HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

43rd PARLIAMENT, 2nd SESSION

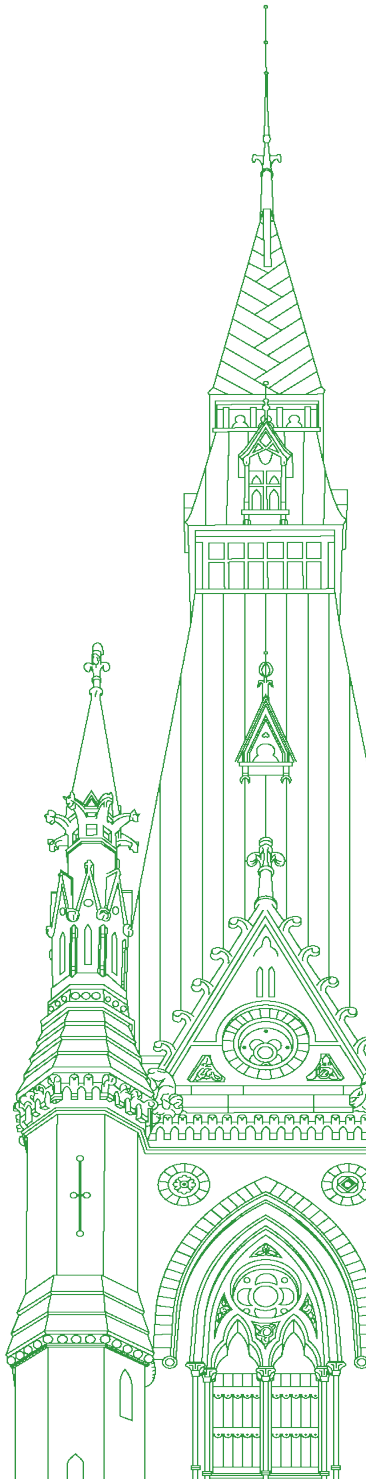
Standing Committee on Government Operations and Estimates

EVIDENCE

NUMBER 033

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Monday, May 31, 2021



Chair: Mr. Robert Kitchen

Standing Committee on Government Operations and Estimates

Monday, May 31, 2021

● (1535)

[*English*]

The Chair (Mr. Robert Kitchen (Souris—Moose Mountain, CPC)): I call this meeting to order.

Welcome to meeting number 33 of the House of Commons Standing Committee on Government Operations and Estimates. The committee is meeting today from 3:36 until 5:36. We will hear from witnesses as part of the committee's study of the government's response to the COVID-19 pandemic. Then we will go in camera to discuss committee business and consider our report on the Nuctech security equipment contract.

I'll take this opportunity to remind all participants at this meeting that screenshots or taking photos of your screen are not permitted. To ensure an orderly meeting, I will outline a few rules to follow. Interpretation of the video conference will work very much like in a regular committee meeting. You have the choice at the bottom of your screen of floor, English or French. Before speaking, please wait until I recognize you by name. When you are ready to speak, you can click on the microphone icon to activate your mike. When you are not speaking, your mike should be on mute. To raise a point of order during the meeting, committee members should ensure their microphone is unmuted and say “point of order” to get the chair's attention.

The clerk and the analysts are participating in the meeting virtually today. If you need to speak with them during the meeting, please email them through the committee email address. The clerk can also be reached on his mobile phone.

For those people who are participating in the committee room, please note that masks are required unless seated or when physical distancing is not possible.

I will now invite the witnesses to make their opening statements.

We will start with Mr. Scott Jones from the Communications Security Establishment.

Mr. Scott Jones (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Good afternoon, Mr. Chair and committee members.

My name is Scott Jones and I am the head of the Canadian Centre for Cyber Security at the Communications Security Establishment, or CSE.

CSE, reporting to the Minister of National Defence, is one of Canada's key security and intelligence agencies, with a mandate to provide foreign intelligence against a broad range of government priorities. CSE is also the country's lead technical authority for cybersecurity. The Canadian Centre for Cyber Security is a branch within CSE. In our national role, we defend the Government of Canada, share best practices to prevent compromises, manage and coordinate incidents of importance, and work to secure a digital Canada.

I appeared before your committee last May at the beginning of the COVID-19 pandemic, and I would like to provide an update on how the cyber-threat environment has evolved and on the work we have done since then to protect, from all types of cyber-threats, the Government of Canada, the health care sector, Canada's broader critical infrastructure and Canadians.

The COVID-19 pandemic has created an uncertain environment that is vulnerable to exploitation. CSE continues to leverage all aspects of its mandate to help ensure that Canada is protected against cyber-threats and to inform the Government of Canada's decisions. CSE and the cyber centre are continuing to work in coordination with industry partners so that malicious cyber-actors and fraudulent sites are less able to take advantage of Canadians.

Since March 2020, the cyber centre's work has contributed to the removal of over 8,000 fraudulent sites or email addresses, including websites impersonating the Government of Canada and impersonating COVID-19 vaccine booking portals. While this important work has been primarily focused on COVID-19-related fraud, this work continues every day as we identify and remove more fraudulent domains impersonating the Government of Canada or organizations involved in COVID-19 support efforts.

The cyber centre has assessed that the COVID-19 pandemic presents an elevated level of risk to the cybersecurity of Canadian health organizations involved in the national response to the COVID-19 pandemic. Throughout the pandemic, CSE and the cyber centre have continued to raise public awareness of cyber-threats to Canadian health organizations by proactively issuing cyber-threat alerts and providing tailored advice and guidance to all provincial, territorial and regional health authorities. federally funded associations and centres of excellence, patient care facilities, biopharmaceutical companies and research entities, medical device manufacturers, and academic research institutions.

Since the beginning of the pandemic, the cyber centre has hosted over 40 health sector community calls that provide timely updates to the health sector on the evolving cyber-threat landscape. Each one of them is tailored to the health sector. We have grown the health community, which we support, from a handful of organizations pre-pandemic to over 150 key health sector entities, and work with the IT security leads from these entities on a regular basis. The cyber centre, in close collaboration with our colleagues at Public Safety Canada, has facilitated cybersecurity posture assessments for many of these entities in the health sector, assisting them with determining their cybersecurity gaps and working with them to improve their cyber-posture and cyber-resilience.

The cyber centre has been focused on supporting COVID-19 vaccine research and development entities across Canada. We are working with a number of specific vaccine support organizations to offer services, such as protected DNS, that will strengthen their cyber-defence capabilities and dramatically reduce their vulnerabilities to cyber-attacks.

To protect and defend the vaccine rollout efforts, the cyber centre continues to work with the federal task force, the vaccine supply chain and the regional health authorities across Canada to raise awareness on cybersecurity, enforce and increase readiness for incident response and inform organizations when looming threats arise. We continue to reinforce perimeter security and access control to safeguard the vaccine ordering, tracking and data repository that is currently being developed by the federal health authorities. Also, to protect critical infrastructure, CSE and the cyber centre continue to regularly monitor and proactively share threat information with Canadian organizations, government partners and industry stakeholders.

Finally, the pandemic has made all of us more reliant on digital infrastructure. It is critical now more than ever that Canadians have access to the right information on how they can protect themselves online.

The cyber centre has created a collection of advice and guidance products available to inform Canadians about how to stay safe online. I encourage Canadians who are looking for easy-to-follow tips on cybersecurity to visit our website, getcybersafe.gc.ca. For businesses and larger organizations, or if you would like to read more of the publications of the cyber centre, they can be found at cyber.gc.ca.

CSE is constantly working to help address foreign threats and cyber-threats facing Canada in the health sector. We will continue to do so during the current pandemic and well after it's over.

Thank you, Mr. Chair.

● (1540)

The Chair: Thank you, Mr. Jones.

Now we'll hear from Shared Services Canada.

Mr. Sony Perron (Executive Vice-President, Shared Services Canada): Good afternoon, Mr. Chair and committee members. It's a pleasure to be with you today.

I'm Sony Perron, the executive vice-president of Shared Services Canada. I'm accompanied today by Mr. Matt Davies, deputy chief technology officer for SSC.

[*Translation*]

As you are aware, Minister Murray's mandate includes leading a transformation of the Government of Canada into a more digital government in order to improve citizen service. To effectively modernize how we deliver digital services to Canadians, we are investing resources to develop a fast and reliable network that is secure.

[*English*]

As we move to more services online, the risk to Canadians' and the Government of Canada's information is increasing. Robust enterprise cybersecurity services are essential to our plan, and we must accelerate investment in order to keep ahead of our threat actors.

As you can imagine, network security is more important than ever as Canadians access more programs and services online, such as the Canadian emergency response benefit, as more public servants are working remotely.

[*Translation*]

Prior to the pandemic, approximately 20,000 public servants accessed the network remotely on a typical day. To enable public servants to work from home, Shared Services Canada,SSC, was able to rapidly increase the secure remote access capacity. It can now support 290,000 simultaneous connections. This allowed public servants to continue to serve Canadians during a critical time.

SSC also acquired a suite of collaboration tools so that federal public servants were able to continue working. Today, almost all federal employees are using Teams, which offers a Protected B level of security.

[*English*]

The number of those working online is just astronomical from our perspective. This transition to a distributed workplace has been done without compromising IT security. We are very aware that as the use of digital tools and teleworking increases, so does the risk of being the target of malicious cyber-activity.

[*Translation*]

SSC is continually updating its security infrastructure and software to leverage the latest security measures. We are committed to protecting the Government of Canada's data, information, and information technology infrastructure, along with the data and privacy of our citizens so Canadians can rely on a secure, stable and resilient digital government.

● (1545)

[*English*]

We collaborate with the Canadian Centre for Cyber Security and the Treasury Board Secretariat office of the chief information officer. They are essential partners for SSC for the conception and deployment of responsive IT solutions.

In addition, each and every day we intercept two billion malicious activities. These are not theoretical cyber-threats. They are real, and they are organized. Again, in such context, the collaboration and coordination with our partners is critical.

[*Translation*]

Recently exploited vulnerabilities to SolarWinds and Microsoft Exchange have highlighted the need to be able to respond to cyber incidents quickly and pivot to new technologies.

We recently published a strategy paper on the way forward to modernize the network, which solicited feedback from our various industry partners and stakeholders on the future state of the network.

[*English*]

The paper outlines a number of Shared Services Canada priorities, including moving towards software-defined infrastructure, leveraging improved wireless technology and adopting a zero trust architecture. We are investing in our cyber-defence capability and migrating toward zero trust.

[*Translation*]

The term Zero Trust means we "never trust, and always verify" everything before granting access, through a process of continuous monitoring. This involves verifying users, validating devices, and ensuring that individuals only have access to the resources needed to do their job.

SSC has increased the overall information technology security of the Government of Canada through services such as multiple-layer defence, vulnerability management, and supply chain integrity. Our integrated cyber and information technology security program protects the infrastructure supporting other departments and agencies.

[*English*]

Let me assure this committee that we are constantly monitoring for cyber-threats, and we have a robust system and tools in place to detect, investigate and take active measures to neutralize them. Under normal operating circumstances, no organization is immune to IT security threats, but these are extraordinary times. Cybersecurity is and will continue to be a priority for SSC to safeguard the government and Canadians from cyber-threats.

[*Translation*]

Thank you.

We will be pleased to respond to your questions.

The Chair: Thank you, Mr. Perron.

[*English*]

We'll now go to the Treasury Board Secretariat.

Mr. Marc Brouillard (Acting Chief Information Officer of Canada, Treasury Board Secretariat): Thank you, Mr. Chair. It's a pleasure to be with the committee again.

I'm pleased to be joined today by Aaron Snow, the chief executive officer of the Canadian digital service, along with my colleagues from the Communications Security Establishment and Shared Services Canada. After my opening statement, my colleagues and I will be available to answer the committee's questions.

It may be helpful to briefly explain the roles and responsibilities of the office of the chief information officer as they pertain to cybersecurity in the Government of Canada. The office provides strategic direction and leadership in information management, information technology, security, privacy and access to information across the Government of Canada.

We also provide support and guidance on capacity building, project management and oversight across the government. Treasury Board policy instruments outline the roles and responsibilities for GC cybersecurity management and departmental management. Leveraging the policy on government security and the policy on service and digital, we provide strategic direction and oversight.

We define cybersecurity requirements to ensure the Government of Canada and departmental information and data applications, systems and networks are secure, reliable and trusted. During cybersecurity events, TBS will perform strategic coordination, which may include the issuance of strategic direction to departments and agencies on measures to minimize the GC-wide impact.

This is critical work, which is why our office works very closely with the Canadian Centre for Cyber Security and Shared Services Canada to collectively form the Government of Canada IT security tripartite, established to develop and maintain a coordinated and collaborative approach to enterprise IT security. This includes maintaining awareness of the global cyber-threat environment, regularly scanning for new vulnerabilities that may impact government systems and ensuring there is a coordinated response to potential and active threats through the Government of Canada cybersecurity event management plan.

This work has only intensified over the past 14 months. Throughout the pandemic, we have been working very closely with SSC to support government operations by ensuring that secure IT infrastructure and systems continue to enable the delivery of critical federal services. Virtual collaboration was a key element in ensuring the continuity of operations. To enable this, the Government of Canada has had to adjust rapidly, enabling over 290,000 employees and contractors to work securely and remotely, representing a significant increase in remote connections from pre-pandemic levels.

From the early days of the pandemic, TBS, SSC and CSE worked very closely together to address the quickly evolving needs of the GC. Shared Services Canada procured and provisioned new devices and equipment and rapidly deployed new secure cloud-based collaboration and communications systems, while the office of the chief information officer provided resources, advice and guidance to Government of Canada departments, employees and contractors on working remotely securely. During this time, CSE provided ongoing advice on the evolving cyber-threat conditions related to the pandemic. This was to ensure that public servants could continue serving Canadians all while ensuring that the security, privacy and integrity of government information was not compromised.

Another example of collaboration is the work of the Canadian digital service, or CDS, a team within the Treasury Board Secretariat that collaborates with departments to address service delivery challenges. CDS has developed GC Notify, a platform tool that allows departments to quickly and easily push email and text messages to subscribers. When the pandemic started, misinformation was prevalent. CDS, Service Canada and Health Canada came together to use GC Notify to build “Get Updates on COVID-19”, an email service to get people quick and trusted info about COVID-19. Since its launch, the service has securely sent over 5.5 million notifications to subscribers.

Indeed, security has been the priority throughout the pandemic. With so many public servants working from home, we have taken concrete steps to ensure the ongoing security and safety of government networks. We have robust systems in place to monitor, detect and investigate potential cybersecurity threats to information, including new and emerging threats that resulted from working remotely. Safeguards such as enhanced and enterprise secure remote access and digital signature workflows, as well as appropriate policy guidance, have been used to protect information while ensuring employees can continue delivering trusted services and programs to Canadians.

It has also been working to protect the Government of Canada by defending important programs against cyber-threats, including COVID-related benefits, such as the Canada emergency response benefit. The centre is constantly monitoring the security of cloud usage across the Government of Canada and evaluating cloud applications, including for the Public Health Agency of Canada.

The COVID-19 pandemic continues to transform the operational and service landscape of government departments. It has forced us to accelerate digital transformation efforts that were already under way and to move quickly to deliver new services that directly support Canadians. At each step of the way, security has remained at the forefront.

● (1550)

We will remain focused on continuously enhancing cybersecurity in Canada by preparing for all types of cyber incidents and protecting Canadians and their data.

Thank you, Mr. Chair. We are ready to take the committee's questions.

The Chair: Thank you, Mr. Brouillard.

We will now start the first round of questions.

We'll start with Mr. Paul-Hus for six minutes.

[*Translation*]

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

Good afternoon, gentlemen. Thank you for being here.

Mr. Jones, the first time I asked you about Huawei was in September 2018, at the Standing Committee on Public Safety and National Security. I asked you about Canada's position on Huawei and the development of 5G. Obviously, it's been almost three years and the information was less known, but now we know very well that our Group of Five partners have made their decision.

Have you delivered your technical report to the government?

[*English*]

Mr. Scott Jones: This matter is before ministers. I don't think it's appropriate for me to comment any further. However, it is something we continuously work on in terms of cybersecurity, working with our partners—

[*Translation*]

Mr. Pierre Paul-Hus: Mr. Jones, I'm asking you, as the chief executive officer of the Canadian Centre for Cyber Security, if you have submitted a report. I'm not asking you for the results of the report, I'm just asking you if you gave the report to the Minister of Public Safety or the Minister of National Defence.

[*English*]

Mr. Scott Jones: Mr. Chair, as I said, we continue to work with our partners across the government. Our information has been shared with our partners, but we are waiting for our.... The Department of Public Safety is the lead on the overall study and report.

[*Translation*]

Mr. Pierre Paul-Hus: All right.

I would like to ask you another question regarding the same company.

Has your organization been consulted about the partnership between Huawei and Ice Wireless, a company that is doing development projects in the Canadian North?

● (1555)

[*English*]

Mr. Scott Jones: I would have to look into anything that we do have.

Under our current existing security review program, we have relationships with the majority of the telecommunications providers around Canada. We do talk to them about their overall deployments and their plans, but it is related to the 4G/LTE environment right now. Any specifics on our dealings with specific companies is something that I'd have to look into.

[*Translation*]

Mr. Pierre Paul-Hus: A group of 60 experts, including members of the RCMP's National Cybercrime Coordination Unit, have made a detailed plan to combat ransomware and are calling on governments around the world to take action.

Will the government accept all the recommendations in this report?

[*English*]

Mr. Scott Jones: In terms of the government accepting the report, I think the report you are referring to, Mr. Paul-Hus, if I understand correctly, is the cybercrime ransomware report.

[*Translation*]

Mr. Pierre Paul-Hus: Yes.

[*English*]

Mr. Scott Jones: It would be unacceptable, I think, for an unelected public servant to speak on behalf of the government, the elected government. However, we certainly do look for any activity we can take to bolster our defences against ransomware, something that we're taking very seriously as part of the Canadian Centre for Cyber Security.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

Mr. Perron, a non-confidential internal report has been released by the Department of National Defence regarding its evaluation of the Defence Information Management and Information Technology Program.

This report, which was released last year, criticizes Shared Services Canada over its management of computer systems. The military complained loudly, first, that it was not understood in terms of operations and, second, especially, that it did not have services. Shared Services sometimes took up to six months to respond to DoD requests.

What can you tell us about that?

Mr. Sony Perron: Thank you for your question.

I am aware of the references in the report that was issued by the National Defence audit group. This report is about actions in the last few years. Since then, we have implemented a new structure at Shared Services Canada that allows us to have better interaction with client departments.

We now have an assistant deputy minister and a team that serves the departments of National Defence and Veterans Affairs exclusively, as well as the Royal Canadian Mounted Police. So we have a new interaction structure in place, and we are trying to develop more integrated plans.

There were, in particular, a lot of questions about the deployment of phone services for military bases. That has been resolved. We now have a joint work plan with DOD and we've started the work. So things are getting better.

Mr. Pierre Paul-Hus: Very good. Have you improved the weekend services? One of the problems was that no one was responding to requests on Saturdays and Sundays. Are there now people on call who can respond? The Canadian Forces work seven days a week, 24 hours a day.

Do you now have personnel who can respond to requests?

Mr. Sony Perron: I'm sorry, but I can't answer that specific question. Each application on the GoC network has its criticality standards and the response time is set for each. For National Defence, the criteria vary depending on the services offered. Some may need to be revised. That said, I am not in a position to answer that question. However, I can provide the answer in writing, if you wish.

Mr. Pierre Paul-Hus: Yes, please. We would like answers on that.

Thank you.

[*English*]

The Chair: Thank you, Mr. Paul-Hus, for your questions and the responses.

As I've indicated in the past, if the responders have indicated they would look into something or provide a response, please provide that to the clerk as that would be appreciated, and the clerk will distribute it to the members.

Thank you.

We'll now go to Mr. Jowhari for six minutes.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Mr. Chair.

First of all, thank you to all the witnesses for the service you and your departments are providing over many years, and especially over the last year and a half, to make sure various parts of the Government of Canada and those who work with them are kept safe.

Mr. Jones, in your opening remarks, you said that the cyber centre has been focused on supporting COVID-19 vaccine research and development entities across Canada.

Can you specifically talk about the measures you've taken and the types of threats you potentially identify?

● (1600)

Mr. Scott Jones: Absolutely, I'd love to talk about that. There are a few aspects.

First of all, we have been working with multiple entities across the sector on providing basic advice and guidance on cybersecurity, but also specific threat information. Early in the pandemic, along with our allies, we did note there was malicious state-sponsored activity targeting vaccine researchers. We went public with a public attribution on that.

We followed that up with private advice on what could be done to protect against those threats, what the threats looked like and what steps organizations could take. Further, though, we continue to work with those organizations to ensure they are strengthening their cybersecurity by providing advice and guidance on things they can do to secure themselves. That includes our sharing everything we learned from our defence of the Government of Canada, so they're well-prepared for any threats. Certainly, using our foreign intelligence mandate, learning what any threat actor is looking for, we also make sure the sector is aware of those threats as well, so it can take action before things happen.

Mr. Majid Jowhari: You also mentioned a number of specific vaccine support organizations you work with. You talked about the protected DNS.

Can you expand on what the protected DNS is and what specifically your organization has done?

Mr. Scott Jones: This is one of those areas where at previous meetings I've talked about a service called Canadian Shield, which is a service we work with with the Canadian Internet Registration Authority.

Let's say you get an email with a piece of malware, and it says, “Click on this”, and it's cybercrime. When you click, you can't go there. It stops it. That's how it's protected. It protects you from making that mistake when you click.

We've partnered with CIRA to provide the same service for commercial entities, in this case vaccine support organizations. We did that because of the threat they're facing during the pandemic. We worked to provide that same service.

That includes everything we learned from the Government of Canada and everything that we block. There are up to seven billion actions per day we take to defend the Government of Canada. We make sure all of that is also shared with CIRA, our partner in this, so that all those organizations also benefit from the same defence.

Mr. Majid Jowhari: I also understand our government recently updated the digital operations strategic plan. I would like to get some input from all three witnesses on what their thoughts are about this. Could you start by explaining what the OSP is and how each one of your departments is contributing to that?

We could probably start with Mr. Jones.

Mr. Marc Brouillard: Mr. Chair, my office is the one that publishes what we call the DOSP. If it's okay, I can start, and then I'm sure the other members will have more to add.

Mr. Majid Jowhari: Okay. Let's start wherever is best.

Mr. Marc Brouillard: Thank you.

The DOSP is a document that is updated every year. It provides a three-year integrated management plan for service, information, data and cybersecurity. The current DOSP has been updated and refreshed to reflect the accelerated digital transformation. I

t's made up of four areas, or what we call the four pillars. The first is modernizing the way we replace, build and manage major IT systems, addressing the legacy, what we call the technical debt within our organizations. The second is providing services to people when and where they need them, ensuring that we provide user-centric services to Canadians. The third is taking a whole-of-government approach to digital operations, providing an enterprise view so that we don't duplicate some of our efforts. The fourth is about transforming how we work, understanding that new ways of working, of providing governance, of providing resources, are critical to being able to answer the challenge.

I would leave it there and allow the others to respond if they wish.

Mr. Sony Perron: Mr. Chair, from the Shared Services Canada perspective, this plan is very critical in the sense that it provides the architecture and direction for all the client departments to advance the agenda, from dealing with legacy architecture and us supporting them, modernizing their infrastructure and us supporting them, and transforming the enterprise and us supporting them. All the signals that are in this plan are essential for SSC to achieve its mandate.

It influences the client department that comes to us for support in advancing its own IT agenda, to provide them a broader framework. We are prepared to support that, so it goes into supporting workload migration. It supports advancing connectivity to the cloud and providing access to the cloud in a secure manner. It supports and directs departments to participate actively in enterprise solutions so we avoid duplication of technology, and rather, use an enterprise approach that serves all departments. It's an essential pillar of our work agenda.

● (1605)

Mr. Majid Jowhari: Thank you. I think I'm out of time.

The Chair: Seeing as the other two have responded, if you would just quickly give us a response, Mr. Jones, we'd appreciate it. Thank you.

Mr. Scott Jones: Thank you, Mr. Chair.

Quickly, I think the digital operations strategic plan lets us ensure that security is built in from the start and forefront and is thought of at the beginning, and also in setting priorities. The fact is we have limited security experts, so it makes sure that we also put those resources on the most important priorities for the entire Government of Canada to advance the agenda. Both of those are critical.

Mr. Majid Jowhari: Thank you, Mr. Chair.

The Chair: Thank you.

Now we'll go to Ms. Vignola for six minutes.

[*Translation*]

Mrs. Julie Vignola (Beauport—Limoilou, BQ): Thank you, Mr. Chair.

My question is for Mr. Jones.

Was the service provided to Canadians interrupted because of malicious cyber-events?

[*English*]

Mr. Scott Jones: There is a continuing range of cyber-activity that we face every day. As I mentioned a few minutes ago, we take between two billion and eight billion actions per day, on average around seven billion, because of cyber-activity targeting the government, but to my knowledge—

[*Translation*]

Mrs. Julie Vignola: I know there are a lot of cyber attacks. However, did any events prevent the provision of services to Canadians?

[*English*]

Mr. Scott Jones: I would probably turn to my colleague Monsieur Brouillard to answer from the Treasury Board perspective, but as far as I know, from my perspective, we've managed. We have not seen any disruption because of cyber-attacks to the Government of Canada. There have been cyber incidents where we have chosen to take action, but nothing that the cyber-attack itself disrupted.

[*Translation*]

Mrs. Julie Vignola: Fine, thank you.

We all know that the personal data of tens of thousands, if not hundreds of thousands of people were stolen. They have received income statements for wages they never earned.

What are the causes of these data thefts? What solutions are in place?

● (1610)

Mr. Marc Brouillard: I can answer that.

You are referring to the credential stuffing attack that took place last summer. The identities of some Canadians were stolen by other sources. We don't know what those sources are specifically, but we do know that there were other events that affected the Canadian economy.

This information is often found on what is known as the dark web, which is sort of the criminal side of the Internet. Criminals take people's identities or whatever information they can gather and try to use it in federal systems. When we saw that there were a lot of attacks on people's identities, we made the decision to shut down the service. We wanted to make sure there were no more significant attacks. Subsequently, the Canada Revenue Agency verified the transactions. In all suspicious cases, citizens were contacted or the situation was reversed.

Mrs. Julie Vignola: Fine. Thank you.

Cyberattacks most often target the same frequently used software. This is the case for the Office suite and anything Microsoft.

Doesn't using software like Microsoft increase the government's exposure to cyberattacks, given that it is that company that is mostly targeted?

Mr. Marc Brouillard: I'll let my colleague Mr. Jones answer that question.

[*English*]

Mr. Scott Jones: Thank you for the question.

There are a few things to consider. Yes, it is the most used software, so of course anybody looks to the most frequently used software in terms of malicious actors. However, it's also the software on which the most security researchers have already been working as well.

One of the important aspects I would point to is the Government of Canada's response to things like patching, updating that software, keeping it up to date and managing it properly. That's one of the aspects of the benefits of Shared Services Canada. We've seen that there is a significant improvement when SSC is the lead for a department to respond very quickly to our alerts. In some of the larger cases, within minutes of our alerts, SSC was beginning the patching process to make sure we were ready to go, and I think that's something.

Every software has vulnerabilities. It's about how quickly you can respond to mitigate and reduce the risk we face as organization. No piece of software is invulnerable, unfortunately.

[*Translation*]

Mrs. Julie Vignola: In the past few months, the Russians have on several occasions amused themselves with attacks on U.S. systems, including software from the American supplier SolarWinds. These folk successfully infiltrated the U.S. Department of Homeland Security and the Treasury Department.

Have such attacks occurred in Canada? If so, who were the targets of these attacks and how were they dealt with?

Mr. Marc Brouillard: There were some companies on the Government of Canada network that were using SolarWinds software, but because of our infrastructure and the capacity of Shared Services Canada and the Communications Security Establishment, they were able to determine what was going on and find that our infrastructure was not under attack. They identified the vulnerabilities and worked to resolve the problem. As far as I know—my colleague Mr. Jones can confirm this—we have not experienced anything like what the United States has experienced.

Mrs. Julie Vignola: Thank you.

[*English*]

The Chair: Thank you. I appreciate that.

We'll now go to Mr. Green for six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you.

I'm happy to pick up on that line of questioning. Just to be clear, through you, Mr. Chair, to Mr. Jones, I believe it was the CRA breaches of close to 50,000 incidents of suspicious activity that my friend from the Bloc just referenced. Would that be something that the Communications Security Establishment would flag and pick up, or would that be left to the agency's forensic analysis?

Mr. Scott Jones: Mr. Chair, I think that's a great question.

One of the areas where, in terms of credential stuffing or information theft, the amount of information that's already been stolen about so many of us from different data breaches and is reused against the government is the threat.

Typically, what you're talking about there is how the application is being abused in terms of attempting to commit fraud. That would be where it would be for the department to look for. They know what normal activity looks like, so the department would look for things that look abnormal, but we would obviously work with them.

We work closely with CRA throughout this and any department that runs these types of services, but that would be something that looks from a cybersecurity perspective from the outside like a normal user. I have your username and I have your password, so it looks very legitimate. That's where we make sure there's no light between departments, so we look outside and the departments look inside for fraudulent activity.

Mr. Matthew Green: We've heard lots of discussion around the prevalence of CERB fraud, and yet we hear Mr. Brouillard talk about 50,000 identities stored in the dark web. Have there been any early indications or cross-reference between information that was taken through these breaches and potential fraudulent applications for the CERB?

● (1615)

Mr. Scott Jones: Mr. Chair, I think I'll turn to my colleague—

Mr. Matthew Green: Before that happens, Mr. Chair, can I just ask Mr. Jones if something like that would be in his purview before it's passed along?

Mr. Scott Jones: We're really talking about two different things, Mr. Chair. I think there's the number of data breaches that have happened. The Privacy Commissioner of Canada, in our national cyber-threat assessment where we highlight this, said that 28 million Canadians last year had their information taken. That information has then been reused to target the Government of Canada. By reusing passwords, for example, somebody was able to log in.

We're not talking about information that was taken from the government. It was taken from other data breaches, but people reuse things. Our security questions are the same. What's your favourite colour? What school did you go to, etc.? That's the information these criminals have stolen, and because passwords are horrible and we all have too many of them, we tend to reuse them. A lot of Canadians reuse them, and so those were able be reused. That's what credential stuffing is. Really, we're talking about information from other data breaches then turned and used against the Government of Canada. But Marc, maybe—

Mr. Matthew Green: I do say this respectfully, because it's not often that we have a member from the Communications Security Establishment before us. This is why I'm trying to get the most out of this intervention, because I don't know when you may be back.

Is there a scenario—this is for my own edification—where the information that might have been obtained through the CRA's vulnerabilities could then have been used to re-access fraudulent CERB applications? Maybe I'm oversimplifying it or conflating it.

I'd love to hear from you, Mr. Jones.

Mr. Scott Jones: I think that would be a pretty unlikely scenario, to be frank, because that wasn't what we saw happening here. We saw Canadians being impersonated in this activity where they were using their legitimate credentials, so essentially logging in as them. I think that's kind of my overall response to this, but Marc might be able to tell you more.

Mr. Matthew Green: That's fair. When I hear that the information would be parked on the dark web, I just have this nefarious vision of what that looks like and how it might be used through organized crime, non-traditional organized crime and other entities to defraud the government. I'm just wondering if some of our own vulnerabilities may have played a role in that in some way.

This is a follow-up question for Mr. Jones through you, Mr. Chair.

I've heard now in many different public accounts committees and different places about the legacy and just how old some of these technologies are. Is this something that is currently being reviewed by the Communications Security Establishment? Would it be in your oversight to review system-wide vulnerabilities and provide information back to departments that would triage and find the biggest gaps in our security?

Mr. Scott Jones: That's a great question, and you have the right group here. It's the tripartite that would really look to say how we would make sure the government is robust. Marc would lead that as the CIO for the government. So yes, the answer is that, in some cases, legacy does work in our favour. Sometimes things are so old that they don't—

Mr. Matthew Green: This is the floppy disk. We're not going to have any floppy disk espionage.

Mr. Scott Jones: Sometimes it's so old it just doesn't connect to the Internet. In most cases, though, this is where Shared Services Canada, our perimeter strategy, making sure that we're ringing security and layering different elements of security to afford that level of protection.... We do take very seriously the need to protect that information.

As we modernize those systems and implement the digital operations strategic plan, we make sure that we're building in security from the start. The fact is there have been so many data breaches—we're talking about outside of the Government of Canada—that there is a tremendous amount of information available on each citizen, about all of us on the web.

I know I have been the victim of data breaches, so when Yahoo was breached—

Mr. Matthew Green: Wow. Did they ever pick the wrong guy.

Mr. Scott Jones: Well, it's the reality.

Mr. Matthew Green: Yes, unfortunately.

The Chair: Thank you, Mr. Green.

Mr. Jones, thank you.

We're finished our first round. We'll now start our second round.

We have Mr. McCauley for five minutes.

Mr. Kelly McCauley (Edmonton West, CPC): I liked where Mr. Green was going with that.

I appreciate the witnesses being here today.

The revised National Security and Intelligence Committee of Parliamentarians annual report showed up on our desks a couple of days ago. I have a couple of questions about that.

It talks about China and Russia as the main malicious actors that we have to be aware of. Is that for industrial espionage, attacks on the government, attacks on our logistics systems, or issues like utilities and so on? Would you be able to let us know about that?

● (1620)

Mr. Scott Jones: Mr. Chair, I'd actually refer back to our national cyber-threat assessment, which we issued in November 2020. We listed four states as the primary threats to Canada: China, Russia, North Korea and Iran. We mentioned that intellectual property theft is one aspect of this, but critical infrastructure was also an interest.

I would really like to emphasize, though, that we did say that absent international hostilities, we think it is extremely unlikely that any nation-state would deliberately disrupt critical infrastructure. I want to really emphasize that point because—

Mr. Kelly McCauley: What do you term as critical infrastructure? You made a comment about the absence of an act of war. We just saw Colonial taken down a couple of weeks ago. Is that not a similar concern for us?

Mr. Scott Jones: It is, absolutely. In fact, that is something I said with the National Post. One of the concerns we have is that when ransomware is deployed against a victim such as a critical infrastructure provider, because of the way technology is merging together, it means that to defend themselves, they take all of their technology offline. They isolate and shut down to take protective measures.

Publicly, we saw Colonial do that. They took their pipeline operations offline so that they could get back control of their infrastructure. Something that we highlight in the national cyber-threat assessment is that we need to be taking this very seriously. Ransomware is the number one threat facing Canada and Canadians. That includes critical infrastructure, for the exact reason that we say. We were all hoping, in the cybersecurity industry, that we wouldn't see something like the Colonial pipeline, but it is the first of many.

Mr. Kelly McCauley: Who would be responsible for following up on such things? We always say it's a wide amount of responsibility. Of course, there are airports, pipeline infrastructures, utilities. Who generally is responsible for that so that we don't have a Colonial situation here, or an attack on an airport, or other issues? Is it just different levels of government?

Mr. Scott Jones: It depends. We work with all levels of government, and we work with critical infrastructure providers. We make sure that all the information is provided and available. We try to build individual relationships with companies. In general, we have a very receptive audience. They all care about this as much as we do.

However, the IT environment is, in general, weak for cybersecurity, and so you have to layer on this tremendous amount of defence. These are areas where we work together. It's a shared responsibility, not just of the federal government but, ultimately, of the infrastructure owner and operator. They own their network. They own their infrastructure. They make investment decisions. We work to make sure that they have all of the best information we can give them, and we work together to try to make sure that we're addressing threats as early as possible. It's a shared responsibility.

Mr. Kelly McCauley: What about Crown corporations? Are they treated exactly like government departments?

Mr. Scott Jones: No, Mr. Chair. Crown corporations have a unique status. We are able to provide the same levels of service that we do for all federal organizations. Just because of their structure, their chief executives tend to have more flexibility in terms of what they decide, more like the private sector, in terms of what they do for cybersecurity, but we do work with many of them.

Mr. Kelly McCauley: Yes, a lot of that, obviously, was decided years ago before we had such issues coming up. Is that something on which we need a rethink? Yes, Crown corporations operate at arm's length, but that being said, for something like cybersecurity, should we have a rethink to bring it under CSE?

Mr. Scott Jones: Well, as I said, we are able to provide the full range of services that we do for the federal government. It is by far our biggest client, but those are optional for Crown corporations. They make the choice. We have made the offer to every one of them to work with them just as we do with every government department.

● (1625)

Mr. Kelly McCauley: Thanks.

The Chair: Thank you, Mr. McCauley.

Now we'll go to Mr. Kusmierczyk for five minutes.

Mr. Irek Kusmierczyk (Windsor—Tecumseh, Lib.): Thank you, Mr. Chair.

Each year the chief information officer hands out community awards. In 2020 Shared Services Canada was awarded the excellence in diversity and inclusion award for the accessibility, accommodations and adaptive computer technology program, or AAACT. I was delighted to see that an additional $3 million was allocated in budget 2021 towards this important program. Again, I'm delighted to see the work of SSC in accessibility and disability inclusion, so well done to the team.

This being National AccessAbility Week, are there specific challenges when we talk about cybersecurity and disability inclusion? In other words, how do we make cybersecurity accessible?

I guess this would be a question for either Mr. Perron or Mr. Davies.

Mr. Sony Perron: Mr. Chair, it's an interesting question in the sense that while we are very focused on security and cybersecurity, we need to make sure that our employees and Canadians have access to the services and the systems we are putting in place. Accessibility is always, besides security, one of the preoccupations.

At Shared Services Canada we have a team, which is called the accessibility, accommodation and adaptive computer technology program team. It reviews and advises departments on applications and solutions to really make sure that when something is launched, whether it's an application or a new process, it's accessible by default, making sure that what has been in place for a while is also reviewed and adjusted. We follow the standards for accessibility. We have that capacity, and it's very important.

The link with security here is that when we implement new measures, we have to make sure we test them from an accessibility perspective so that it doesn't become a barrier for those who legitimately need to access these applications and these systems to do their work or to access their services. It's critical that we maintain that attention.

There are two other aspects to this program. One is about supporting the employees so they receive an assessment of what might be needed for them to fully operate in the workplace, so making sure that we have equality there. The other is about providing advice. Last year we added a dimension that had been missing from that, which is that new employees or temporary employees coming in also benefit from what we call the lending library. It's to make sure that early on in their employment with the federal government, as an employer of choice, we provide them with the tools and the adaptations in terms of technology, monitors, devices and applications that can help them to fully participate in the workplace. This program is essential.

Thank you for mentioning that. It's very important, particularly this week.

Mr. Irek Kusmierczyk: That's it exactly. I appreciate the fact that whenever we're looking to introduce cybersecurity measures, we're always putting an accessibility lens on those measures themselves so that they don't add barriers to our federal employees.

According to the digital operations strategic plan, the federal government is on track to launch the OneGC program, which will allow individuals and businesses to use a single identity and password to access federal government services through a single window on Canada.ca. We're talking about making things easier as well for people.

What is the status of the work on the OneGC platform? What are some of the challenges to delivering on that vision?

Mr. Marc Brouillard: The principle behind OneGC is that we don't want Canadians to have to try to understand and decode all of the government bureaucracy machinery behind it, and really have a single window for all services to Canadians. That's Canada.ca. To enable that to the next level, to take it to a service-oriented environment, the foundation of that is digital identity. We want to be able to allow Canadians to use the trusted identity of their choice to access services on Canada.ca and to move between those services seamlessly.

We've recently launched a pilot project with ESDC, which is called the benefits delivery modernization program, to enable what is called Sign In Canada. This is going to be used specifically to access those benefits that ESDC delivers in a way that is seamless to Canadians. They'll be able to log in once and access multiple services.

We're doing that with an enterprise lens so that once that work is completed, it will be reusable by other departments and agencies, so that ultimately and eventually all GC services will be available through a single identity capability. That's what we call the OneGC.

Thank you.

● (1630)

Mr. Irek Kusmierczyk: Are there additional risks or challenges that this service simplification or streamlining represents in terms of cybersecurity?

Mr. Marc Brouillard: Under the current model, if you had all services accessible under a single credential and that credential was compromised, there would obviously be an increased risk. What we're doing to address that is making sure this is bound not just through a credential but through a true digital identity, something that is verifiable and highly secure. For example, you would need to be able to provide access to your provincial identity plus maybe a password or some other form of identification. Multiple actions are required to gain access to it. We call that multifactor authentication. That's how this service will be more secure.

The Chair: Thank you, Mr. Kusmierczyk.

We'll now go to Ms. Vignola for two and a half minutes.

[*Translation*]

Mrs. Julie Vignola: Thank you very much.

My question will be to Mr. Jones or Mr. Brouillard. They are sharing the task.

Mr. Brouillard, last week there was some half-joking, full earnest talk about outdated systems, comparing them to our old DOS systems. Joking aside, what are the biggest risks and threats caused by our outdated systems? The Auditor General talked about breaking points caused by obsolescence.

Are we at that breaking point? What might the consequences be for citizens? Where exactly are the threats coming from? Are they domestic or international threats? If they are international, which country is attacking us?

Mr. Marc Brouillard: I will answer the question first.

I'll explain the difference between technical debt and legacy system risk.

First, the older the systems, the more expensive it is to maintain them. It's like buying a car and not putting oil in the engine: sooner or later, you'll have to replace the engine.

Second, as systems age, cyber risks increase because systems are exposed for much longer to cyber attackers.

I will turn the floor over to Mr. Jones to explain this risk.

[*English*]

Mr. Scott Jones: Thank you.

There are a couple of things I would just add. The first one is that if the system is connected to the Internet, it has to be kept up to date. That's where our legacy environment just isn't connected in that same way. This is where a modern environment does change the threat.

That being said, in general, where we're looking at threats coming from actually doesn't matter as a cyber defender. We look at what the malicious activity could look like, no matter where it comes from, because we don't differentiate that. Then if there is a threat it's dealt with by the proper authorities who investigate those types of activities. In most cases it would be the RCMP if it were something of a criminal nature.

When we're looking at the IT environment there are a few things we've said, and they're in our top 10. One of the biggest ones is maintaining systems up to date, keeping them up to date and ensuring that they're continuously improved. That's one area where we need to be working on the next generation of technology with security built in from the start. Security is not something you bolt around systems; it's built in throughout the process. When Marc was talking about the digital identity process, security was thought of from the start, before a single piece of code was written or a simple application was purchased. That's what we need to be doing going forward.

The Chair: Thank you, Mr. Jones and Ms. Vignola.

We'll now go to Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you.

On May 25, 2020, Mr. Glover told the committee that in the first 10 weeks of the pandemic, there had been no incidents involving data breaches. However, during the same period, there had been incident blocks every day, but none of consequence.

How has the situation evolved since May of last year? Have there been any incidents involving data breaches?

That's for the CIO, Mr. Brouillard, I believe.

● (1635)

Mr. Marc Brouillard: Mr. Chair, to my knowledge, there have been no significant data breaches related to cyber-activity since the pandemic started. There was the credential stuffing incident from last summer, which as Mr. Jones talked about, wasn't a breach of our systems; it was people accessing the system with fraudulent credentials. That really becomes fraud, not cybersecurity.

Some other incidents we've talked about today—SolarWinds, the Microsoft Exchange vulnerability, some third party vulnerabilities as well—have been addressed. They were remediated, but there was no significant breach of data.

Mr. Matthew Green: Have there been any incidents concerning blocks that are of consequence? If so, how many and when?

Mr. Marc Brouillard: I'm sorry. Please define “blocks”, as in—

Mr. Matthew Green: Well, Mr. Glover was quoted as saying that there had been incident blocks every day, but none of consequence. I think I know what it means, but I don't want to—

Mr. Marc Brouillard: On the technical aspects, maybe Mr. Perron or Mr. Jones would like to comment.

Mr. Matthew Green: Is it a denial of service type of deal?

Mr. Marc Brouillard: That they stop, yes.

Mr. Sony Perron: Maybe I can add that in the first, I would say, 10 weeks of the pandemic, there were difficulties for the system to accommodate remote access and there was not enough connection. When it came to the end of May to June last year, the capacity ramped up in terms of secure remote access, so these blocks have stopped.

You may have noticed at the time that Mr. Glover was talking, we were also talking about the situation where we were asking employees to use the system only at certain times of the day. We went over this during the summer by increasing the capacity of secure remote access.

I will insist on the words “secure remote access”. The idea is not to give access. It's to give secure remote access, allowing our employees to work from home and not increase the risk for the network and the government's activities. Now we are able to provide 290,000 simultaneous connections, and we have answered all the demands from the departments in terms of increasing capacity.

With regard to these situations that were visible in the first few weeks of the pandemic, with hard work and collaboration among the parties, we were able to put in place solutions that have allowed hundreds of thousands of federal employees to do their work from home.

The Chair: Thank you, Mr. Perron and Mr. Green.

We will now go to Ms. Harder for five minutes.

Ms. Rachael Harder (Lethbridge, CPC): Mr. Perron, my question is for you.

Shared Services is responsible for all IT-related procurement. We're talking about emails, telephone, computer data centres for the entire Government of Canada. Given your role, can you tell this committee whether or not there is a prohibition on securing Huawei technology for any department within the Government of Canada?

Mr. Sony Perron: Mr. Chair, there is a process that is called the supply chain integrity process that is managed by the Communications Security Establishment. SSC will refer procurement activities with suppliers or new products to CSE for review and advice, to look at the security aspect. It's not only the product or the service, but it's how the service is constructed and delivered that needs to be reviewed before we make a decision.

On this, maybe if you agree, Mr. Chair, we'll turn to Mr. Jones to explain what is being performed in terms of assessments.

Ms. Rachael Harder: I'll just interject for one second.

I'm not looking for an overall summary of the evaluation process. I'm actually looking for quite a simple answer, and that is whether Huawei technology is prohibited from being secured by the Government of Canada for any of its services.

Mr. Sony Perron: Okay. I will try to be a bit more clear.

We don't have any Huawei technology operating on our network at this time. If there were any provider that would be coming with that technology, it would be part of the package that would be reviewed through the supply integrity chain, and CSE would provide its advice.

At this point, we haven't procured...we are not using Huawei technology on the Government of Canada network.

Ms. Rachael Harder: I can appreciate that you're not doing that at this time, but is there a policy in place in order to protect us from any future procurement of Huawei technology?

Mr. Sony Perron: With regard to the policies when we are acquiring services or technology, we go through the supply chain integrity process. We ask for advice from CSE before taking action. There is a built-in process to assess the integrity of the supply chain and to make sure we are making the best decisions to support government operations and the service to Canadians. This is called the supply chain integrity process.

● (1640)

Ms. Rachael Harder: What I'm hearing from you is that Shared Services Canada would be open to the possibility of securing Huawei technology. Is that correct?

Mr. Sony Perron: What I'm saying is that each time we are procuring new products or new devices, we are going through the supply chain integrity process that has been put in place to assess each and every transaction.

Ms. Rachael Harder: That supply chain you're talking about, that integrity—there's nothing in there that would preclude Huawei technology from being set up here in Canada.

Mr. Sony Perron: Mr. Chair, to answer the question from the member of Parliament, this process is managed by the CSE, so in terms of describing what the steps are and how this proceeds, I think Mr. Jones would be better equipped than I would be to explain that.

Ms. Rachael Harder: I will allow Mr. Jones to comment on the question.

Mr. Scott Jones: In the supply chain integrity checks, we check a number of things—the type of equipment, the vulnerability, foreign ownership control and influence, and many other aspects. Then we come up with a risk rating. If the risk rating is too high, the department, in this case Shared Services Canada, would make the decision on whether or not to accept or reject and look for another type of product. Because we do this on a product-by-product basis, we always look from the start so that we are always following the rules of things like trade agreements, etc., and providing the best advice to Shared Services.

The goal for us there is to make sure that we're giving a complete and comprehensive assessment of the supply chain risk so that departments can make their decisions.

Ms. Rachael Harder: Thank you.

To my specific question, then, with regard to Huawei, we have concrete evidence of Chinese espionage, infiltration and systematic interference in Canadian companies and the federal government. That seems like a pretty high risk in terms of doing that risk assessment that you're talking about, which includes foreign ownership, and then, of course, the risk that this type of technology would pose to Canadians and the government.

Is Huawei being discussed? I mean, the Five Eyes have all banned Huawei technology or come up with very significant protocols in terms of its use. Is Canada going in that direction? Are you giving that any consideration? Is that going to be part of the policy going forward?

Mr. Scott Jones: As Monsieur Perron has said, the Government of Canada does not have any Huawei technology operating on our networks. We put our equipment purchasing, any equipment purchased, through our supply chain integrity process.

Ms. Rachael Harder: I'm sorry. That didn't answer my question. Is there a process being put in place to protect Canadians and the government in terms of the sensitive information that is held within our data systems? Is there any initiative being put in place to make sure that Huawei technology is not used in future endeavours?

Mr. Scott Jones: The supply chain integrity process is there to ensure that all decisions made are made to ensure the safety and security of Canadians' information and Canadian networks and Government of Canada networks, in this case with Shared Services Canada.

The Chair: Thank you, Ms. Harder.

We'll now go to Mr. Drouin for five minutes.

Mr. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Thank you, Mr. Chair.

I want to thank the witnesses who are before the committee.

I want to jump back to the supply chain integrity. Perhaps I can ask Mr. Perron how long this supply chain integrity has been in place.

Mr. Sony Perron: You're asking me a historical question. I haven't been at Shared Services Canada that long. I won't be able to answer that and give you a date.

I think Mr. Jones or Mr. Brouillard could probably give us the date when this was created.

Mr. Marc Brouillard: Unless Scott knows the exact date, we would have to get back to you on the specifics. I've certainly been aware of it for many years. I've been here since 2016, but I couldn't specify an exact date.

Mr. Francis Drouin: Okay.

Mr. Jones.

Mr. Scott Jones: In terms of the formal program, it goes back to the initial stand-up of Shared Services Canada. However, there was supply chain integrity advice given well before that, in the years leading up to it and before my involvement in cybersecurity, which has been about 14 or 15 years.

The formal program really started with Shared Services Canada and the fact that there was one central place to work with in the procurement and to work on these big projects.

● (1645)

Mr. Francis Drouin: Okay.

I just want to make sure that I understand this correctly. A company—and it doesn't matter whether its Huawei or whomever it is—may be able to participate in a procurement, but as soon as it goes through the supply chain integrity, that may come back and say, “Sorry, but your security just won't pass, so you can't participate.” Is that the goal here?

Mr. Sony Perron: Exactly. It's also to make sure that we don't only look at the surface. The process looks deep. What is behind? What is behind in terms of technology?

Sometimes we buy services. These service providers will have their own technologies and their own infrastructures. These have to be transparent. This information is supplied by the bidders through the process to SSC, and this information is provided to the CSE to perform the assessment. We are relying on the advice to make a final decision on the procurement.

Mr. Francis Drouin: Right.

A Canadian company could appear at the forefront to be secure and whatnot, but its own suppliers may be compromised or may use technologies that are compromised. That's the point of the supply chain integrity process.

Mr. Sony Perron: It's the assurance that SSC is looking for through that process. It's to make sure that those with the expertise and the knowledge will go through the process and perform that kind of assessment that our technical team may not have the expertise to do. We are lucky in Canada; we have this centre with specialized resources that focuses 100% of its energy on this question. It's providing us with the assurance that we are making the best choice from a security perspective.

Mr. Francis Drouin: Great. Thank you.

I'll switch gears.

Some Canadians, obviously, felt the impact of their government accounts being closed with the CRA. Can someone explain to me what happened there and why the government took the precaution to shut down these accounts? What is the best way for Canadians to prevent that from happening?

Mr. Marc Brouillard: I can answer the first part of that question, Mr. Chair.

The CRA has been proactively using different methods and third parties to look for signals that accounts have been identified and potentially compromised. This is anything from, again, going back to the capabilities where there have been previous compromises or known lists of identities that are suspicious. All they do is deactivate the accounts. They contact the users, and they tell them that they may have been compromised and that this may have been part of some other event that may affect other accounts like their bank accounts, Facebook accounts and things like that. It is giving Canadians a proactive piece of advice that they need to look at their cyber-hygiene and that they need to take action.

With regard to the CRA accounts, there's a process for them to re-establish their accounts. They don't lose their accounts permanently. It's just that they have to reset their passwords and re-establish their identities.

I would leave it to Mr. Jones to talk about what other cyber-hygiene activities Canadians should take to protect themselves overall when this happens or just even as part of due course.

Mr. Scott Jones: Mr. Chair, I'll quickly add in on what Canadians can do.

The first thing is this: Don't reuse passwords on accounts that you really care about. In fact, don't reuse passwords. We recommend that Canadians use things like password managers, something that will autogenerate some random, complicated string of passwords.

For things that you really care about though, use unique passwords. Turn on multifactor authentication. That means asking it to send you a text message when you're logging in, logging in from a trusted device, or having one of those hard tokens, although most people won't use those because those are kind of hard to use. However, turn on something so that it verifies.

Security questions are not multifactor authentication. That information has been stolen, so don't count on that as a second factor. When we talk about that.... So, it's something you know: your password. It's something you are: in the physical world, a fingerprint or a picture or something like that. It's something you have. That's where we talk about your getting a text message on your phone that gives you a code to log in with for the next few minutes, etc. That's multifactor authentication.

Turning on those things already makes you a much harder target. Those are simple things you can do. I encourage every Canadian to go in and change the passwords for the things you care about, the things that can have harm to you as a citizen. Set it to a hard password—better yet, a pass phrase if its allowed—something that only you know, that only you can remember. If you're going to write it down, lock it away somewhere and hide it. Don't tape it under your keyboard. That's the first place anybody looks.

● (1650)

Mr. Francis Drouin: Great. Thank you.

Is this it, Mr. Chair?

The Chair: Yes, Mr. Drouin. Thank you very much.

We have heard some great questions and answers. I look at the time, recognizing that we have to go in camera. If we go into the next round, it would take us well past that point.

I'll remember not to put it under my keyboard anymore. I appreciate that.

With that said, I would like to thank the witnesses for being with us today—all five of you, although Mr. Jones, Mr. Perron, Mr. Brouillard did all the answering. We appreciate that. You did indicate that you might have to look up some further questions and respond to us. If you would do that and respond to the clerk with those answers, it would be greatly appreciated.

We go now from the public portion of this committee to the in camera portion meeting. When I suspend the meeting, the technical staff will end this part of the meeting in Zoom. This means that members cannot remain logged into this meeting. You will have to go out and then come back in using the pass code the clerk has sent to you.

I will suspend the meeting until we're back together in a couple of minutes.

[*Proceedings continue in camera*]