HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 044 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, February 7, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 7, 2017

● (1600)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): I'm going to call this meeting to order. I see quorum at the table. I know we have a few members who are still coming in.

This is the 44th meeting of the Standing Committee on Access to Information, Privacy and Ethics. We are studying the Security of Canada Information Sharing Act, affectionately known as SCISA.

First of all, I want to apologize to our witnesses for the votes, points of order, and so on in the House that prevented the committee from starting on time, but we do appreciate your all being here.

Our original plan was to have two groups of witnesses for one hour each. I appreciate the fact that you were able to scramble and all come together for the time that we have. I understand there are four individuals from the various organizations who will be doing the initial presentations. If all of you use approximately your 10 minutes and we have one round of questions, that will be exactly 90 minutes, the allocated time, and our committee will be done at 5:30.

Without further ado, I will introduce you and then once I am done, please start your presentations of up to 10 minutes in the order you are introduced.

We're starting with the Department of Foreign Affairs, Trade and Development. We have Mr. David Drake, director general, counter-terrorism, crime and intelligence bureau. With him is Victoria Fuller, director, case management, consular operations; Jeffrey K. McLaren, director, mission security operations; and Patrick Picard, director, access to information and privacy.

From the Department of Citizenship and Immigration, we have Mr. Glen Linder, director general, international and intergovernmental relations; and Michael Olsen, director general of corporate affairs.

From the Financial Transactions and Reports Analysis Centre of Canada, more affectionately known as FINTRAC, we have Gérald Cossette, director. Thank you for being here. And we have Monsieur Stéphane Cousineau, deputy director, corporate management services sector, and chief financial officer.

From the Canadian Nuclear Safety Commission, we have Terry Jamieson, vice-president, technical support branch; and Ms. Lisa Thiele, senior general counsel and director.

My understanding is that Mr. Drake, Mr. Linder, Mr. Cossette, and Mr. Jamieson will be the presenters at the table, and we'll go in that order. We have Mr. Drake for up to 10 minutes, please.

[*Translation*]

Mr. David Drake (Director General, Counter-Terrorism, Crime and Intelligence Bureau, Department of Foreign Affairs, Trade and Development): Good afternoon, Mr. Chair and members of the committee.

I would like to thank you for inviting Global Affairs Canada to speak to you about the Security of Canada Information Sharing Act. I'm the director general of counter-terrorism, crime and intelligence. Mr. Chair, you have just introduced my colleagues.

[*English*]

I will provide a bit of context to help situate the department's perspective on this act. As you are very aware, Canada is facing a wide range of threats to its national and international security.

We are co-operating closely with the many like-minded partners internationally to address the threat posed by terrorists and foreign fighters and to control the export of materials related to the manufacture of chemical weapons and other kinds of weapons of mass destruction. All of these issues are transnational in nature.

The department manages Canada's membership in bilateral or multilateral defence and security organizations that deal with traditional threats to security, as well as non-traditional threats such as threats to cybersecurity and space security.

The department is charged with the maintenance of an international platform with which to perform its functions, namely our network of missions abroad. Global Affairs Canada must therefore continually assess threats to the security of missions abroad, provide appropriate protection, and manage any residual risks to life and property, including diplomatic personnel and assets abroad. Global Affairs Canada provides travel advice and advisories to Canadians, as well as notifications to registered Canadians about safety and security conditions abroad, so they can make their own informed decisions regarding foreign travel.

Our international efforts are complemented by our work with partners within the government to advance Canada's national and international security objectives. A coordinated whole-of-government approach is necessary in addressing international issues like terrorism and foreign fighters. In this respect, the ability to share relevant information is key.

The department already had an established process to facilitate the appropriate sharing of information when issues of national security were at stake. Processes and caveats are in place to ensure that only information that is relevant, reliable, and accurate is shared. The requests must also be compliant with Canada's privacy laws or framework, including the charter and Privacy Act.

Prior to the enactment of the Security of Canada Information Sharing Act, or SCISA as we call it, the information was typically shared under the provisions of paragraph 8(2)(e), when pursuant to a request, or subparagraph 8(2)(m)(i), when proactively shared, of the Privacy Act.

Officials are further guided by the findings of past commissions of inquiry, in particular the report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.

[*Translation*]

SCISA was designed to help the government improve how it deals internally with national security issues, by improving national security information sharing domestically. SCISA aims to ensure that information relevant to national security is shared both effectively and responsibly.

SCISA provides an authority for other departments and agencies to share with our department any information that might bear on the safety of our staff or the security of our missions abroad. SCISA also provides other departments and agencies with a clear authority to request from Global Affairs Canada information relevant to national security or for Global Affairs Canada to proactively share such information.

A number of steps have been taken to ensure that the department is appropriately implementing the new legislation, and that officials understand its impact and limitations.

First, the Minister of Foreign Affairs gave three divisions within the department the authority to receive national security-related information pursuant to SCISA. These areas are international security and intelligence; security and legal; and trade, specifically the international business development and chief trade commissioner in addition to trade agreements and negotiations.

Second, a letter explaining SCISA was sent to all Canada’s heads of missions abroad, asking that they sensitize their staff to the importance of timely and appropriate information sharing to keep Canada and Canadians safe. The letter was jointly signed by the deputy ministers of Foreign Affairs, the director of the Canadian Security Intelligence Service and the commissioner of the Royal Canadian Mounted Police. The letter explained that SCISA doesn't create an obligation to disclose and that this authority needs to be balanced against other statutory obligations, including privacy rights. It directed that, to ensure a systematic approach, requests for information to be shared under SCISA should be referred back to headquarters for decision.

● (1605)

[*English*]

With respect to proactive disclosures, the letter confirmed that information available at mission that could be relevant to Canada's security or to other federal institutions' mandates should be sent without delay to headquarters, where officials would determine whether, how, and with whom the information will be disclosed. It emphasized that for urgent cases, headquarters will respond quickly, including outside of normal business hours.

An exception is made for exigent circumstances where there is an imminent threat to life or a threat of serious bodily harm. In those instances, the good judgment of all heads of mission is relied upon, wherever they may be, to share information directly and immediately with the relevant counterparts, and then to report to headquarters to advise of any such disclosures at the first available opportunity.

The third implementation step taken was to develop an information sharing agreement between the consular operations bureau and CSIS. This agreement lays out the parameters within which the department will share consular information with CSIS under SCISA, including practical modalities. We are also seeking to develop a similar agreement with the RCMP based on that model.

Lastly, the department has been taking steps to ensure wider understanding and better use of SCISA. For example, in 2015, the director general for consular policy held a number of teleconferences, open to all heads of missions across the Global Affairs missions network, to discuss SCISA and other privacy and information sharing considerations in the consular context.

Now in terms of practice, since SCISA came into force, most of the department's sharing of consular-related information with national security agencies is done under SCISA rather than pre-existing authorities. In practical terms, there are two types of disclosure that are taking place.

The first type of disclosure is a result of a request from a national security agency. In these situations, the national security agency will send in a request in writing. These requests must provide sufficient detail to indicate a clear link to the agency's national security mandate. The requests also indicate the type of information that the agency is seeking. If the division targeted by the request, which is normally consular operations, determines that they have relevant information, they will gather the relevant information and seek legal advice regarding compliance with SCISA and Canada's privacy laws. Officials then exercise their discretion on whether or not to share the information.

The second type of disclosure is proactive disclosure. These arise when department officials—again typically with consular operations—collect information that they believe is relevant to the national security mandate of a Canadian department or agency. The same process for requests is followed as for proactive disclosures.

The decision to share is always taken at headquarters. Although we have left open the possibility of sharing directly at a mission where there is imminent risk to life or bodily harm, in practice this has not happened. The reason for the headquarter's decision is, first, to ensure that individuals with sufficient experience and level are ultimately making the decision following our established process; second, to ensure consistency in the interpretation and use of SCISA to disclose the information, including confirming that the threshold for disclosure has been met; and finally, to ensure documentation and tracking of disclosures to meet reporting and accountability requirements.

As you are likely aware, the Office of the Privacy Commissioner commenced an investigation of SCISA under section 37 of the Privacy Act last fall. Global Affairs has met with the OPC and has provided information on the number and nature of the disclosures we made under the act during the first year it has come into effect.

It is also worth noting that SCISA amended the Chemical Weapons Convention Implementation Act to permit Global Affairs Canada to share information pertaining to the production, processing, consumption, import, and export of certain chemicals and related facilities where appropriate. Before SCISA came into force, we were prohibited from sharing this information. This was an important change for the department.

To conclude, as I mentioned before, SCISA does not alter the department's existing authorities to collect national security information. However, before it came into force, we anticipated that it would create new possibilities for sharing information that is relevant to national security. I would say that SCISA provided an opportunity to refresh the discussion on how this type of information is shared. Also, practically speaking, it has created a context and a tool, both of which have focused efforts on ensuring that national security information is flowing appropriately yet responsibly.

Mr. Chair, that brings my remarks to an end. Some of your questions may require a detailed answer, for which I may not be the best person to answer, and therefore we have experts from different parts of the organization to respond.

Thank you very much.

● (1610)

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

Mr. Linder. We are pleased to have you here. You have up to 10 minutes please, sir.

[*Translation*]

Mr. Glen Linder (Director General, International and Intergovernmental Relations, Department of Citizenship and Immigration): Thank you, Mr. Chair.

My name is Glen Linder. I'm the director general of international and intergovernmental relations at Immigration, Refugees and Citizenship Canada, or IRCC. My branch is the policy lead for the implementation of the Security of Canada Information Sharing Act, or SCISA, within IRCC.

I'm accompanied today by Michael Olsen, chief privacy officer of IRCC.

Today, I'll be discussing how IRCC's mandate relates to national security, how SCISA was implemented within the department and how IRCC is using these new authorities.

Following my opening remarks, my colleague and I will be happy to answer any questions committee members may have on this topic.

[*English*]

IRCC is responsible for a diverse mandate, which includes facilitating the arrival of people and their integration into Canada while protecting the health, safety, and security of Canadians; managing the granting of Canadian citizenship; and issuing Canadian passports. Several of IRCC 's powers, duties, and functions relate directly to addressing activities that undermine the security of Canada. These include assessing the criminal and security admissibility of immigration, citizenship, and passport applicants.

One of the Immigration and Refugee Protection Act's objectives with respect to immigration is "to promote international justice and security by fostering respect for human rights and by denying access to Canadian territory to persons who are criminals or security risks".

In an effort to maintain the integrity of the immigration, citizenship, and passport programs, IRCC works closely with its security partners to identify applicants who are inadmissible to Canada on security grounds, to remove or revoke the status of those who engage in activities deemed to undermine Canada's national security, and to deny passport services to persons posing a threat to our national security. For example, IRCC ensures that individuals who are deemed inadmissible by engaging in terrorism, or instigating the subversion by force of any government, are not admitted to Canada. IRCC is also responsible for conducting revocations of citizenship if a person has obtained citizenship by false representation or fraud with respect to facts that may render persons inadmissible to Canada on grounds of security.

IRCC takes very seriously the operationalization of the new authorities granted by SCISA. The Department of Public Safety has developed a desk book and related resources that support government institutions in the implementation of SCISA to ensure its effective and responsible use. To complement this, IRCC has developed department-specific guidelines for employees authorized to disclose information under SCISA and receive information disclosed by other institutions under the act.

IRCC has developed a policy manual on how IRCC officials may work with SCISA. The manual provides information regarding topics such as disclosure and collection of information, directives on safekeeping, retention and record-keeping, and lists the limited IRCC positions that have been delegated for disclosure and receiving information under the act. Other tools, such as a step-by-step instructional document on the disclosure of information under SCISA, have also been made available to IRCC employees.

Given IRCC's responsibilities with regard to immigration, citizenship, and passport issuance, it is required to maintain a large volume of immigration records, and is a key institution for questions pertaining to the identity of newcomers and Canadians born here or abroad. Consequently, IRCC engages in reciprocal information-sharing with other government institutions to ensure the efficient use of government holdings while safeguarding the privacy rights of all individuals.

In the past, the absence of clear national security disclosure authorities made it cumbersome for partner agencies to support each other in countering threats to national security. SCISA has added a valuable tool to the information-sharing toolbox by allowing for the disclosure, sometimes proactive, of specific and targeted information to listed institutions. SCISA does not override any provisions found in existing legislation, such as the Privacy Act, but it does constitute a clear authority for efficient and expeditious information-sharing for national security purposes.

● (1615)

Since August 2015, IRCC has disclosed information in response to requests from security partners on 64 occasions, and in six instances has proactively disclosed information to partner agencies. IRCC has also been the recipient of information on one occasion, information that has been used in an investigation for revocation of citizenship under the Citizenship Act.

For illustrative purposes, I'd like to present you two possible scenarios for when information might be disclosed under SCISA.

First, in the context of an individual suspected of travelling abroad to engage in terrorism-related activity, IRCC may be the first institution aware of the potential return to Canada of this individual, as he or she may have to apply for travel documents to return to Canada. Under SCISA, IRCC has the authority to proactively inform institutions listed under the act to ensure that key partners are aware of the imminent return and are ready to respond to the potential threat to the national security of Canada. Prior to SCISA, there was no mechanism in place to promptly and proactively share such information.

Second, as a listed institution under SCISA, IRCC can also benefit from other federal institutions disclosing information to IRCC, which could support the department's mandate in relation to national security. A federal institution may come across information demonstrating that an individual who is a citizenship applicant has ties to terrorism, for example, through the financing of terrorist organizations. SCISA is an explicit authority for all federal government institutions to disclose information to designated recipients such as IRCC. Therefore, the institution could release to IRCC information related to the applicant's ties to terrorism, allowing the department to make an informed decision on the individual's citizenship grant. Before SCISA, it would have been difficult for an institution that had no specific information-sharing mechanism or authority related to national security in place to disclose such information to IRCC, and the individual may have received Canadian citizenship.

The authorities provided for in SCISA enable enhanced collaboration and better targeted information sharing through interactions among program experts of the listed institutions. The number of instances in which SCISA has been used is minimal compared to the volume of IRCC holdings, and it has been used in very specific situations.

Once again, we would like to thank you for inviting us to appear here today to discuss SCISA. We are happy to answer any questions from committee members about anything we have presented today.

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

We now move to Mr. Cossette from FINTRAC.

Go ahead, please, for up to 10 minutes.

Mr. Gérald Cossette (Director, Financial Transactions and Reports Analysis Centre of Canada): Thank you, Mr. Chair, for inviting Stéphane Cousineau and me, on behalf of FINTRAC, to speak with you regarding the committee's study of the Security of Canada Information Sharing Act.

I can assure you that we will be as forthcoming as we can with our answers today; however, I know you understand that we cannot provide classified information in this public venue. We are also limited by legislation in what we can say about specific information that FINTRAC holds.

I would like to take a few minutes to describe FINTRAC's mandate and the role we play in helping to protect Canadians and the integrity of the Canadian financial system, as well as the comprehensive measures we have adopted in our privacy framework to safeguard the personal information of Canadians. I will also focus on the centre's responsibilities under the Security of Canada Information Sharing Act.

● (1620)

[*Translation*]

FINTRAC was created in 2000 by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. As Canada's financial intelligence unit, FINTRAC facilitates the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control.

The legislation establishes obligations for financial services entities, real estate brokers, money services businesses, casinos and many other business sectors. These obligations require them to establish an internal compliance program; identify clients; monitor business relationships; keep certain records; and report specific types of financial transactions to FINTRAC, including suspicious transactions, international electronic funds transfers of $10,000 or more and large cash transactions of $10,000 or more.

As part of Canada's anti-money laundering and anti-terrorist financing regime, FINTRAC houses supervisory, compliance and intelligence functions. Our supervisory function involves assessing and enforcing the compliance of regulated businesses with their legal obligations. Our intelligence function enables us to produce financial intelligence for our police, law enforcement and national security partners.

As a result of the financial transaction reports received from regulated businesses across the country through its supervisory function, FINTRAC can provide financial intelligence that assists our partners in combatting money laundering, terrorism financing and threats to the security of Canada. FINTRAC also produces strategic intelligence about trends and typologies of money laundering and terrorist financing.

[*English*]

FINTRAC's role under the Security of Canada Information Sharing Act is limited, given that the provisions of FINTRAC's governing legislation set out narrow disclosure provisions and take precedence over any other legislative provisions related to the reception and communication of information. To be very clear, we can only receive information in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. As well, FINTRAC can only disclose information as specified under the same act to the appropriate police or national security agency when it has reasonable grounds to suspect that it would be relevant to investigating or prosecuting a money laundering or a terrorist activity financing offence, or that it would be relevant to threats to the security of Canada.

Section 5 of SCISA does not change in any way when, or to whom, FINTRAC discloses financial intelligence. The centre may only disclose financial intelligence when the legislated thresholds have been met, and only to recipients listed in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Given this, to date, FINTRAC has not received or collected any information under SCISA.

Before concluding, I would like to touch on the protection of personal information. FINTRAC's first priority is to safeguard the information it receives, including financial transaction reports under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Indeed, the obligation to do so is set expressly in FINTRAC's mandate. Clear principles for the protection of privacy are set out in its governing legislation, which respects both the Canadian Charter of Rights and Freedoms and the Privacy Act, and are reinforced by FINTRAC's own operational policies and security measures.

FINTRAC does not have access to the bank accounts of Canadians. It does not have any legal authority or the technical means to monitor the financial activities of individuals. It develops the financial intelligence that it discloses to its police, law enforcement, and national security partners exclusively from the information received from reporting entities and partners as specified under its legislation.

● (1625)

[*Translation*]

In addition, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act requires that the Office of the Privacy Commissioner conduct a review every two years of the measures FINTRAC takes to protect the information held. FINTRAC is the only government institution subject to this type of mandatory audit by the Office of the Privacy Commissioner.

The protection of Canadians' privacy is the key reason FINTRAC was created. We understand very clearly that, to maintain our credibility and the confidence of Canadians, we need to continually demonstrate that we take the protection of personal information and the limits of our mandate seriously. The protection of privacy is a clear priority for FINTRAC. We're determined to help protect Canada and Canadians, while meeting our obligations under the Privacy Act, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Security of Canada Information Sharing Act.

Thank you, Mr. Chair.

[*English*]

I would be more than happy to answer your questions.

The Chair: Thank you very much.

We'll go to our last presentation now. We move to the Canadian Nuclear Safety Commission.

Mr. Jamieson, you have up to ten minutes, please.

Mr. Terry Jamieson (Vice-President, Technical Support Branch, Canadian Nuclear Safety Commission): Good afternoon, Mr. Chairman and honourable members of the committee.

[*Translation*]

My name is Terry Jamieson and I'm the vice-president of the technical support branch at the Canadian Nuclear Safety Commission, or CNSC.

I'm joined today by Lisa Thiele, our senior general counsel.

Thank you for inviting us to discuss the CNSC's participation as a recipient institution under the Security of Canada Information Sharing Act.

[*English*]

Here's a little bit about the CNSC. The CNSC is Canada's nuclear regulator. Under the Nuclear Safety and Control Act, or NSCA, the CNSC carries out its threefold mandate.

First, we regulate the use of nuclear energy and materials to protect health, safety, security, and the environment. Second, we implement Canada's international commitments on the peaceful use of nuclear energy; and third, we disseminate objective scientific, technical, and regulatory information to the public.

We are an independent, quasi-judicial administrative tribunal. The CNSC regulates all things nuclear in Canada, including uranium mining, nuclear fuel fabrication, nuclear reactors and power plants, the production and use of medical isotopes, the decommissioning and remediation of nuclear sites, and the safe management of nuclear waste.

The CNSC was established in 2000 under the Nuclear Safety and Control Act and reports to Parliament through the minister of Natural Resources. The commission may have up to seven appointed permanent members whose decisions are supported by more than 800 employees. Our employees review applications for licences according to regulatory requirements. We make recommendations to the commission and we also enforce compliance with the Nuclear Safety and Control Act, regulations, and any licensed conditions imposed by our commission members.

The CNSC has two key responsibilities related to national security under the NSCA. First, the CNSC is responsible for preventing risk to national security by regulating the development, production, and use of nuclear energy, nuclear substances, prescribed equipment, and prescribed information.

The CNSC has one of the top nuclear security programs in place in the world. Our focus is on preventing sabotage of a nuclear facility or theft or loss of nuclear materials. We identify potential risks and threats to the Canadian nuclear industry and we develop the regulatory requirements necessary to ensure these risks are mitigated and that the threats are prevented, detected, or responded to appropriately.

In 2015, Canada welcomed a peer review mission from the International Atomic Energy Agency that concluded that Canada operates a mature, effective, and well-established nuclear security regime.

Our second area of responsibility related to national security is the implementation of Canada's obligations relating to the safeguarding and non-proliferation of nuclear materials. An example of how the CNSC works to prevent proliferation is through our licensing program, which controls the import and export of nuclear material, equipment, and information. This program requires information in order to assess applications and verify compliance with control measures.

The CNSC became a recipient organization under SCISA to ensure that we receive timely information about a nuclear-related activity that could potentially undermine the security of Canada. The frequency of such events is thankfully low, and I'd like to stress that to date, CNSC has not had to use SCISA. Under the act, the CNSC's authorities to receive information have not changed, but rather, other Government of Canada institutions are provided a better understanding of our mandate as a recipient institution and are given the authority to disclose relevant information to us.

● (1630)

[*Translation*]

As a recipient institution under SCISA, the CNSC considers the protection of national security information and the personal information handling provisions of the Privacy Act to be of the highest priority.

[*English*]

While we have existing processes in place, we are committed to continuous improvement and, as a result of the Privacy Commissioner's annual report, the CNSC is undertaking a privacy impact assessment that will capture SCISA. We're also working to clarify our procedures to ensure that they're well understood by all impacted areas of our organization.

This concludes my remarks, and I would be pleased to answer any questions that you might have.

Thank you.

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

We appreciate the fact that we've come in a little bit under time. That gives us a little bit of breathing room on our questions. We have an hour left, and the rounds of questioning are slated for about 50 minutes. Given my liberal tendencies to let members go over in their time, we should be able to get through at least one round, so we appreciate that.

We'll start with Mr. Erskine-Smith. We have four people on the seven-minute round.

Mr. Erskine-Smith, the floor is yours.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks, everyone, for your testimony.

Mr. Linder, I just want to confirm from your remarks if the 64 requests for information, and six proactive disclosures you've made, were all through SCISA.

Mr. Glen Linder: Yes. That's correct.

Mr. Nathaniel Erskine-Smith: Mr. Drake, do you have similar numbers with respect to Global Affairs?

Mr. David Drake: I'm going to ask my colleague Victoria Fuller to respond.

Ms. Victoria Fuller (Director, Case Management, Consular Operations, Department of Foreign Affairs, Trade and Development): Global Affairs Canada has received requests, which we responded to 25 times. We've made 20 responses in which we did not provide information for one reason or another, and we've made 16 proactive responses.

Mr. Nathaniel Erskine-Smith: In the 20 times you declined to share the information, did you determine they weren't relevant to the national security mandate?

Ms. Victoria Fuller: There would be three reasons to be in that category. One was a decision not to share the information. One was a decision that this was not the appropriate mechanism to share the information, and the information was shared in another way. The third reason was that we had no information that met what they were looking for.

Mr. Nathaniel Erskine-Smith: Mr. Drake and Mr. Linder, in the instances that information has been disclosed or received, was it because of SCISA? Would that information-sharing have been precluded by the other authorities to which you are subject, or have you turned to SCISA just because it's there? Is SCISA necessary to that information-sharing?

Mr. Glen Linder: In our case to answer your question directly, yes, in all cases the information could have been provided without SCISA, but SCISA essentially allows for a dedicated service channel for national security cases and for a much simpler approach for our being able to disclose that information.

In view of the timeliness often associated with national security cases, it facilitates that prompt information-sharing, provided all the tests within SCISA are met in that particular case.

● (1635)

Mr. Nathaniel Erskine-Smith: Could you expand on that? What in SCISA in particular would facilitate that information-sharing outside the authorities that pre-existed SCISA?

Mr. Glen Linder: With respect to our department, essentially outside of SCISA the authorities are in the Privacy Act. What do we have in the Privacy Act? We have the provision on consistent use. In our case we're collecting information to assess someone's admissibility to Canada, to assess their request for a passport or their application for citizenship.

The consistent use with respect to national security is somewhat limited in that case. We're essentially limited to being able to confirm the person's name and immigration status in Canada with respect to consistent use, so it doesn't provide much of an avenue.

The other area we can share information under the Privacy Act is when it's requested by an investigative body. There, absolutely, the information can be shared, but in that particular case, it's on request only. We can't proactively provide anything. It's also done as part of the other business under the Privacy Act, whereas under SCISA you again have this designated channel, you have these national security experts who are dealing with it, who are cleared to the appropriate level, and who have the expertise to be able to assess much more clearly and promptly what's provided.

Mr. Nathaniel Erskine-Smith: If I can jump in, I note from your remarks that SCISA provides a mechanism for proactive disclosure, and so it does provide a new authority to facilitate information-sharing.

We had Professors Roach and Forcese attend before us. They recommended that we adopt the Privacy Commissioner's recommendation to amend section 5 of SCISA to require that shared information be necessary or proportionate, and not simply relevant to the receiving institutions' security jurisdiction.

I wonder if you would agree, and if you wouldn't agree, why that would be a bad idea for your organizations.

Mr. Glen Linder: That's entirely in your hands, obviously, as our elected representatives.

Mr. Nathaniel Erskine-Smith: Maybe I'll put it a different way then to be fair, because I don't want to put you on the spot on a policy matter. In your view, given your operations and the number of times you have received and disclosed information, would that necessity standard get in the way of protecting national security?

I ask because we had CSIS before us. They are already subject to a strictly necessary test on receiving information, so perhaps you could give us some clarity on relevance versus necessity. Would necessity get in the way of you guys doing your jobs and sharing this information to protect national security?

Mr. Glen Linder: From my perspective on having a more stringent test, we take the test of relevancy very seriously. If there were to be a more stringent test in terms of necessity, for example, it would be helpful for you to consider what that would do in terms of balance. There has been a lot of discussion at this table about balance. If it were a test of necessity, we would need to be convinced with a lot more information that were necessary, in fact, not simply relevant. And what would that mean in practice? I think that would mean that our national security agencies, the investigative bodies that were requesting information from us, would possibly have to give us a lot more national security information for us to make that determination and be satisfied that it was, in fact, necessary and not simply relevant.

Could we do that? Absolutely, but it's worth considering whether the benefit of having that higher standard is outweighed by having more sensitive national security information in circulation, in order for us to make that determination. More generally—and I think this is possibly the intent—it obviously would put a chilling effect on the amount of information we would disclose under SCISA. That would be a necessary outcome.

The Chair: Thank you, Mr. Erskine-Smith.

We will now move to Mr. Jeneroux, please, for up to seven minutes.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, everybody, for being here today, and thank you for waiting for us to finish our votes.

Mr. Linder, I do just want to give you an opportunity to perhaps expand or clarify one of the comments you made with respect to your department. You said in your brief:

> IRCC is also responsible for conducting revocations of citizenship if a person has obtained citizenship by false representation or fraud with respect to facts which may render persons inadmissible to Canada on grounds of security.

I imagine that is no matter how naive or innocent the case may be. Would you mind expanding and perhaps clarifying some of those comments for us?

● (1640)

Mr. Glen Linder: With regard to citizenship revocation, essentially citizenship can be revoked if we have evidence that the person made a false or misleading statement, or committed fraud with respect to an element regarding admissibility. A ground for admissibility, for example, would be whether a person is a threat to the security of Canada. So if we later determined that there had been fraud, that the person had covered up membership in a terrorist organization at the time he or she applied for citizenship, we would be able to go through a process that would essentially allow us to revoke citizenship if we could determine fraud had been committed or misrepresentation with respect to what was told us at the time of application for citizenship.

Mr. Matt Jeneroux: Would something as simple as putting a different country as where they are from fall under that?

Mr. Glen Linder: No, not necessarily. It would have to be a grounds of inadmissibility that's listed under the act. It's usually regarding security, criminality, or public health, so a simple misrepresentation is not necessarily grounds for inadmissibility in itself.

Mr. Matt Jeneroux: That would certainly be concerning, I would think as a Canadian generally, but it's fair enough, if that's your department's position.

For the rest of the table, there is a very heated debate surrounding the creation of SCISA. Many were concerned that the new information-sharing powers provided to our intelligence organizations were too broad and were not sufficiently accompanied by appropriate oversight mechanisms.

Could we get everybody to comment? Since SCISA has come into force have you seen any abuse of the new information-sharing powers, or misuse of them?

We'll start with Mr. Drake and go in order of the speakers.

Mr. David Drake: Thank you.

The answer is no. We certainly have not seen any kind of misuse of this. I would also point out that, of course, as I made clear in my statement, we deal with these issues with great attention to detail according to the law and individual agreements we have set up with other organizations. The answer is clearly no.

Thank you.

Mr. Matt Jeneroux: To the second speaker, I forget who you are.

The Chair: It's Mr. Linder.

Mr. Glen Linder: I'm sorry. I'm going to ask you to quickly repeat the question.

Mr. Matt Jeneroux: That's all right. Since SCISA has come into force, have you seen an abuse of the new information-sharing powers or a misuse of them?

Mr. Glen Linder: No, we have not.

Mr. Gérald Cossette: It's the same thing with FINTRAC. We haven't received or disclosed anything under SCISA.

Mr. Terry Jamieson: For CNSC, likewise, we have not received or disclosed and we've seen no misuse.

Mr. Matt Jeneroux: Again, we'll go in the same order.

Do you think this legislation helps our national security organizations do their jobs more effectively?

Mr. David Drake: I think, from our perspective, there is no question that it helps. It provides an additional tool. As I mentioned, it provides a general context in which to address these things positively, so I think it definitely helps us in our day-to-day practice, although we do not use it for absolutely all instances.

Victoria, do you want to comment on that?

Ms. Victoria Fuller: My only comment is that one of the benefits is that it allows for greater coordination across government departments, because more departments have more relevant information available in order to make decisions.

Mr. Glen Linder: I would agree with my colleagues from Global Affairs. As I said before, we do see it as helpful. We do see it as creating this dedicated service channel for national security information to be discussed and exchanged among relevant experts who have the appropriate security classification.

● (1645)

Mr. Gérald Cossette: From our standpoint, the legislation hasn't had any impact on our operation, positive or negative.

Mr. Terry Jamieson: Again, there has been no impact on either our mandate or our operations. But in terms of commentary, we would view SCISA as being a very efficient, effective, and consistent framework to facilitate information sharing across a broad range of government entities.

Mr. Matt Jeneroux: Perfect.

Under the Five Eyes alliance, we see information-sharing models of other countries. I'm curious as to whether anybody around the table has any experience with what those information-sharing models might be, and whether perhaps there are benefits we could obtain here in Canada to use. Does anybody have any experience with the Five Eyes?

Mr. David Drake: Thank you. I think this probably would be best addressed to CSIS.

Under SCISA, we don't share with the Five Eyes. My own level of contact with the Five Eyes is not specific enough to really be able to honestly respond to your question.

Mr. Gérald Cossette: It may not pertain specifically to SCISA, but when it comes to FINTRAC, in fact, we were created to prevent law enforcement agencies from accessing directly the information of Canadians without a warrant or a production order.

If you compare us, for instance, to other organizations or colleagues abroad, lots of organizations do receive the information, structure it, and leave it in their database, and then the database is accessible to all law enforcement agencies of that country. We do not do that in Canada. Basically, our responsibility is to make sure that the information that is disclosed responds directly to the mandate that was given to us by Parliament, so from that standpoint our regime is much more rigorous than what you will see elsewhere.

The Chair: Your time is up.

We'll now move to Mr. Blaikie for seven minutes.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thank you very much.

I'm going to ask a question that is similar to my colleague's, but I think also different. I apologize if I am being repetitive.

I know we heard from Mr. Cossette and Mr. Jamieson that they haven't used SCISA. I'm wondering if Mr. Linder or Mr. Drake has received or disclosed information under SCISA, and, if so, how many disclosures or receipts have occurred under SCISA.

Mr. David Drake: With your permission, Mr. Chair, I'm going to ask my colleague Victoria Fuller, from the consular area, who is a specialist in this area, to respond. Thanks.

Ms. Victoria Fuller: Those would be the same numbers that I provided to Mr. Erskine-Smith. I'm not a set delegated recipient of information, so I couldn't address whether the department as a whole has ever received under SCISA.

Mr. Daniel Blaikie: Okay, so you're not sure.

The Chair: Mr. Linder.

Mr. Glen Linder: At IRCC, we have disclosed information on 70 occasions under SCISA. Sixty-four of those times it was as a result of a request to us, and six times we've disclosed it proactively. We have been the recipient of information on one occasion.

Mr. Daniel Blaikie: I'm curious to know from you, then, Mr. Linder, because you seem to be the only one here today with experience either receiving or disclosing information under SCISA, how is a disclosure or a receipt defined? Does that mean information on 70 individuals? How many people could be captured by any one disclosure or receipt of information under SCISA?

Mr. Glen Linder: In each case, the request for disclosure tends to be very specific to a particular situation. To my knowledge, it is usually associated with a single individual. I think it's possible that it could be a family as well, but in general, it is extremely limited. Within that data set, we take extreme care to make sure that we're only providing those information fields that are absolutely necessary for the objective of the act to be carried out.

● (1650)

Mr. Daniel Blaikie: Are there any explicit guidelines somewhere for how to report on those disclosures, and what would count as one disclosure? Or, is it the case that if you were to get a request from CSIS asking for information on a category of persons and you were to make that disclosure, that would count as one instance of disclosure, even though it may cover 100 people, 150 people, or 1,000 people? Are there any explicit guidelines saying say what should count as one instance, as opposed to many, when you're reporting on these disclosures?

Mr. Glen Linder: I can't answer that specifically. I can tell you that in my experience and to my knowledge, we've only had situations that have been on that one-off basis, and we look at each one very carefully in each case. Within the department, we have put together a very detailed desk book for anyone who deals with SCISA. It lays out the rules very carefully. There is a detailed checklist that a delegated official needs to go through each time to make sure that everything is done in accordance with the act. Each delegated official also undergoes training, which we provide internally in the department, to make sure that the parameters of the act are respected.

Mr. Daniel Blaikie: If it is the case that your officials are already working with written and explicit guidelines for how to perform disclosures or receive information under SCISA, do you think there would be any operational consequence for trying to put some of those guidelines into law so that those ways of disclosing or receiving information under SCISA apply fairly across departments, so that Canadians have some confidence?

That's not to impugn any of the organizations that are here today, but it's a fact that part of being able to live safely and securely also means having confidence that, when information is shared, it's done properly. Canadians don't typically have access to internal policies and guidelines, and they want to know that if those are breached, there will be consequences. We have seen instances where government sometimes doesn't follow its own policy, whether it's a Treasury Board policy or otherwise, and there aren't consequences for that as a result. With respect to these kinds of issues, Canadians would like to know that if there is a breach of those guidelines, there will be consequences.

If it's a matter of writing a better law to make legal, or write into law, some of those guidelines, do you foresee negative operational impacts on your organization?

Mr. Glen Linder: It's difficult for me to answer that. To a great extent, we're in your hands. A lot of legislation, particularly legislation around information sharing, is accompanied by directives, policy documents, and so on for their implementation. The balance between what you put in the legislation versus what you put in regulations or directives and policy documents varies on a case-by-case basis. Where those rules are located, from my perspective, is less important than the fact that the rules need to be followed to ensure that we get that right balance between protecting privacy and protecting Canada's national security.

Mr. Daniel Blaikie: That's definitely one of the themes that has been coming up in this whole study. How do you get Canadians' confidence that their personal information is not being shared recklessly?

We've heard from the departments that they have their own internal controls and mechanisms, but we've also heard from a number of experts who say that, as far as the law is concerned, this is a pretty broad and sweeping power that has been conferred on your organization.

We saw today in the news that the RCMP has been monitoring protests, or people demonstrating in favour of an inquiry into missing and murdered indigenous women. When Canadians learn about those kinds of things, it undermines their confidence and trust in our governmental institutions. Then, when they see a law as broad and sweeping as SCISA, they say, “Okay, if we can't trust them not to be checking up on people who are just concerned about the plight of indigenous women in Canada, why would we want to let them share so broadly, and though they say they have appropriate internal controls, why should we trust that those are adequate and being followed?”

If you look at SCISA in that light, what kinds of changes do you think could be made to SCISA to give Canadians the confidence that there is someone looking over your shoulder and observing that you're doing things as you say, while retaining the operational flexibility that you need to be able to make use of the information you receive to fulfill your function to ensure that important information about threats to Canada and Canadians is being communicated in a timely fashion? I open that up to anyone here.

● (1655)

The Chair: Regrettably, the Chair has to acknowledge that we're already eight minutes into Mr. Blaikie's seven minutes. That was a very long question.

Mr. Daniel Blaikie: Is that your way of saying you're not that liberal?

Some hon. members: Oh, oh!

The Chair: That is a correct assumption, but if there's a quick and efficient response, I will entertain it.

Mr. David Drake: I don't have a quick response, Mr. Chair.

The Chair: Thank you. We'll move on then.

Daniel, you do have three minutes coming up, so maybe we can get your answer then.

Mr. Saini, you have seven minutes, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon everyone. I thank you so much for coming.

I want to change the conversation a little bit to international sharing agreements. The reason I want to bring this topic up is the executive order that was issued last week in the United States. I will just read you a part of it:

> Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

I am sure that a lot of you probably share information with the United States because our two nations are intertwined with various instruments, treaties, and agreements. This executive order is about one week old. Has it affected your ability in any way to exchange information with the United States?

Ms. Lisa Thiele (Senior General Counsel and Director, Canadian Nuclear Safety Commission): From the perspective of Canada's nuclear regulator, we do have statutory authority to enter into information-sharing arrangements with other regulators in other countries. We have several of those. The type of information that we share is regulatory information; it's never going to be personal information.

Some of the information has to be adequately protected with classifications, but that's usually to protect commercial interest. It's not about personal information. Our information sharing is unaffected, I would say.

Mr. Glen Linder: For IRCC, I can't comment specifically on that particular situation, but I can say that we are looking into all the elements of all three executive orders that have been issued so far to determine the impacts, if any, and are working with our U.S. counterparts. This is one that we would look at.

Mr. Raj Saini: The executive order is pretty clear that it applies to non-United States citizens or lawful permanent residents. Have you stopped sharing information, or is information still ongoing? What protection is there for Canadian information that is currently being shared?

Mr. Glen Linder: I'm sorry. I don't have that information with me today.

Mr. David Drake: On the Global Affairs Canada side, under SCISA we only share information very, very carefully, as I pointed out, with Canadian government entities. It's not the role of our ministry to share information of a personal nature with other governments, so it doesn't apply to our ministry. Thank you.

Mr. Gérald Cossette: As we mentioned before, we do not exchange information internally, and surely not externally under SCISA, but under our mandate we have signed 92 MOUs with different countries of the world. The MOUs are quite specific as to the kind of privacy protection we're asking for from the countries with whom we've signed those MOUs.

We ask those countries to be members of the Egmont Group, a group of 146 countries with exactly the same responsibilities—well, not 146 countries, but 146 FIUs, or financial intelligence units, because they do not represent their national governments—to have the same framework as we do. Also, we have the authority to disclose or not and can decide what we are willing to disclose.

When it comes to FINTRAC, it is always the same issue. It has to relate to money laundering, terrorism financing, or the national security of Canada. If the country that requests the information is not specific enough, we don't have to provide anything. We may also provide information proactively. Most of the requests we receive are fairly specific and relate, as I said, to money laundering, and in our exchanges with the Americans, a significant number of exchanges on terrorism financing also.

● (1700)

Mr. Raj Saini: The second question I have is whether sometimes you could possibly receive the information from your departments inappropriately or maybe in error. Can you explain to the committee what mechanism you have to dispose of that information? How long do you keep it for? Is there some oversight? When do you dispose of it? How do you make that decision?

Mr. Glen Linder: For IRCC, if we receive information in error or information that's not relevant, the guidelines we have within the department are that the information must be destroyed immediately.

Mr. David Drake: On our side, SCISA is not a collection authority. I'm just looking to my colleagues, Victoria or perhaps Patrick, on the privacy side, because it's a very specialized question.

Mr. Patrick Picard (Director, Access to Information and Privacy, Department of Foreign Affairs, Trade and Development): On the privacy side, for information that's collected legitimately, I believe the standard is a minimum of two years. If the information is not collected for the purpose intended, then I would suspect we wouldn't keep it as long.

The Chair: That's it, Mr. Saini.

Colleagues, we'll now move to the five-minute round. That will start with Mr. Kelly.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you.

Perhaps I'll begin with Ms. Fuller. Despite the "minimal" use—which is maybe not the right word—SCISA is a new law. Many of the institutions that we've heard from, including today, have not used SCISA or its authorities to exchange information, though your department has. It sounded to me like you used SCISA on at least half a dozen occasions or so to share information. In your opening remarks, I think you had characterized it as a useful instrument on at least those occasions. Could you expand on that a bit? I don't know if there's a way for you to describe what the nature of some of those individual cases might have been where SCISA was used. Perhaps the ability to share would not have existed in the absence of SCISA.

The Chair: Go ahead, Mr. Linder.

Mr. Glen Linder: Thank you.

With respect to the information we have shared under SCISA, what I can do is perhaps give you some illustrative examples of the kinds of information that we might disclose. For example, if there's a national security investigation under way by one of our national security organizations, say the RCMP, we might disclose to them personal information to confirm the identity of someone who's suspected of planning or performing an act that would undermine the security of Canada. That would assist them in making a positive identification of the person and be able to take appropriate law enforcement action. That might be one example in terms of our disclosing to another organization.

In terms of a proactive disclosure that we might do under SCISA, an example might be an individual who is suspected of travelling abroad to engage in a terrorism-related activity and who has just acquired a Canadian passport to return to Canada. There again, proactively providing that information to our national security agencies could help them in terms of making sure that appropriate enforcement action is taken when that person returns to Canada.

Another example might be information disclosed to us by a security organization. As I mentioned in my opening remarks, we're responsible for determining admissibility of people into Canada, so if an organization has information that a person is a threat to Canada's national security, that is very helpful to us in terms of determining that they're inadmissible to Canada and we should not issue a visa to them to facilitate their entry into Canada.

Those are some illustrative examples of where SCISA can be used in our context.

● (1705)

Mr. Pat Kelly: And has it been used?

Mr. Glen Linder: I wouldn't want to comment on any specific case, but those are some potential uses.

Mr. Pat Kelly: Is the threshold of undermining the security of Canada appropriate, do you think, for your department and your use of information?

Mr. Glen Linder: I guess what I can say about the threshold of undermining the security of Canada is that it's working for us. I would say a more stringent threshold would have a chilling effect in terms of the amount of information we would disclose or that others would disclose to us. I think that would be normal, but we're in your hands on that.

At present I can say that we have made, as I said, a total of 70 disclosures by our department, which has a considerable amount of personal information on Canadian citizens, permanent residents, and foreign nationals. It's not a lot of times that we've used it, but when we have used it, I think it has been helpful and effective.

Mr. Pat Kelly: You mentioned that the effect of raising the bar, if you were to adopt the necessity test and move to a higher bar, would have a chilling effect. Would it affect your organizational culture, the people on the ground in your organization with a desire to share or perhaps make them more concerned about whether they have met the bar rather than trusting their instincts on a particular file?

Mr. Glen Linder: No, I wouldn't say it would affect the culture in that way, but I think, as we do currently, that we would take that new threshold very seriously. If you do have a higher threshold, I think it's fair to assume that you would have fewer cases of disclosures simply because there wouldn't be the same number that would meet that more stringent threshold.

Mr. Pat Kelly: I'm pretty sure I'm out of time.

The Chair: You are, Mr. Kelly.

[*Translation*]

Mr. Massé, you have five minutes.

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Thank you, Mr. Chair.

Thank you everyone for being here to speak to our committee. Given the number of witnesses here today, I think there's a clear interest in our study.

My first question is for you, Mr. Drake.

Mr. Drake, you mentioned earlier that SCISA makes you more coordinated and effective when sharing information, for example. I'm asking this question because 17 organizations are included in the schedule to SCISA. However, at every committee meeting, I discover a new entity that falls under a department. For example, I learned today that Global Affairs Canada now has an entity called the counter-terrorism, crime and intelligence bureau.

Explain to me how it's more effective. How does SCISA make you more effective and coordinated when sharing information?

Mr. David Drake: Okay. Thank you for the question.

With all due respect, I don't want to avoid your question. I want to respond as clearly as possible. I think we were misunderstood earlier. I have someone with me who is really an expert and who handles this type of communication every day. She could be called on to do so on the consular side. I'll ask Victoria Fuller to give you an accurate response that describes our perspective in greater detail.

Thank you.

● (1710)

Ms. Victoria Fuller: I'll respond in English.

[*English*]

For us, the better coordination comes from the fact that, under SCISA, once we realize that the information is relevant and necessary and meets the national security test, we're able to take a 24/7 decision to share that information. In the world that we work in, many of our cases are in Asia or the Middle East where the hours of work are quite different; and to go through the previous exercise, which was using paragraph 8(2)(m) of the Privacy Act regarding a public interest in disclosure, required us to get authority from the head of the organization who has the delegation to do that. It's a much more bureaucratic process; it takes longer for the information to flow. As a result, at the moment of a terrorist attack abroad, for example, or in the initial stages of the detention of a Canadian citizen abroad, key things would not necessarily be able to move as quickly, and as you're likely aware, the first 72 hours of detention are the most critical for us. For us, in cases where we have a Canadian citizen detained on national security grounds, we would like to notify our partner departments immediately, where the test was met, because that ensures, first, that any relevant information they have would be given to us, and, second, that our consular officials are going first in taking the lead and providing services to the Canadian citizen now that he or she has been detained overseas.

Mr. Rémi Massé: Based on your answer, does that mean that you are in fact collecting information on Canadians?

Ms. Victoria Fuller: In regard to the term “collection”, I don't collect information, but I have proactively disclosed information under SCISA; and we have received requests under SCISA that we have responded to.

Mr. Rémi Massé: Let me understand, because Mr. Drake, in his testimony, said that departmental officials collect information that they believe is relevant to the national security mandate.

Ms. Victoria Fuller: The distinction is that our organization is one of the 17 listed entities. Within that, they have subdelegated certain parts of the department that can receive that information. Mr. Drake's part of the department is one of those areas. In consular operations, we are not one of those areas.

Mr. Rémi Massé: Just so I understand, do you collect or do you not collect information?

Ms. Victoria Fuller: Consular operations does not, but other parts of our organization would have the ability to receive the information that was disclosed.

Mr. David Drake: To receive the information, that's right. We're not a collector ourselves. That would be CSIS or others. Of course, what we're talking about here is not collection per se, but in the case of consular operations, they have a database based on their engagement with Canadians who require assistance. It's that database that is accessed in the case.

Perhaps you'd like to explain a bit more so we can clarify this.

Ms. Victoria Fuller: The consular database is information received from Canadian citizens who have sought consular assistance abroad. That database is restricted to the consular program only within Global Affairs. So, any information in that database is covered under the Privacy Act. To access information that I would hold would require a request under one of the authorities from another government department before we would take a decision on whether that threshold was met and what would be shared.

Mr. David Drake: Just to be absolutely clear, while my title includes “intelligence”, this is really as a result of the requirement to make sure that my group is connecting with the intelligence agencies. We are not an intelligence agency ourselves. The term is perhaps a bit open to a misunderstanding, but it's other organizations that do that, not us. We act as an interface.

Thank you.

The Chair: Thank you, Mr. Massé. We're already at six minutes.

We'll have Mr. Kelly again for five minutes, please.

Mr. Pat Kelly: Thank you. I'm going to continue right where my colleague left off and perhaps allow Ms. Fuller to continue with this.

I want to make sure I understood you correctly. The pre-existing authorities for information sharing did not move quickly enough to maximize your ability, or to have the ability, to quickly assist, for example, a Canadian detained abroad. When time is a critical factor in being able either to assist a Canadian or to prevent a crime from being committed, SCISA allows for greater efficiency and, perhaps, professionalism in the dealing and exchange of information because it is a single act for 17 agencies. Is that a fair characterization of your response?

● (1715)

Ms. Victoria Fuller: Previously, there was an ability to share information. The challenge was that while consular works 24/7, and we have a 24/7 watch and response centre and are accessible at all hours of the day, other departments, especially officials in the privacy area who would have to sign off on disclosures, do not work on that same cycle. To track them down and to disclose lawfully and properly with the advance authority was much more of a bureaucratic hurdle for us.

The introduction of SCISA has allowed the decision to be taken at headquarters very quickly based on the ability to call on people who know they could be called in the middle of the night to make a quick decision, and to get all the information, including the legal opinion, and whatever's required. It has provided a mechanism with our partner departments so they can access that information in a secure way.

Mr. Pat Kelly: Okay, thank you.

Since we have different departments here today, maybe I'll go to a question that will allow each department to address some of the criticisms of SCISA that we have heard from past witnesses. We've had other witnesses who have characterized SCISA as a calculated piece of legislation designed to enable government agencies to collect and exchange bulk data on a massive scale, both between departments in Canada and with foreign governments.

I'll perhaps let each department representative here quickly comment on that characterization that other critics have made.

Mr. Terry Jamieson: Well, I'd like to stress that the CNSC does not collect personal information in the context of security, so we would not say that that's the case.

Mr. Pat Kelly: Okay.

Mr. Glen Linder: In terms of IRCC, SCISA contains no new authorities with respect to collection. When we do obtain information from applicants who are seeking benefits under our existing legislative authorities—be it the Immigration and Refugee Protection Act or the Citizenship Act—disclosure of that information, as I mentioned before, is done on a case-by-case basis. Again, SCISA only permits disclosure to the 16 other listed agencies.

Mr. Pat Kelly: So nuanced and targeted collection in sharing is what you would make use of under SCISA, not the bulk sharing of large pools of data?

Mr. Glen Linder: I'm not even aware of there being an ability to share bulk data under SCISA.

Mr. Pat Kelly: I raise it because it has been discussed by the witnesses.

Mr. Drake.

Mr. David Drake: I know you've had previous discussions about this with relevant parts of our organization. Certainly, from my department's perspective, it's simply not an issue. We don't deal with bulk data, and we certainly don't share it. We don't share any information under SCISA outside of the federal government.

I think, from my reading of the previous testimony, others have answered your query.

Mr. Pat Kelly: Thank you.

Mr. Cossette.

Mr. Gérald Cossette: From the different business sectors, we only receive information that is designated under the legislation. It may be semantics to people, but we do not collect information; we receive information. We have no authority to go back to a financial institution and ask. So what we receive is what we have.

The Chair: We're at five minutes now, Mr. Kelly.

[*Translation*]

Mr. Dubourg, you have five minutes.

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

I want to say hello to the witnesses. There are many of you here to answer our questions. Thank you for being here.

My next question concerns the Financial Transactions and Reports Analysis Centre of Canada. It's for Mr. Cossette.

You presented your brief. It concerned FINTRAC's mandate and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. You said that, since the legislation's implementation, you haven't proceeded with any information sharing.

Under these conditions, I want to know why it's necessary to be one of the 17 institutions included in the legislation, in terms of information sharing.

● (1720)

Mr. Gérald Cossette: The legislation itself doesn't change our ability to receive or share information. However, it gives other departments that didn't have the authority to share information with us the ability to do so now.

Mr. Emmanuel Dubourg: Okay.

Mr. Gérald Cossette: As a result, the institutions and citizens that communicate with us under these circumstances would have more authority than certain departments in possession of relevant information.

Mr. Emmanuel Dubourg: In other words, if you have information regarding terrorism, for example, you have the authority to share it with others.

Mr. Gérald Cossette: We had the authority before, but we could share the information only with the institutions mentioned in the legislation, meaning our own legislation and not the legislation on information sharing.

Mr. Emmanuel Dubourg: I imagine that the Canada Revenue Agency is likely one of the agencies you deal with the most.

Mr. Gérald Cossette: No. The RCMP and law enforcement in major Canadian cities receive the most information from our agency. We communicated 204 times with the Canada Revenue Agency last year. However, to communicate with the Canada Revenue Agency, we first need to establish that money laundering then tax evasion occurred. Two thresholds must be reached in the Canada Revenue Agency's case.

Mr. Emmanuel Dubourg: Okay.

I know that FINTRAC closely monitors electronic funds transfers of over $10,000.

Mr. Gérald Cossette: Yes.

Mr. Emmanuel Dubourg: The data is very relevant for the Canada Revenue Agency.

Mr. Gérald Cossette: Yes. However, as I was saying, we ourselves need to establish that the threshold has been reached before the information is shared.

Mr. Emmanuel Dubourg: Thank you.

Given that the time is passing very quickly, I'll ask Mr. Linder a question on immigration.

On page 5 of your presentation, you said that you disclosed information on 64 occasions in one context and on six occasions in another context. However, at the end of the paragraph, you said the following:

> IRCC has also been the recipient of information on one (1) occasion, information which has been used in an investigation for revocation of citizenship under the Citizenship Act.

The Security of Canada Information Sharing Act refers to national security. Is the information you receive used for this specific purpose, or have you used it for citizenship revocation even though that wasn't the main goal?

[*English*]

Mr. Glen Linder: In order to do a revocation of citizenship, one of the aspects is whether the person meets the grounds for admissibility. As I mentioned before, citizenship can be revoked if a person has obtained the citizenship by false representation or fraud with respect to issues that could render a person inadmissible to Canada on grounds of security.

I fully admit that it's a bit of a complex formulation and the test in the act is a bit complex, but essentially what it means is that if there is fraud with respect to what the person said at the time they applied for citizenship, then, absolutely.... In this case, that fraud related to the grounds of admissibility, specifically to national security. The information that we were proactively given by another agency was to do with national security, was legitimately received under SCISA, and was helpful to our being able to make a determination as to whether or not to revoke citizenship in that case.

● (1725)

[*Translation*]

Mr. Emmanuel Dubourg: So, you conducted the test for security purposes to reach this finding. It was a national security issue.

[*English*]

Mr. Glen Linder: That's correct.

The Chair: Okay, thank you, Mr. Dubourg. We're at five minutes.

We'll now go to Mr. Blaikie. Do you want an answer to the previous question you asked, or are you going to...?

Mr. Daniel Blaikie: I was going to look for that, but I just thought maybe I'd try not to use up all the time. But I think it's important because the nature of the question that I asked earlier about trust and what we can do to engender the trust of Canadians in these processes is, I think, if not at odds, certainly taking a different tack from some of my Conservative colleagues, who are asking if this is a good tool. There are lots of things that would be good tools for law enforcement but don't adequately respect the rights of Canadians and don't give Canadians an adequate amount of confidence in their security officials. Charter issues notwithstanding, warrantless search and seizure I am sure would be a great tool for law enforcement, but it's not therefore acceptable.

How do you think we could recommend either that we change SCISA or scrap it and come up with something else that would give you that operational flexibility but pay adequate attention? I know that you guys are concerned with these questions and you have your internal guidelines. Canadians are not part of that conversation. They want to make sure that the guidelines you're following are actually enforceable by a third party. How can we get that into the law without creating so many hurdles to the sharing of information that something bad may happen that ought not to have happened and need not have happened?

The Chair: We can start on the left and go across the table.

Mr. Terry Jamieson: To begin with, I think it would be important for the committee members to understand from the various agencies here today just what mechanisms they already have in place to ensure that there's proper use of the information. Certainly from the CNSC that test starts with relevance. We would only receive information if it were relevant to the continued assurance of nuclear security in Canada. We have internal mechanisms to oversee this. We have our audit and ethics group. We have our departmental audit committee. Where appropriate, we could use our independent commission tribunal—

Mr. Daniel Blaikie: I just want to ask about that. At what point is there any kind of external oversight? At what point does someone come in and say, “Given your own internal guidelines, are you following those adequately?” Who is that person, or what is that body, and when is that kind of external review triggered? Is there anything regular?

Mr. Terry Jamieson: For external oversight, perhaps all I can offer is that all decisions of the commission can be reviewed by the Federal Court, so ultimately there is that outlet.

Mr. Glen Linder: No, I don't have much to add on that point. I hear what you're saying. I think that the review you're doing, the review that's being done internally within the 17 departments we're collaborating with as part of that review.... Ultimately, if there are improvements that we can make to the legislation, and there is a necessity to change the balance along the lines you describe, I don't have any concerns with that. But I do think it is important both to have the confidence of Canadians about their private information and to ensure that we are meeting the expectations of Canadians as well in ensuring that national security information is shared at the appropriate time with the appropriate people.

Mr. David Drake: Drawing on what's already been said, I don't want to repeat it, but certainly I think on our side we've done a lot to try to increase the robustness of what we're trying to do. We negotiated a specific agreement with CSIS. We've tried to communicate with our posts abroad to make sure everyone is plugged in and that we know what to do. There are very specific issues that we've tried to address. Certainly I think using that kind of experience and working.... For example, what we agreed and are trying to do with the RCMP and so forth are the sorts of things that eventually can be fed into that process, and we're making them available to you as much as we can.

I do think that not entirely correct that we're not subject to oversight. For example, when we share with CSIS, it has an oversight body. That oversight body certainly does not deal formally with us, but functionally it does because it deals with everything that CSIS deals with, and likewise with the RCMP.

So, those are a couple of points to respond to your question. Thank you.

● (1730)

Mr. Daniel Blaikie: Thank you.

Mr. Gérald Cossette: The Privacy Commissioner basically conducts an assessment of our privacy framework every second year. So far he has conducted two audits, and he is in the process, in fact, of finalizing his third one. On every occasion his conclusion has been that we never disclose information for purposes other than those provided for under the legislation. Therefore, I'm quite confident that this mechanism works well.

There are other things in our framework. People have access on a need-to-know basis and that kind of thing. So internally there are a series, if you wish, of mechanisms that ensure that the information is properly protected.

But as a third party, the OPC does that on a two-year basis.

The Chair: You got five and a half minutes out of your three-minute round, Mr. Blaikie, so you did well.

Mr. Daniel Blaikie: You're Liberal after all.

The Chair: If the committee will indulge me quickly for one second, I would like some clarification regarding a few things that arose. Witnesses have alleged that there is the potential for a breach of Canadians' privacy.

I'm just looking for a “yes” or “no” answer. Since its implementation, for those of you who have used SCISA, has there been any breach of Canadians' private information?

Mr. Linder or Mr. Drake.

Mr. Glen Linder: At IRCC, there has not been.

The Chair: Mr. Drake.

Mr. David Drake: At Global Affairs—and I'm checking with both of my colleagues here—there has not been.

The Chair: Thank you very much.

I have one last quick question for you, Mr. Linder, if you'll humour me. In recent days a report was tabled in the House of Commons indicating that 310 foreign visas were rejected, seven due to terrorism-related activity, nine for espionage or subversion, 13 for subversion by force, 79 for people being members of terrorist organizations, 26 for posing a danger or threat to Canada, and 48 for war crimes convictions. As well, 1.4 million were rejected due to false information on the applications.

Are you aware of this report, sir?

Mr. Glen Linder: I'm not personally aware of it.

The Chair: That's unfortunate, because a lot of those numbers match some of the sharing of information numbers you provided to this committee, and I would like to be able to draw some inferences there. If you could take a look at that report, please, Mr. Linder, and respond to the committee on my behalf, I would appreciate that.

Colleagues, we're out of time.

I'd like to thank our witnesses for their assistance in helping us with our deliberations, and I know we'll be issuing a report very soon.

Thank you very much.

The meeting is adjourned.