this since 9/11 in terms of collaborative arrangements. I have a joint management meeting in a couple of weeks again with CSIS senior managers and my senior management team, some of these folks and a few others, and we're trying to get perfect. One way that I put it is that nothing less than perfect is acceptable. In this day and age, where if we miss something it could have disastrous effects, you have to keep striving towards it. So we're working hard at it.

We've worked very hard with CSIS. Without the legislation, CSE wasn't of much value to CSIS. Now, with the legislation we're on the security agenda. We're producing intelligence of value to them, and we're tightening up tremendously as an organization as well.

We've had a traditional partnership with DND that goes back to the Cold War. We actually last year brought in a formal integrated model, directed by the minister, who's the minister for the Canadian Forces as well as CSE, where I and some of my folks sat with generals and we worked out a way to get better at this. We're implementing what we call the integrated SIGINT operational model. So that's coming along.

We're working closely with the RCMP, and it's getting better. We're working through the issues.

I'm not declaring perfection here, but I think it's going in a good direction.

● (1950)

Mr. Tom Wappel: Do you collaborate at all with the Border Services Agency on immigration matters?

Mr. Keith Coulter: We provide intelligence. When you talk about, for example, what we do with DND and with CSIS, there's so much back and forth, analyst to analyst kind of work and whatnot. With the Border Services Agency we are trying to provide them with more and more meaningful foreign intelligence so that they can paint the picture outside of the country, which helps them react the right way at the border.

For example, the deputy minister of the Border Services Agency was out for a visit a week or so ago, brought a couple of his people, and we had another go at it, just to try to keep getting better.

So the track we're trying to take here is to get better and better over time at providing the kind of intelligence that really makes a difference and is actionable by these agencies.

Mr. Tom Wappel: Thank you, Chairman.

I'd like a second round, please, if possible.

The Chair: Thank you.

I may as well get Roy in here, because I know he has to go.

Roy, go ahead.

Hon. Roy Cullen: Thank you, Mr. Chairman, and thank you to the witnesses.

The 1,600-odd employees you have are all based in Ottawa? Is that what I thought I heard you say?

Mr. Keith Coulter: Almost all. We have a few working exchanges abroad, and we also have a few who are Ottawa-based, but with departments and agencies on an exchange basis.

Hon. Roy Cullen: And the kinds of communications you track, are they phone messages, telegrams, e-mail? Do you track Internet-based communications as well?

Mr. Keith Coulter: Again, we don't publicly acknowledge anything we do in terms of a specific thing, because to do so would reveal capabilities. But I would refer you in the legislation to the definition called “the global information infrastructure”, and that can be thought about as the whole communications landscape and all of the electromagnetic emissions. We're a technical collection agency. We don't have agents running around getting close to people to get information. We do it technically, so we are into the electromagnetic spectrum.

Hon. Roy Cullen: You must use satellites...there must be gear located around the world that you access. Anyway, we won't go there.

I'd like to come back to the business of the ministerial authorities, and I'm trying to get my head around how broad they are, how targeted they are. Also, maybe you could answer my first question. Are they at times specific, or is it that once you get an authorization, it's there? And would it be country- or region-specific, or target-specific?

Just help me understand a bit more the coverage and the breadth of these authorizations.

Mr. Keith Coulter: The answer to the first part of your question is that they can be good for up to a year, so automatically they are no longer valid after a year; you need to renew them with the minister at that point, if you still want them. So that's the time constraint.

In my opening statement, I did try to say something to describe what they are, as far as we can go. Basically, what we're trying to do is to protect ourselves in each zone, where we may end up intercepting private communications because of the way the technologies are. We seek a ministerial authorization to protect ourselves, and we make it as narrow as we can. We can apply the legislative phrase “activities or class of activities”, and we would go to the minister to seek an authorization for each one of those. Then we have to demonstrate that we meet the conditions for that activity, or class of activities, in terms of the conditions that are laid out.

● (1955)

Hon. Roy Cullen: In terms of the targets then, it could be a region or it could be a specific...? Or maybe you can't even tell me that.

Mr. Keith Coulter: We can't do so publicly. I'm looking forward to the committee's—

Hon. Roy Cullen: That's okay.

I'll move along to another part then, and you may not be able to answer this either.

Let me give you an example. Let's say the finance minister was going to an IMF or World Bank meeting in Rome or somewhere. Given the past history of people dissenting and creating some security threats, do you have any kind of blanket authorizations now? Let's say you wanted to monitor some of the communications traffic to see if there were going to be demonstrations, or perhaps if characters who have been violent at previous meetings were going to show up, etc. Do you have any blanket authorizations to track that, or would you have to go...? Next year, there might be a G-7 meeting in Brazil or something. How does this work?

Mr. Keith Coulter: By legislation, as well as practically, we have to follow Government of Canada priorities. There is a priority-setting process that we follow, so if there is anything happening abroad, a troop deployment, a major area of interest for the Government of Canada, and it's on the priority list, then we do the best we can.

In terms of the priorities, there is also a PCO-chaired committee where that's narrowed down. It's called a requirements committee, dealing with the more operational things we do or with lists of things we would do.

So with that list, we try to stay out in front of this with whatever authorizations are required, so we can pursue Government of Canada priorities.

Hon. Roy Cullen: But would you have any sort of...? Anyway, the ministerial authorizations only last for a year, so if there were a G-8 conference and the PCO or government said it were a priority and it wanted to know what was, or could be, going on at the G-8 meeting next year in Rio, would you have to go back and get a new ministerial authorization to monitor all of the traffic leading up to that meeting, because the last G-8 meeting might have been in Nassau or somewhere? How would that work?

Mr. Keith Coulter: Our authorizations are more technology-based; in our world, we start with the specific realities of technical programs. Before we can apply any technology, the first thing we have to do is demonstrate with 100% effectiveness—with absolute, 100% effectiveness—that we will always target a foreign entity abroad, because it's illegal to target a Canadian, or to be uncertain about that. Once we get to that stage, we can seek a ministerial authorization to carry out a specific collection activity, so the authorizations are based more on technologies, and our activities are not event- or threat-based.

Hon. Roy Cullen: Let's say, for the sake of example, that there was a G-8 meeting in Nassau—it would be nice if there were, not that I'd be going. Let's say you've got an authorization, there were some rumours, and the government said, we want to know...there could be some people who might descend there and create some security threats for our Prime Minister or whatever. That's considered a priority by the PCO, by the government. So you get authority to monitor communications traffic, and in doing so you come across, for example, an indication that there's someone in Canada laundering huge amounts of money into Nassau, maybe for terrorist acts, drug money, or whatever. Tell me what you can and can't do with that information.

● (2000)

Mr. Keith Coulter: You're talking about a foreign communication abroad based around an event with a connection into Canada, is that right?

Hon. Roy Cullen: It just so happens that you're monitoring all this stuff and then, whoops, there's someone moving huge amounts of money into Nassau—laundering money. There's enough evidence to tell after a while that it's drug money or terrorist financing or whatever.

Mr. Keith Coulter: It's a good question because this is exactly what the legislation allows us to do in very strict circumstances.

What you're describing would be a piece of information that could have big consequences. It's in the security zone and all of that. We would put it through the essentiality test. Before we can produce a report based on a communication into Canada, that piece of information would have to meet a rigorous essentiality test. It's written in the legislation.

The Department of Justice has to come up with a lot of legal analysis, and it's a very high bar that we have to go over before we can report. If we've passed that essentiality test and can issue a report, then we would give it to the Canadian government agency for whom it would be of direct interest. That's what the legislation gave us the ability to do.

The Chair: Thank you very much.

Mr. Sorenson, please.

Mr. Kevin Sorenson: Thank you for being here this evening.

You talked about the resources and the increase in resources especially in personnel. Can you tell me what the levels of personnel were in the early 1990s?

Mr. Keith Coulter: It was pretty static there.

Ms. Barbara Gibbons: It was pretty static. In the early 1990s—and I'm going on recollection now because I don't actually have those figures—we were just under 900 or so in size.

Mr. Kevin Sorenson: We know that CSIS, for example, had somewhere between 2,800 and 2,900, and it was cut back to 1,800. The RCMP, in the mid-1990s, lost 2,200 positions. Did CSE have cuts then?

Ms. Barbara Gibbons: No, we were not affected by program review. We were not cut.

Mr. Kevin Sorenson: Maybe there were no cuts, but was there a freeze on hiring?

Mr. Keith Coulter: There was no growth in the budget; therefore, it was a very static population in terms of numbers. I should say that I started five weeks before 9/11, so my whole experience is this growth scenario.

Mr. Kevin Sorenson: Before 9/11—I'm trying to get a grasp on how 9/11 really changed your mandate or the ability you had to collect—you couldn't eavesdrop on any conversation that originated in Canada or was received in Canada, could you?

Mr. Keith Coulter: Correct.

Mr. Kevin Sorenson: After 9/11, you're allowed to do that, right?

Mr. Keith Coulter: That is correct.

Mr. Kevin Sorenson: Before 9/11, were there other countries where the security organizations had the ability to do that?

Mr. Keith Coulter: Absolutely.

What we presented to Parliament after 9/11 was that all of our closest international partners had solved this problem. The United States, the U.K., Australia, and even New Zealand had already acquired the ability to do this.

We couldn't get into the security game. We couldn't get into the terrorist game without this authority for those two reasons that I mentioned in my opening statement. One, we couldn't do that on one end, in Canada; and, two, with the technological revolution, the communications we were trying to protect and the communications we were trying to acquire coexisted in those electronic highways and haystacks.

Mr. Kevin Sorenson: So you were screwed—the French already picked that up.

Yes, you were. And in reality it took the terrorist attack to get Canada really into the game. Other countries had recognized the need, but we were slow coming in on this.

● (2005)

Mr. Keith Coulter: It was a wake-up call. It brought us rapidly forward to the authority structure we needed to get in the game. So it was a historic moment for CSE as well as broadly for North America in terms of the security agenda.

Mr. Kevin Sorenson: I know you came in then, but CSE had certainly tried to get the ability or encourage people to get that ability, but it took 9/11 before you got it.

Mr. Keith Coulter: Parliamentarians asked me when we were presenting the legislation why I hadn't been arguing for this all along. I started just before 9/11, so this wasn't me personally, but there was a public environment in which I think there wasn't support for taking this lead.

Mr. Kevin Sorenson: But there was support in New Zealand, in Australia, in Great Britain, and the United States.

Mr. Keith Coulter: But it became obvious to us at that moment that this was a necessary step for CSE or we were not going to be able to help with this problem and agenda.

Mr. Kevin Sorenson: You're quoted as saying that by late 2001 the agency had so few resources and such limited powers that it was hard-pressed to collect much of the information that is now being intercepted—prior to 2001.

Now just as it took 2001 to get us up to speed on some of the resources and some of the abilities you have, are there other countries now that have other measures for collecting intelligence, for making sure our security is up to speed that we haven't yet incorporated into our plan?

Obviously, you guys must sit around conferences where you say to New Zealand, “Oh, you have that”, or to the United States you say,“You have that ability?” There must be something that these other countries that really have security and intelligence gathering as a priority have that we maybe don't have yet.

Mr. Keith Coulter: You've helped me with the answer. We have very similar authority structures. There are little differences here and there in the way things have been built up over the years. For example, we get a ministerial authorization by the Minister of National Defence; in the U.K. it's the foreign minister. The authority structures are very similar.

If we were talking about the little differences, they're very much on the margins. We have an authority structure that is very similar now to that of those four countries.

Mr. Kevin Sorenson: My last question is this. I think Mr. Wappel or someone asked you which departments would make requests for the information. You said Public Safety and Emergency Preparedness, about safety and emergency preparedness; you said National Defence, obviously, since that's the department you're under. You said Foreign Affairs. And you said other countries may as well.

Tell me exactly what Foreign Affairs would be asking for that National Defence wouldn't. Would it be with...?

Mr. Keith Coulter: It's a good question because we map this kind of stuff, and there's tremendous overlap. Foreign Affairs is in the game of diplomacy and trying to play the security agenda through diplomacy and whatnot. Defence is very focused on their troops and what might come as well as what's really in play, and they generate different, specific requirements for information.

We're in the business of providing information. Wherever there are information gaps we can fill, we're asked to fill them. We get more demands than we can meet, so the game is one of prioritization, and often that means deciding whether we put our weight of effort against specific requirements in Foreign Affairs or Defence. That's why we have that PCO-chaired requirements committee where the discussion gets quite intense, because people want information on the pieces they care about the most.

The Chair: Thank you.

Colleagues, it's moving late into the evening, but Tom has a couple of very short last interventions.

● (2010)

Mr. Tom Wappel: No. I have some questions.

The Chair: All right. Go ahead.

Then Mr. MacKay has a short one.

Mr. Tom Wappel: Mr. Chairman, with all due respect—

The Chair: No, no. Go ahead.

Mr. Tom Wappel: If you don't mind, I'm here and I've given up my evening. I'd like to go through this.

The Chair: We'll be glad to hear you. I'm only wrapping it up.

Mr. Tom Wappel: I only have a few things, if I may, on subsection 273.65(1) on ministerial authorizations.

I don't have a copy of the Criminal Code here, and that's my fault. Do private communications, as defined by the Criminal Code, mean private communications within Canada? Is that what we're talking about?

Mr. Keith Coulter: That's correct. A private communication is basically a communication where the person in Canada has a reasonable expectation of privacy and communicates. That can be outside Canada as well as within Canada.

The private communication provision is geographically defined as in Canada. So you could have two foreigners in Canada communicating with each other in a foreign language, and that is a private communication under the Criminal Code.

Mr. Tom Wappel: What about two Canadians communicating with each other in Las Vegas?

Mr. Keith Coulter: That would not be a private communication, as defined by the Criminal Code, because it's outside the geography. However, we are prohibited in law from targeting a Canadian and therefore could not acquire that communication.

The other thing is that we still have to follow all of the Canadian laws, and charter rights apply to Canadians wherever they are. It's not only the Criminal Code provisions that apply to us; it's all of Canadian law.

Mr. Tom Wappel: But there's nothing that stops you from listening to non-Canadians, and there's nothing that stops you from listening to other governments. Isn't that right?

Mr. Keith Coulter: There is indeed nothing in law that prevents us from doing that.

Mr. Tom Wappel: That's what you do.

Mr. Keith Coulter: Some of that is our business.

Mr. Tom Wappel: Yes. Now dropping down to paragraph 273.65 (2)(c), it says, "the expected foreign intelligence value of the information that would be derived from the interception justifies it". What is "it"?

Mr. Keith Coulter: It justifies the interception.

Mr. Tom Wappel: What is the test for justification?

Mr. Keith Coulter: We have to satisfy the minister that this is not wheelspinning and that it's going to be a productive enough source of intelligence that it justifies the risk.

David, this is clause-by-clause again.

Mr. David Akman: I think the test is that it would meet the foreign intelligence priorities of the government.

Mr. Tom Wappel: So it's not a test of money, or a test of morality, or anything. It's simply a test of whether it would meet the intelligence-gathering needs of the country. Is that right?

Mr. David Akman: Yes.

Mr. Tom Wappel: All right.

On a completely different topic, do you have any facilities located outside Canada?

Mr. Keith Coulter: No.

Mr. Tom Wappel: Okay. You said you have about 1,600 employees, more or less, and you have an operation here. Do you have other locations in Canada?

Mr. Keith Coulter: No, but we work very tightly with the Canadian Forces.

Mr. Tom Wappel: That was my next question. You get support from the Canadian Forces, or listening posts, if I could put it that way, in other parts of the country.

Mr. Keith Coulter: We're the national cryptological agency, as we call ourselves, which means we are the national authority for this kind of business. The stuff the Canadian Forces does is done under our authority and umbrella.

● (2015)

Mr. Tom Wappel: Very briefly, I understand you have an arrangement for information exchange with your counterparts in various countries, such as the U.S., Britain, Australia, and New Zealand. What kinds of arrangements are those? Can you talk about that?

Mr. Keith Coulter: Yes, I can. I'll say this.

This arrangement goes back to the Second World War. It's an historic partnership that has been a very valuable one for Canada as well as those other countries. We benefit from the partnership in ways that are immeasurable. It has become an international effort, and it swung behind the security agenda very effectively. We're all on to it, and we're working very tightly together. It's not only information sharing, and that kind of stuff. It's also technology sharing.

Mr. Tom Wappel: So in that context, do you parcel out the world, and you look after, let's say, North America, and Australia and New Zealand look after the southern hemisphere, or something like that, by agreement?

Mr. Keith Coulter: It's not quite that way. We follow Government of Canada priorities. The legislation says we have to do so, my minister says we have to, and that's what we do.

We help each other. We ask each other for help, and if we are asked by a partner for help, the first thing we do is check to see if this fits with Government of Canada priorities, and if it does, then we will offer assistance, if we can, given our workload and everything. But we share intelligence, and that's a huge benefit, because some of those agencies are a lot bigger than CSE.

Mr. Tom Wappel: I'm sure.

All right. Thank you very much.

Thank you, Chair.

The Chair: Mr. MacKay.

Mr. Peter MacKay: Thank you, Mr. Chair. I want to follow up very briefly on a few questions asked by my colleague Mr. Wappel.

The subject you've been talking about is the anglo-American information sharing, Echelon. Is that the name this group calls itself?

Mr. Keith Coulter: It won't surprise you when I say I can't speak about any alleged or actual operational arrangements.

Mr. Peter MacKay: Okay, just say warm or warmer.

All right. In regard to this group with no name, has Canada ever made the request of one of these alleged partners to intercept information within their country, of a Canadian citizen? Has that request ever been made?

Mr. Keith Coulter: No. It's illegal and couldn't be named.

Mr. Peter MacKay: Okay.

I appreciate that if you can't answer these questions, just do as you've been doing.

Does CSE have the ability, currently—I guess it's more a capacity question—to work in foreign languages? Is that something you are specifically working towards, and can you currently do that to a large degree?

Mr. Keith Coulter: We do. We have expertise in every major language group. That's about as far as we can take it. Language is the—

Mr. Peter MacKay: It's the trade. Sure.

Presumably your analysts are familiar with culture as well as language in that regard.

Mr. Keith Coulter: Absolutely. They're crypto-linguists, not just linguists, which means they have to be able to work in an environment where nuance and meaning are everything.

Mr. Peter MacKay: Sure, and presumably as well then there is a fair bit of recruitment looking for that skill set.

Mr. Keith Coulter: There is, and it's not just linguists. It's engineers, computer scientists, mathematicians, and analysts.

Mr. Peter MacKay: Okay.

Well, to that extent, part of your mandate is also assisting with the security of the government computer systems overall, securing those systems. Can you tell us a little bit about that role? Protecting the integrity of the government's computer systems presumably is a huge task.

Mr. Keith Coulter: It is, and if you're thinking about us the right way, you're thinking of us as the high-end, cutting-edge, leading-edge technical experts. We're small in that area, but we have the technical knowledge that's helpful to the government.

PSEPC, the new department, has overall responsibility for coordinating things, those within government and critical infrastructure in the country and everything, but what we provide into the mix is the leading-edge technical expertise. We're evolving in the direction of the national security policy that came out a year ago, which highlighted the need to be more predictive and preventive, not just reactive. We got some money to move in that direction, and we're evolving to put more weight of effort in that area so that we stay out in front of problems.

I should say here that I worry about the future, because we had some work to do here. The cyber-security issues are going to get bigger if we don't do the right things. I'm encouraged by some of the latest developments, including the latest budget increase for CSE to get out in front of things rather than just react as incidents and cyber-attacks occur.

Mr. Peter MacKay: Presumably that's part of just the accelerated pace at which technology is changing—

● (2020)

Mr. Keith Coulter: Yes.

Mr. Peter MacKay: —and back to my colleague Mr. Sorenson's question about keeping up with our partners and keeping up with technology and the advances that other countries are making.

There would be a fair bit of...I don't want to call it computer envy, but we're watching to see what technology is happening and making sure Canada is keeping pace.

Mr. Keith Coulter: If I could, I'll put in a plug for Canada here. We're hiring people out of the universities into this area who are world-class. We can stack them up against staff of international partners that are doing the same things, and our people hold up really well. It's a strength of Canada, but we have to do some work here in order to keep out in front of the problems we're going to face if we don't do it.

Mr. Peter MacKay: Is that work you're talking about specifically giving them the support and the R and D in some cases to keep the pace?

Mr. Keith Coulter: Absolutely.

Mr. Peter MacKay: That's good to hear. It's good news.

My last question relates to, again, an area we touched on briefly earlier. You were understandably reluctant to answer on the number of ministerial authorizations, but can you say generally if these authorizations are occasionally renewed, and can they be renewed more than once? What I'm getting at is, is there a process of ongoing renewals?

Mr. Keith Coulter: Yes. Indeed, the first one we put in place after 9/11 has been renewed every year. It's possible they'll be in for a long time, but each year we do our assessment before they run out. Some of them are on different timelines, obviously, so it's a constant process.

Mr. Peter MacKay: In the process itself, when you go back, do you have to follow the original process? Is it like a warrant? Do you have to present ongoing evidence or a status report that justifies the renewal?

Mr. Keith Coulter: Yes. The justice department seems to make these documents longer and longer each time—I'm sorry, David—but as we learn, we try to be more precise. As indeed the commissioner makes comments and whatnot, we're getting the process very finely tuned. The minister has to go through documentation. Normally I brief him, and we get a signature—or not—as he sees fit.

John just passed me a note; we can say we've had 24 authorizations. This would be in two categories. We have them for cyber-protection and we have them for foreign intelligence. The total that have been in force since 2002 is 24, and we have six in force now.

Mr. Peter MacKay: Thank you very much, Mr. Coulter. Thank you all.

The Chair: Thank you, Peter.

Joe, you're going to have the wrap-up with just a short, last question.

Mr. Joe Comartin: With regard to the arrangements for sharing, I know CSIS certainly shares with other countries other than the four traditional allies. Does CSE?

Mr. Keith Coulter: We share in general. If you're talking about intelligence products, I can say we share those with our international partners but not all. We have a category of intelligence that is “Canadian eyes only”. We are selfishly in the business of national advantage and we don't share everything with our allies, but we share a good deal.

Mr. Joe Comartin: Who makes the determination as to who we share with and how much we share? Does that go to your desk?

Mr. Keith Coulter: The policy and parameters around that are beyond me; they go to the national security adviser, who has responsibility for CSE. But those are broad parameters; I narrow them down. Below me I have an assistant deputy minister in charge of foreign intelligence, and he makes more tactical decisions within parameters.

But we're careful about it. We share a lot, but we certainly do not share everything, and our international partners don't share everything. In the ultimate end, this partnership works because what we share is to the advantage of the sharer as well as the recipient if it's a security issue, but there are some times when we keep things to ourselves.

Mr. Joe Comartin: Thank you.

The Chair: Thank you.

Well, ladies and gentlemen, I appreciate your indulgence.

Chief of CSE...do they call you "chief"? Is that your title?

● (2025)

Mr. Keith Coulter: They do.

The Chair: They call you "the chief".

Well, thank you very much. We appreciate your presentation this evening and look forward to chatting with you sometime soon again.

We're adjourned.

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

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

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