HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

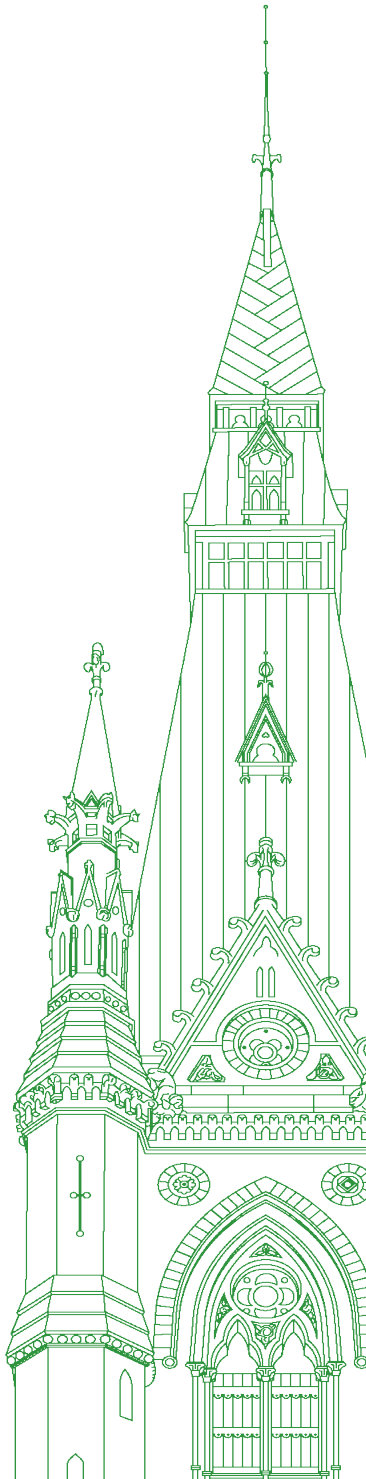
43rd PARLIAMENT, 1st SESSION

Standing Committee on Government Operations and Estimates

EVIDENCE

NUMBER 014

Monday, May 25, 2020



Chair: Mr. Tom Lukiwski

Standing Committee on Government Operations and Estimates

Monday, May 25, 2020

● (1700)

[*English*]

The Chair (Mr. Tom Lukiwski (Moose Jaw—Lake Centre—Lanigan, CPC)): I will call the meeting to order.

Welcome, colleagues. This is meeting number 14 of the Standing Committee on Government Operations and Estimates.

The meeting will last from 5 p.m. to 7 p.m., and the minister, I understand, will be with us for only the first hour. Her officials will be able to remain in the meeting until 7 p.m.

The committee's next meeting will take place this Friday from 11 a.m. to 1 p.m., eastern standard time. We have not yet received information about next week's meetings from the whips. As soon as we have that information we will be sending that out to all committee members directly.

I will go over a couple of the quick procedural and housekeeping matters.

We will go to a full complement of questions using the six-minute, five-minute, two and a half minute rule that we've established. That should give us adequate time to get all of the questions in, but we will be suspending, or at least excusing, Minister Murray at 6 p.m. sharp and then going on to a second full round of questions with the witnesses at that time.

I would ask that if you are making a statement or asking a question, you begin and please continue in one official language. I would ask that you do not alternate between French and English because we have had, over time, some technical difficulties when we've switched between the two. If we can do that, I think it would make for an easy facilitation and a much quicker meeting, because we won't have to worry about getting interrupted by our technicians.

With that, colleagues, I think you all know the drill.

Madam Minister, it's good to see you once again. The floor is yours for what I believe will be a five-minute opening statement.

Minister Murray, please go ahead.

Hon. Joyce Murray (Minister of Digital Government): Thanks so much, Mr. Chair. It's good to see everyone virtually.

I'm pleased to appear before this committee from my home in the traditional territory of the Coast Salish peoples. I'm joined today by Paul Glover, president of Shared Services Canada; Raj Thuppal, SSC, senior assistant deputy minister for networks, security and digital services; Marc Brouillard, acting chief information officer of Canada; and Scott Jones, head of the Canadian Centre for Cyber Security.

Mr. Chair and colleagues, as Minister of Digital Government, I'm leading the Government of Canada's digital transformation. My mandate is to provide public servants with the tools they need and to deliver the digital services Canadians expect. This transformation is critical for the government to keep pace digitally, and as the pandemic has shown, it's more important than ever that we have secure, reliable and easy-to-use digital services to make sure that no Canadian is left behind.

It has been about 10 weeks since our government took the unprecedented step of asking federal employees to work from home, and to support this, the digital teams right across government stepped up their efforts to ensure the public service could continue working safely and effectively, because our government's first priority is to continue serving Canadians.

I have been so impressed by the work of Shared Services Canada, the office of the chief information officer and the Canadian Digital Service have been doing to ramp up our digital capacities almost overnight. SSC has been working to maintain IT support for efficient and secure delivery of critical services as citizen needs escalate, and this in addition to supporting an unprecedented increase in public servants teleworking from their homes. I can't express enough the magnitude of this work and I thank all of the public servants who've been doing it.

SSC expanded networks, boosted services and provided equipment and tools so employees were able to continue to deliver critical services while working from home. They also enabled WiFi-calling so that employees could call and receive calls where there was poor cell service, and they increased departments' Internet capacity, in some cases up to 300%. They nearly doubled government's secure remote access capacity so that we can currently have up to 270,000 simultaneous remote connections. SSC also tripled the ability of the CRA to manage the flood of Canadians applying for the Canada emergency response benefit and the emergency student benefit.

The Canadian Digital Service has also been helping with digital responses right across government. They created a digital tool kit, helping departments recruit tech staff and access a library of open source code solutions—and how to use them—and helping citizens navigate the multiple benefits that are available and sign up for secure notifications about COVID-19 from Health Canada and other ministries.

The office of the CIO has been working across government to provide guidance on COVID-19 IT challenges, making sure that private sector offers of help are assessed and connected quickly with departments as well. To keep information safe, this office has helped all federal employees make telework more secure and provided best practices for using digital tools safely.

Disruption attracts cybersecurity challengers and we're very aware that increased and new uses of digital tools carry the risk of malicious cyber-activities. Cybersecurity is and will continue to be a high priority for our government as we safeguard Canadians from cyber-threats. Let me assure this committee that we are constantly monitoring, detecting and actively neutralizing cyber-threats, and that we coordinate events effectively through the Government of Canada cybersecurity event management plan.

Shared Services Canada has increased the overall security of the government through services such as perimeter defence, vulnerability management, supply chain integrity and an integrated cyber and IT security program to protect the infrastructure supporting departments and agencies.

To combat COVID-19 misinformation and fraud, the Canadian Centre for Cyber Security coordinated with industry partners to help remove thousands of fraudulent websites and email addresses that could have been used for malicious activity.

● (1705)

In conclusion, every crisis can be an opportunity to change for the better, and this pandemic is no different. In short order we have seen a move towards collaboration across all orders of government and industry. We've adopted digital solutions to unprecedented challenges at unprecedented speed, and we're doing it safely. I thank all our public servants for their Herculean efforts in this digital response.

Thank you. We'll be happy to now take your questions.

The Chair: Thank you very much.

We'll now go to Mr. Aboultaif, for six minutes, please.

Mr. Ziad Aboultaif (Edmonton Manning, CPC): Good afternoon, Minister. I hope you are keeping well with your family.

There was a story that came out showing hundreds of thousands of credentials being hacked from Zoom. There was a story also about Skype, some actual videos being stolen for external analysis where the users were unaware.

We've been using Zoom, as well as other methods such as Skype. How are we protecting sensitive information from being hacked or communicated over video chat? How are we making sure that sensitive information is not going into the wrong hands?

Hon. Joyce Murray: First, we understand that during a time of pandemic there are always those who look to take advantage of the crisis, and we're taking every precaution to ensure that Canadians and our systems are protected.

You refer to Zoom. In particular, I understand that the House of Commons is using zoom for virtual Parliament. It's widely known to be an insecure application, of course, but it is not used in the public service nor with Parliament for anything that is required to be confidential. It is only for matters that can be discussed and dealt with in the open that Zoom and that type of public tool are appropriate.

We have been providing guidance to public servants on what the appropriate tools are for which type of activity in supporting Canadians.

Mr. Ziad Aboultaif: Minister, a lot of public servants are working from home, from politicians to everyone else. Different departments are operating from homes and there is some sensitive information being exchanged back and forth.

Are you aware of any sensitive information being leaked, or have you received any complaints of any kind or any reports of such an incident?

Hon. Joyce Murray: Mr. Aboultaif, I'll ask my officials to add to my answer because they will have more information about details, but I am not aware of any breaches.

We have rapidly increased the capacity of the secure networks to be able to support the public servants working from home. In fact, before this pandemic emergency, an average number of secure remote connections at a single point in a day was about 40,000. We are now up to 200,000 such connections, which means that there was a very fast and very effective transition to public servants working from home through secure networks. There have also been secure cloud-to-ground networks created for other types of specific work.

It's an important question and I think the public servants have been doing a great job to protect the integrity—

● (1710)

Mr. Ziad Aboultaif: Minister, was any cybersecurity assessment done before we used Zoom, and since when has any Zoom application been used by the government in any capacity?

Hon. Joyce Murray: The answer is yes. Zoom is being used by government employees but only in circumstances where their communications are public, or can be public. For anything that is restricted or confidential, Zoom is not used. The chief information officer provides clear guidance on that, and again, I invite my officials to add.

I know in this format it's a little more difficult, but if there is anything they have to add, I welcome that.

Paul.

Mr. Paul Glover (President, Shared Services Canada): Thank you, Minister.

We have definitely done security assessments of all the different pieces of software to make sure their uses were appropriate. That is what translates into the guidance that the minister referenced, which the chief information officer then communicated to all departments.

We have provided departments with secure remote access so that their employees, when working from home, when they need that secure access, have that available to them. Because there were limits in the early days to the amount of bandwidth and secure remote connections, we also made unsecured channels available so that we could optimize the channels for what was secure and what was non-secure. We continue to do that every day.

Mr. Ziad Aboultaif: I have a quick question.

Definitely there were some breaches—I will verify—if I understood correctly the minister's aide. Was there any exchange of intelligence with other partners such as the Five Eyes, for example, on incidents happening to us or happening elsewhere within our allies?

The Chair: Please give a very brief answer.

Hon. Joyce Murray: We're continually monitoring, and yes, the Centre for Cyber Security, which my ministry is a partner in, works closely with the Five Eyes to identify threats.

The Chair: Thank you very much.

We'll now go to Mr. MacKinnon for six minutes, please.

[*Translation*]

Mr. Steven MacKinnon (Gatineau, Lib.): Thank you, Mr. Chair.

I'm delighted to see my colleague the minister and the people who are with her today.

I'm extremely proud of what these people have been able to accomplish in terms of resources, having visited Shared Services Canada. The progress we're seeing at Shared Services Canada is quite remarkable. So, Madam Minister, I want to acknowledge the success of the men and women at Shared Services Canada who have provided public servants with access to the secure networks and technological tools they needed to maintain services to citizens during this crisis. I know that Shared Services Canada has often been the target of criticism, but this time it is showing us the way forward. We are very proud of what these people have been able to accomplish.

[*English*]

I'm sure my colleagues don't always appreciate that we highlight the success stories here, Madam Minister, but I think it's important that the women and men of our public service are recognized for the incredible work they have done.

There's a lot of talk lately that everyone is going to be able to work from home. We'll be able to empty all of our downtowns and no one will ever have to go back to the office again.

Minister, you've been working very hard on technology-enabled workplaces. That's work that goes on with Public Services and Procurement Canada as well, with respect to enabling flexibility, enabling unassigned workplaces and enabling the kinds of workplaces that we're really going to need going forward, and doing so in part using technology. Maybe we could have the benefit of your thinking on that.

Hon. Joyce Murray: Thanks, Mr. MacKinnon.

There has been certainly commentary in the public about the emergency we've been responding to with so much increase in digital tools and secure digital tools, and how that will translate into changes post-COVID. We are certainly thinking about what might be a strategy for going forward post-COVID.

I think we've all been surprised, and pleasantly surprised, as you mentioned, by how quickly we as a government were able to continue to serve Canadians, and not just that, ramp up service. As we know, almost a million Canadians applied for the CERB on day one.

I see this as a continuum. From 2018's budget of over $2 billion over five years there has been a very concentrated effort to have a more integrated approach to our information storage use and our digital government. That was an SSC budget. There has been a half a billion dollars put into the whole arena of cybersecurity and the creation of a collaborative approach to cybersecurity, which is really serving us very well as a government right now. On some of those building blocks of addressing the old data centres and migrating them, I think about 40% have now been migrated to modern data centres and the cloud.

Some of these fundamental pieces that may have not been given the attention they deserved over the years have really been a key focus of this government, which is what the ministry of digital government is all about. It's to continue focusing on better serving Canadians. Really, what we know is that it just is not good enough if the only channels the public has to get service from their government is through downloading PDFs and faxing documents, or potentially standing in line and waiting to see someone.

● (1715)

Mr. Steven MacKinnon: We've moved it into the modern era.

I know Mr. Chair's going to cut me off very soon, but I just want to perhaps point out or even ask.... We've spent a lot of time doing things as basic as putting WiFi into the new GC workplace standard, so that public servants across departments can collaborate and come together in new, modern workplaces and are able to use technology to unleash creativity. That's going to be an important part of the mix going forward as well. I'm just wondering if you have any closing thoughts on that, if we have any time left.

The Chair: Unfortunately, we do not have any time left.

Mr. Steven MacKinnon: All right.

The Chair: Since there was an open-ended question, Minister, if you care to respond to Mr. MacKinnon, I would ask you to do so in writing as soon as possible and send that response to our clerk.

Hon. Joyce Murray: That's excellent.

[*Translation*]

The Chair: Ms. Vignola, you have the floor for six minutes.

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

Good evening, Ms. Murray.

Indeed, the pivot that employees performed in recent months has been dramatic. Nonetheless, we will have many questions in this regard.

On May 8, the Acting Chief Information Officer told the committee that there was ongoing monitoring of the federal government network by the Communications Security Establishment.

What are the greatest risks, the major threats, to the federal government network? How is the federal government mitigating these risks and threats?

[*English*]

Hon. Joyce Murray: Thank you for that question, Madame Vignola.

I think one key is that we have an integrated approach to threats. There may have been a previous day when each of the ministries had to deal with its cybersecurity threats. We have a very collaborative approach right now, and that's through the Canadian Centre for Cyber Security.

One example of how this works well is in the creation of the new benefits, which happened so quickly, for example the emergency response benefit. There are cybersecurity officials who are monitoring that application to make sure there are no vulnerabilities and there are no attacks that succeed in disrupting our service.

It's a very collaborative approach. Each of the ministries has a clear and separate responsibility with respect to preventing and responding to cybersecurity threats and attacks. I think it has been working very well.

● (1720)

[*Translation*]

Mrs. Julie Vignola: In your speech, you referred to fraudulent websites that were copying Government of Canada sites. How many of these websites have been detected? Were they all shut down?

[*English*]

Hon. Joyce Murray: I will ask the official from the Canadian Centre for Cyber Security, Scott Jones, to elaborate on that.

I would say that the monitoring and the very effective Government of Canada perimeter within which all of our secure government activities are placed and take place have resulted in a remarkable absence of real cyber-incidents over the past time period during COVID when so much activity is happening.

Scott, do you have something to add?

Mr. Scott Jones (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Yes. Thank you, Minister.

In general what we've done is that we've worked with commercial partners and with cyber-centres from around the world to take down anything that is impersonating the Government of Canada to try to dupe Canadians into taking some sort of online action. We've taken down hundreds of websites or malicious indicators, but we've also taught the commercial sector what the official CERB site, for example, looks like, so that they know and can recognize it and can take the malicious sites down on their own as well. That way they protect all Canadians quickly.

[*Translation*]

Mrs. Julie Vignola: Could you tell us how many victims there were before these sites were detected by your services?

[*English*]

Mr. Scott Jones: Unfortunately, because we look for the malicious activity, we don't look towards Canadians. The CSE Act precludes us from looking towards Canadians. We don't have a count of victims. We have to turn to our colleagues at the Canadian Anti-Fraud Centre, if a Canadian has reported it.

[*Translation*]

Mrs. Julie Vignola: Are there any teleworking public service employees whose computer systems have been targeted by a cyber attack?

[*English*]

Mr. Scott Jones: In general, the Government of Canada is targeted with approximately two billion malicious activities per day. A lot of that is purely reconnaissance, looking for any vulnerable service, but we're able to take action and we block those with our colleagues at Shared Services.

Yes, there continue to be attempts to target Government of Canada users. The extreme majority of those, greater than 99%, are blocked before any public servant even sees them.

[*Translation*]

Mrs. Julie Vignola: Among the 1% of cyber attacks that remain, have there been any consequences either on government data or on the personal data of Quebeckers and Canadians?

[*English*]

The Chair: Give a very brief answer, please, Mr. Jones.

Mr. Scott Jones: We have seen no breach of any government systems since the beginning of this event.

The Chair: Thank you very much.

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

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

I certainly appreciate having the opportunity to hear from the honourable minister today.

As you know, constituency offices across the country have been absolutely inundated with calls for every single government announcement, particularly as it relates to EI benefits and CERB, and certainly for small businesses it's the same, so I can appreciate the Herculean effort it must take to provide responses throughout the public service.

We've been hearing, though, from many people that they've had problems with the processing of their EI and CERB applications and cannot get in touch with an agent from the CRA or Service Canada. A constituent in my riding, Shannon Cooper, applied for EI leave on March 19 and is still waiting to receive her first payment. She has needed to call Service Canada to help sort out problems with her application. One of the biggest challenges she's facing is that when she's finally able to talk with an agent on the phone, her call gets dropped and the agent doesn't call her back. This has happened multiple times. She's now gone with close to 70 days without pay.

Given the IT infrastructure challenges that certainly all of government is facing, are you aware of this issue of calls being dropped by call centres?

● (1725)

Hon. Joyce Murray: Well, to be—

The Chair: Minister, before you attempt an answer, I would just remind Mr. Green to, again, try to keep his questions focused on the government's response to the COVID-19 pandemic. That is the frame of reference.

Mr. Matthew Green: Mr. Chair, respectfully, CERB applications are in direct response to COVID, and it's a very important question.

The Chair: It is an important question. I appreciate that. I'm just trying to make sure the precision of the question is there.

Please go ahead.

Mr. Matthew Green: It's rooted in CERB, so I assure you it's 100% related.

Hon. Joyce Murray: Thanks for that question.

Of course, because serving Canadians quickly, effectively and securely is a high priority for our government, I always regret to hear that somebody is having a challenge having an interaction with our government.

I can say that, through the work of the public servants of Canada to very quickly ramp up the capability to work from home, and even call centre employees who are working from home in some cases, it has been a unique circumstance. Given the millions of Canadians who have needed the government's help and the millions and millions who have received that help, I'm very proud of the work that has been done, but we will never stop trying to improve our systems and the infrastructure and the secure tools that are needed.

Mr. Matthew Green: I can appreciate that, and I would expect that and hope that, certainly from the government's perspective. However, in order to basically address these challenges that you're faced with, understanding that it's probably a function of old technology—and I'll let you comment on that in a moment—do you know exactly what percentage of calls are getting dropped? What type of evidence are you using to help improve the systems of IT?

Hon. Joyce Murray: Thank you for that question. I'm going to ask Paul Glover to answer.

Mr. Paul Glover: Thank you, Minister, and thank you, Chair, for the member's question.

Absolutely, we are aware of these issues and I'm pleased to report that the situation is improving each and every day. The number of calls that were being directed to ESDC and CRA by Canadians were literally unprecedented, so steps have been taken to improve the system's ability to handle the number of calls that are coming at it and route them quickly and properly through to agents.

We have been tracking the number of calls. It has improved quite substantially, and the number of calls being dropped now is very few.

Mr. Matthew Green: I like the generalities, but I would prefer the specific—

Mr. Paul Glover: Yesterday, there were none.

Mr. Matthew Green: There were none. No calls were dropped yesterday. Is that your assertion?

Mr. Paul Glover: With all respect, it would depend on the definition of “dropped”. There are busy signals where, because there is a limit to the technology and the number of calls, or how long the system knows an average call will take for somebody to be placed on hold, it gives them a busy signal, so they don't even get in. If we don't include those types of calls, for calls that entered the system and then were routed through, I'm not aware of any dropped calls in the last number of days.

Mr. Matthew Green: Just to close it out, in terms of the improvement you've identified, I'm very happy to hear that. I think our constituency offices might have a different anecdotal perspective.

Could you just give us a sense of, when this unprecedented wave happened for dropped calls until now, what it would have been at its peak?

Mr. Paul Glover: We'll provide that through the clerk. I don't want to estimate.

I do know that there have been a number of steps too. There were problems with calls that weren't dropped, but frankly, simply never got answered. That was another issue. People would get in and the call would never get dropped; it would just never get answered and the business would shut. The departments have been adding on. They've virtually doubled the number of agents they've brought on, so we've handled that.

The other thing, in addition to the dropped call issue, is that we tried to stand up more channels so that people can use voice response. They can still phone in, but rather than speaking to an agent, they can ask frequently asked questions, they can enter their information if they don't have access to a computer and they can still enrol in the benefit. We've expanded the number of channels, and that has also made an improvement.

We'll get you a full breakdown of the progress from the outset to where we are today.

● (1730)

Mr. Matthew Green: That's helpful.

Mr. Chair, thank you very much.

The Chair: Thank you very much.

We'll now go to our five-minute round of questions, starting once again with Mr. Aboultaif.

Mr. Ziad Aboultaif: Thank you again, Chair.

Minister, the federal government wants to help provinces build a framework for contact tracing through personal cellular devices. Is it safe to assume that this is pre-COVID, or after COVID?

Hon. Joyce Murray: This might be a question for the health minister, but I'll take a shot at it.

I think this is in response to COVID, and in response to the very important program of opening up our economy and enabling our businesses to continue serving Canadians. I think it is as we open up. Therefore, at that time, we need to be doing more contact tracing and more testing, and the federal government has offered to support the provinces, which are responsible for that.

Mr. Ziad Aboultaif: Speaking of which, we know there have been previous attempts by this specific government to invade the privacy of Canadians, specifically the incident of Statistics Canada and personal banking information, about half a million of these records being out without the knowledge of Canadians.

We know that our people, Canadians, are very concerned about their privacy and their private information being leaked. That's in addition to, obviously, their being under constant surveillance. They'd be under surveillance all the time.

Could there be, or will there be, any chance that the voluntary contact tracing initiative could be made mandatory, yes or no?

Hon. Joyce Murray: I can't comment on that. I can say—

Mr. Ziad Aboultaif: Minister, I appreciate that but it's your department. You're going to have to be doing the work at the end of the day.

Hon. Joyce Murray: I know we'll be providing any advice, guidance and support we can as digital government. The provinces are doing the testing and the tracing. Our federal government has offered funding to help them ramp that up and has offered the work of federal employees to do the hours of contact tracing. However, through the chief information officer and our other public servants, we oversee very strong policies and guidance on privacy and respecting individuals' privacy.

Mr. Ziad Aboultaif: Then you're not only supporting the provinces financially. You're also putting out guidelines or guidance as to how this is going to be done.

It's very important because Canadians are going to look at two things: They're going to look at their privacy, and they're going to look at the information that's needed by the government.

Between public safety and privacy, how are you going to cross that fine line?

Hon. Joyce Murray: We have guidelines and laws around privacy. For example, SSC has a privacy risk checklist and a requirement for privacy impact assessments in many cases for new infrastructure or initiatives. That would be SSC's initiative.

Government's collection, use and disclosure is subject to privacy notice statements and consent forms, consent for any data to be used for a purpose other than the one for which it was originally collected. We have strong rules and we will make sure that the appropriate ministries are aware of them.

Mr. Ziad Aboultaif: In light of this whole thing, since this is happening because of COVID-19, so that at least Canadians, and even policy-makers on the opposition side, can understand where the government is headed with this, when was the last legislation or policy put forward by the ministry?

● (1735)

Hon. Joyce Murray: I'll ask my official, the acting chief information officer, Marc Brouillard, to answer that question.

The Chair: Monsieur Brouillard, respond very briefly, if you could.

Mr. Marc Brouillard (Acting Chief Information Officer of Canada, Treasury Board Secretariat): I'm sorry. Is the question, when was the last time the privacy policy was updated?

Mr. Ziad Aboultaif: Yes.

Mr. Marc Brouillard: I don't have the exact date, but it has been a while.

I'm hoping to get that—

The Chair: Only because we're out of time, could you get the exact information that Mr. Aboultaif has asked for and submit it in writing to our clerk as soon as possible?

Mr. Marc Brouillard: I'd be happy to.

The Chair: We appreciate that very much.

Mr. Ziad Aboultaif: Thank you.

The Chair: We will now go to Mr. Weiler for five minutes, please.

Mr. Patrick Weiler (West Vancouver—Sunshine Coast—Sea to Sky Country, Lib.): Thank you, Mr. Chair.

Thank you, Minister and the other witnesses, for joining our committee today.

I also want to give a quick shout-out to all the employees who have been quickly able to shift from working in the office to working remotely and continue to deliver a high level of service in a really stretched time. It's also incredible and amazing to hear that there have been no breaches of cybersecurity for public sector employees during the pandemic.

Minister, first, what is the Government of Canada doing to protect the personal information of citizens in this increasingly digitally enabled government?

Hon. Joyce Murray: We were just talking about privacy, the government's privacy policy. Every public servant has training on the privacy policy and is aware of it.

Shared Services Canada has a very important role to play in the privacy of Canadians' data and personal information, because SSC is the main government infrastructure and storage of information. It's a very strong gatekeeper, actually, a custodian of the majority of this information. There are very clear guidelines for its staff on secure document use and storage, as well as an inventory of all personal information handled by SSC enterprise staff. They restrict and manage the collection, use, storage and disposal of data to respect the intended purpose and privacy laws. This is a high priority for us.

Paul, do you have anything to add?

Mr. Paul Glover: Thank you, Minister.

Just briefly, in addition to what you've said, any of the personnel who work in the data centres where this data is housed are subject to the appropriate security clearance. All the data centres are monitored. The data is encrypted, so even if we did look at it, we wouldn't be able to understand what we were looking at. You need the keys at both ends, so it is the departments that get that data back and are able to use it appropriately. We take that safeguard to make sure that anybody who handles it has the appropriate clearance, and that the data is always encrypted and only really available to those who need to see it when they need to see it.

Mr. Patrick Weiler: Thanks for that answer.

Next, how is cybersecurity addressed in the Government of Canada, including cyber-threats that might pose a risk to government infrastructure, or potentially, when they're aimed at private enterprise?

Hon. Joyce Murray: Cybersecurity is addressed in a very integrated way so that there is not a patchwork of approaches across the Government of Canada. This is essential to the success we've been hearing about from officials today in terms of reducing the vulnerabilities and the success of attacks. The Canadian Centre for Cyber Security is the core organization that provides the various aspects of being able to protect government networks and activities from being hacked or threatened.

The chief information officer branch, SSC and CSE, the Communications Security Establishment, are the triumvirate in what is a coordinated approach. They have written what is called the Government of Canada cybersecurity event management plan, so that when an event or an incident occurs, it is very clear who has what role in responding so that we can be effective as an organization right across the government.

I will ask whether Scott has other elements of that to add.

● (1740)

The Chair: Sir, you have about 30 seconds to respond.

Mr. Scott Jones: Thank you. I'll just add a bit more onto that.

The Government of Canada has multiple layers of defence that we use. Then we take everything we learn in defending the Government of Canada and make sure it's available to every Canadian business.

We've done that in many different ways. One is to give it to an organization called the Canadian Internet Registration Authority, so that every Canadian can benefit from something called Canadian Shield, which I'd be happy to talk about, but also to send out unique indicators of compromise that have never been seen anywhere else in the world because of the world-class defence we've been able to build for the government. We're making sure we're leveraging that to give it to all Canadians, including, of course, Canadian businesses.

The Chair: Thank you very much.

We'll go back to Mr. Aboultaif, for five minutes, please.

Mr. Ziad Aboultaif: The government operations committee once requested from the department.... The department on digital government indicated that 11% of the federal government's application portfolio is unused, basically.

Minister, can you tell us, in numbers, how many applications are unused, or haven't been assessed, as a better term?

Hon. Joyce Murray: If I could clarify, they haven't been assessed for what purpose, Mr. Aboultaif?

Mr. Ziad Aboultaif: For all purposes, for validity, for the benefits of it, and actually whether we need it or not.

You know and I know that there are still many of the digital centres that have either been shut down or are not being used. We've spoken about that before. I'm wondering, with regard to the software applications, how many software applications haven't been assessed yet.

Hon. Joyce Murray: Thanks for that question.

Software applications are owned by the departments that use them to provide their services. They are not part of the responsibility of digital government.

I can say that there are many, many applications, somewhere around 18,000 applications, and some of them are older. There's no question about that. We're working with all of the departments to encourage them to reduce the number and to consolidate their applications, as well as to use digital principles, so that we have an approach across government where we're working together and sharing applications that can be used for various departments.

Mr. Ziad Aboultaif: Do I understand that the 18,000 applications haven't been assessed? Is that correct?

Hon. Joyce Murray: I will ask Mr. Brouillard to comment on that question.

Mr. Marc Brouillard: Thank you, Minister.

The 18,000 number refers to the total inventory of applications in our application portfolio. Of those, we have an annual reporting exercise where departments report in on their status, their health, and as you mentioned, their technical validity. Out of that inventory, there are about 10% or 11% that aren't reported on. This could be because they've been closed and they're no longer in use, or it could be mistakes in reporting.

The other way of looking at it is that we have over 90% of applications reporting.

Mr. Ziad Aboultaif: The answer from the department shows that there are 7,363 software applications that haven't been assessed. That is based on the report that came out of your department. To clarify the record—at least to correct the records in place—the answer is that 7,363 software applications haven't been corrected.

This is showing that the digital infrastructure is collapsing. Is it a fair assessment to say that, because only 36% of the applications are in a healthy state and the rest are not?

Hon. Joyce Murray: Thanks for the question.

I would characterize our situation in Canada as doing a great deal of work to transform our government's Internet and telecommunications technology foundations to be able to serve Canadians better. There are many examples of where that's working. Yes, there are some legacy systems, data centres, as well as applications that pose challenges, and we are working in a very thorough and step-by-step way to address those issues.

● (1745)

Mr. Ziad Aboultaif: As mentioned, only 36% of those applications are in a healthy state. The 64% are not, which is basically two-thirds.

What is the timetable, Minister, that you're going to achieve, looking forward, to make sure that what we have is basically 100% healthy, to be able to operate properly?

The Chair: You have about 30 seconds, Minister.

Hon. Joyce Murray: I'll ask Mr. Brouillard to respond to that.

Mr. Marc Brouillard: Thank you, Minister.

The importance is not to.... We do not have a timetable for the whole application, but it is to focus on modernizing those applications of the highest criticality and the highest business value to government, and that is what we're doing. We have plans to look at those applications and migrate them to either end-state data centres or cloud.

The Chair: Thank you very much.

We'll now go to our last five-minute intervention.

Mr. Kusmierczyk, you have five minutes, please.

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

Just to pick up on the line of questioning of my colleague, according to the SSC's 2020-21 departmental plan, nearly 80% of the federal government's roughly 18,000 applications reside in aging and unreliable data centres that are at risk of service outages and failures, and it will prioritize moving these applications to the cloud or enterprise data centres.

I just wanted to know whether the COVID crisis has accelerated this process. Are there also advantages to moving to the cloud in terms of cybersecurity? Maybe we'll just begin with those two questions to start.

Hon. Joyce Murray: There certainly are advantages to moving to the cloud. I would say security is a big one, but also cost-effectiveness.

I will ask Paul Glover of Shared Services Canada to comment on whether that initiative, that migration of data centres, which our government funded several years ago and is well under way, has continued during the last three months while we have had to really focus on emergency answers to millions of Canadians in a way that hadn't been anticipated.

Mr. Paul Glover: Thank you, Minister.

Without a doubt, that work has continued. It's really important. Some of the buildings were at their end of life. We needed to get the data centres out of there and into what we call modern end-state data centres. We continue to work very hard. In the last two years we've exceeded our targets—120% last year, and over 100% of target this year. Just about 100 data centres were closed this past year.

We continue to significantly reduce the number of data centres that we're closing, but the goal isn't just to shut data centres. As you say, it's the applications that reside in them and making sure that we have robust strategies so that those applications can continue to operate. We're doing that. We're moving them to more modern data centres. We're making sure that when we can't get to them, we're replacing hardware so that they no longer have the same risks. Not all of them need to be moved. For some of them, it's just a good bit of maintenance and upgrades to make sure they're functional.

With respect to cloud, absolutely, we've seen an acceleration because it's about speed and scale. To some of the comments about call centres earlier, when you go from a few thousand calls to hundreds of thousands of calls a minute, you need to be able to scale up very quickly. Cloud provides the ability to do that.

We're very pleased to report that, through the co-operation of the CSE and the policy direction of the CIO, we're ensuring that the journey to cloud is safe for Canadians and for the government. We have a secure channel to cloud, so that when applications do exist in the cloud, the network and the path there is secure.

All of our cloud contracts are protected. That includes things like the Patriot Act and others, where all the cloud data centres are on Canadian soil for departments to be able to use for protected information. The work has accelerated, and we are ensuring that it is done in a very secure and safe manner.

● (1750)

Mr. Irek Kusmierczyk: Thank you very much for that very detailed response.

Just to follow up on that, I'm wondering whether the federal government has experienced fewer cybersecurity incidents affecting applications that are already in the cloud.

Mr. Paul Glover: I would repeat what Scott Jones has said. Our perimeter is really world-class and is the envy of many other nations. It is constantly blocking threats, so to say there are none.... There are literally billions every day, but they don't get through. Even in those exceptionally rare cases where they do get through, they're spotted very quickly and contained. Services are shut down, brought offline and unplugged before any damage can be done. There were literally no incidents in the last 10 weeks that I can think of where there has been any data breaches at all. There are incident blocks every day, but none of consequence.

Hon. Joyce Murray: Could I just add—

The Chair: Very briefly, Minister, please....

Hon. Joyce Murray: Okay.

For those who are listening or watching, as well as our members, there is access to a free version of CIRA's Canadian Shield firewall. That's for small businesses, but also for individual Canadians. That is drawing on the experience and expertise of the combined team through the cybersecurity initiatives in the Government of Canada.

The Chair: Thank you so much.

We'll now go to our two and a half minute interventions, starting with Monsieur Barsalou-Duval.

[*Translation*]

Mr. Xavier Barsalou-Duval (Pierre-Boucher—Les Patriotes—Verchères, BQ): Thank you very much, Mr. Chair.

Earlier, I heard repeatedly that since the beginning of the COVID-19 pandemic, when people were encouraged to work from home, there have been no security problems, no intrusions and no data leaks regarding our officials. The same would seem to be true for House of Commons staff.

However, I've also heard that in the majority of cases where there are leaks, data leaks or espionage, for example, people are not aware of it or don't notice it.

How do you know there wasn't one, when people rarely notice?

[*English*]

Hon. Joyce Murray: Thank you for that question.

What we do know is that it was a high priority for us to be able to serve Canadians and to provide the tools so that our public services could do that and do it safely within the perimeter of the Government of Canada's security perimeter. It has been very successful.

We're also clear on what activities have to happen through secure channels and which ones can happen through other public tools like Zoom. I will ask Mr. Glover to explain how we—

[*Translation*]

Mr. Xavier Barsalou-Duval: So you can't guarantee that there have been no leaks, data leaks, espionage or anything like that.

[*English*]

Mr. Paul Glover: I will turn to Scott from the CSE to round out this answer, but the reason we can say this is that we have tools that monitor the traffic, so we're able to understand, and these tools are intelligent, using artificial and other things—the firewalls—to both block and monitor what's happening. If traffic is getting redirected and is inappropriate as flagged, we would be able to see that and stop that.

Scott.

The Chair: Mr. Jones, I know that you're going to be sticking around for another hour. Perhaps you can expand upon the answer you were about to give, but we're completely out of time, unfortunately.

We'll go to our final intervention.

Mr. Green, you have two and a half minutes, please.

Mr. Matthew Green: Thank you, Mr. Chair.

In its digital operations strategic plan 2018-22, the federal government recognized the need to modernize its aging at-risk IT infrastructure and systems. It also indicated that its “IT systems and assets that have been in service beyond their normal useful life will fail to meet the current and emerging requirements for the delivery of timely and critical services and information to Canadians”.

For the minister, in your mandate letter, the Prime Minister asked you to identify “all core and at-risk IT systems and platforms”. Has the federal government modernized its at-risk infrastructure and systems since the beginning of the pandemic? If so, what is the estimated cost of updating all identified core and at-risk IT systems and platforms?

● (1755)

Hon. Joyce Murray: Thank you.

That's a pretty big task that you just laid out there. This is something that is being done over the course of a number of years. Shared Services Canada was assigned $2.2 billion in the 2018 budget, and there have been other budget amounts since then.

I will ask Marc, who is the acting CIO, to continue with the details for that question.

Mr. Marc Brouillard: Thank you, Minister.

As you mentioned, Minister, in budget 2018, funds were allocated to modernize, and that included an application modernization fund of $110 million that was designed to support departments in taking their legacy applications and moving them into modern cloud infrastructures. At the same time, that's the right opportunity to look at their digital processes and to look at improving the way they deliver those services.

Identification of core services is ongoing. There's an inventory of the critical systems that require those modernizations, and we're continuing to work with departments on supporting those initiatives.

Mr. Matthew Green: Thank you, Mr. Chair.

The Chair: Thank you very much.

Minister, that ends our first round of questions. We want to thank you very much for your appearance here today. I can safely say that I suspect when you signed up for this job as Minister of Digital Services you didn't think, nor did any of us, that the situation we see today, in which we're living in a virtual world, would be upon you and your officials. Thank you for being here. We appreciate your appearance. Good luck to you. I hope you stay healthy and safe.

Hon. Joyce Murray: Thank you.

The Chair: Colleagues, we will not suspend. I will excuse the minister, however.

We will go directly into our second hour. We have with us the head of the Communications Security Establishment, Mr. Scott Jones. He has a brief, five-minute opening statement.

Mr. Jones, I'd ask you to deliver that statement now.

Mr. Scott Jones: Thank you, Mr. Chair, and thank you for having me continue to appear before you today.

I am the head of the Canadian Centre for Cyber Security within the Communications Security Establishment. We are one of Canada's key intelligence agencies and the country's lead technical and operational agency for cybersecurity. We report to the Minister of National Defence.

CSE continues to leverage all aspects of our mandate to ensure that Canada is protected against cyber-threats and that the Government of Canada has access to information that can help inform decisions on Canada's approach to COVID-19.

In October 2018, the cyber centre was launched as a unified source of expert advice, guidance, services and support on cybersecurity operational matters, providing Canadian citizens and businesses with a clear and trusted place to turn for cybersecurity advice. The COVID-19 pandemic has required us all to make changes to our daily routines and has impacted the way we work and communicate with one another.

During these uncertain times, cyber-threat actors are attempting to take advantage of Canadians' heightened levels of concern and fear around COVID-19. Many Canadians are naturally feeling fearful and stressed, and those strong emotional responses can be exploited online. We've seen an increase in reports of malicious actors using COVID-19 in phishing campaigns and malware scams.

I would like to provide you with an update on the work the cyber centre is doing to protect Canadians, systems of importance, the House of Commons and the Government of Canada from cyber-fraud occurring before, during and after the pandemic.

First, to protect Canadians we continue to leverage all of our mandate to help ensure that Canada is protected against threats. The cyber centre is working tirelessly to continuously raise public awareness of cyber-threats to Canadian health organizations by proactively issuing cyber-threat alerts and providing tailored advice and guidance to Canadian health organizations, government partners and industry stakeholders.

In addition to our advice and guidance for Canadian organizations, we continue to enhance the Get Cyber Safe public awareness campaign to help every Canadian take action to help themselves be safe online. In coordination with industry partners and the international network of cybersecurity organizations, we have contributed to the removal of fraudulent sites and other materials used to lure Canadians, including sites impersonating the Government of Canada as I mentioned before.

As many people and organizations have shifted to working and learning from home due to COVID-19, their personal devices and home networks have become more attractive targets for cyber-threat actors. Cyber-attackers are looking to exploit teleworking connections, because so many people are now working outside their organizations' IT security perimeters and they needed to quickly shift.

In response, we have partnered with the Canadian Internet Registration Authority, CIRA, to create and launch the CIRA Canadian Shield. The minister gave a great description of what CIRA is, and I would like to take this opportunity to thank CIRA for their tremendous leadership in giving Canadians an option to better protect themselves online. They are terrific partners.

To further protect Canadians, the next important step we've taken is informing them about cybersecurity matters. Through targeted advice and guidance, we're helping to protect Canadians' cybersecurity interests. We've shared security tips on video teleconference tools and telework to help inform and educate Canadians so they can make good decisions about staying safe online.

We've created a collection of advice and guidance products, many of which are more relevant than ever. I encourage Canadians to visit our website to learn more about our specific guidelines and best practices that can be applied to protect themselves.

We have taken action to protect programs of importance to the government, including monitoring and protecting important Government of Canada programs, such as the Canada emergency response benefit web application, which you heard Mr. Glover talk about earlier.

As well, we have continued to evaluate cloud applications, including for the Public Health Agency of Canada, and enabled cybersecurity monitoring and defence for cloud usage across the government. The cyber centre has continued to collaborate with the Canadian Anti-Fraud Centre operated by the RCMP, the Ontario Provincial Police and the Competition Bureau, which are Canada's trusted sources for reporting and mitigating mass-marketing fraud.

I'm also happy to mention that the cyber centre has a long-standing partnership with the House of Commons. As Parliament has shifted to virtual meetings, we are working alongside the House of Commons by providing tailored advice and guidance, including working to support virtual sittings and committee meetings. The cyber centre's shared advice and guidance have helped you and all members make informed decisions when selecting, installing and using video teleconferencing tools. We are very proud to be supporting Parliament and the continuation of open parliamentary proceedings.

Finally, it is important to note that the Government of Canada has a strong and valuable relationship with our international cyber partners. We regularly share information, which has a significant impact on protecting our respective countries' safety and security. I want to reassure Canadians that CSE and the cyber centre continue to work hard to mitigate these threats and protect Canadians.

Thank you very much, Mr. Chair.

● (1800)

The Chair: Thank you, Mr. Jones.

We'll now go into our six-minute round of interventions, starting with Mr. McCauley.

Mr. Kelly McCauley (Edmonton West, CPC): Thank you, Mr. Chair.

Mr. Brouillard, welcome. I'll start with you. Most of this is going to be around access to information.

How are we updating the guidelines for employees on Government of Canada information management?

Mr. Marc Brouillard: You mean in terms of the new working conditions, working from—

Mr. Kelly McCauley: Of course, yes.

Mr. Marc Brouillard: We've reiterated to all Government of Canada employees that they have the responsibility to ensure that for any information of business value on GC equipment that is worked on from home, there's no issue with—

Mr. Kelly McCauley: Right, but are we doing anything besides reiterating to them?

Mr. Marc Brouillard: We are reminding them that they have the responsibility and that, again, any public infrastructure, like Zoom or other collaboration sites, is for unclassified material only.

Mr. Kelly McCauley: Okay.

The directive on record-keeping outlines effective record-keeping practices that enable departments to manage and protect the integrity of information.

If we have so many people working from home now, what are we changing, one, to protect that information, and two, to make sure it is available for ATIPs?

Mr. Marc Brouillard: We're providing the guidance that if GC employees are providing critical services, they still have access to the networks and to those tools. For users who are not—and we're sometimes asking them to either connect to the networks after hours or sporadically—we remind them that they still have the responsibility to get records of business value back into those systems.

There's a bit of tolerance for delays because they may not be able to connect to the network at all times. However, they're working on secure, government-furnished equipment from home, and they're still able to connect when possible.

Mr. Kelly McCauley: Okay.

The ATIP process has been put on hold. Obviously people are working at home. When are we going to see it reopen so that the public, politicians, etc., can start getting answers to access to information requests?

Mr. Marc Brouillard: I don't believe the process has been put entirely on hold.

Again—

Mr. Kelly McCauley: It has been, yes.

Mr. Marc Brouillard: Is it completely on hold? Okay.

Mr. Kelly McCauley: I would challenge you to find a single response in the last two months.

Mr. Marc Brouillard: I would have to check on that.

Certainly there are allowances for the fact that people don't have access to their offices, so they may not be able to do the same type of research that they would from internal—

● (1805)

Mr. Kelly McCauley: Are we developing a plan to address this? We can't just sit and say we can't access it forever. Are we developing a plan, or are we doing a wait-and-see to see how COVID bears out?

Mr. Marc Brouillard: We are working with the office of the chief human resources officer to start planning on the resumption, the return to the workplace. As part of that, we expect there's a backlog of activities, things potentially like ATIP, where they will have to be addressed on a priority basis. Those plans are in the process of being developed.

Mr. Kelly McCauley: The Information Commissioner, Ms. Maynard, has been very critical—I guess that would be a polite word—of the government's handling of transparency right now. She put on her website, "institutions are reminded that they must continue to properly document their decisions as well as their decision-making process in accordance with the Policy on Information Management."

How are we ensuring that's done, besides saying they're using government servers?

Mr. Marc Brouillard: That guidance is provided to departments. It is up to the departments to ensure it's being followed and to make sure the documents that are critical to recording the decisions—

Mr. Kelly McCauley: The CIO of Treasury Board is the overseer. Is this another example of, "Well, that's the departments, and if they fail, that's too bad"?

Mr. Marc Brouillard: I wouldn't say that it's too bad. I think it's the responsibility of the departments and the deputies to follow the policies that are put out by Treasury Board.

Mr. Kelly McCauley: Right, but what is Treasury Board doing to follow up to make sure this is being done? That's my concern.

Mr. Marc Brouillard: I appreciate that.

We do have active reviews of compliance and annual reporting, to report back to....

Mr. Kelly McCauley: Are we ramping up these active reviews, considering nothing is going on ATIP-wise and there's this very real concern, as expressed by the Information Commissioner?

Mr. Marc Brouillard: Right now the activity is focused on understanding where departments need support and providing that capability, making sure that the operational priorities come first.

Mr. Kelly McCauley: What's your confidence level that the policy and information management is going to be followed?

Mr. Marc Brouillard: Fairly high, as I think everyone is aware of their importance. We've had an amount of collaboration and communications in the community that we've never seen before, so it's not that people are not aware of this, and there's an honest desire to make it work.

Mr. Kelly McCauley: Thanks.

I have just a last question on that. She lists tips on her website, the nine email tips for maintaining information. Have you rolled that out to the departments, or are you just waiting for departments to look at her website on their own?

Again, Treasury Board is responsible for this. If you let it go.... We've seen this repeatedly from Treasury Board on human resources, whistle-blowing and departmental plans. Treasury Board is responsible but always says that it's the departments, and then nothing gets done.

Mr. Marc Brouillard: I haven't personally—

The Chair: Mr. Brouillard, I'm going to ask you to provide that answer—in writing, as I've mentioned before—to the clerk as soon as possible. I'm sure you want to give a fulsome answer to Mr. McCauley's question. I'll give you the opportunity to do so as quickly as possible, sir.

We will now go to our second round of questions, for six minutes again.

Mr. Jowhari.

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

Welcome to all of our witnesses and thank you for the information you've provided so far.

My question is for Mr. Brouillard. A lot of my colleagues have taken an approach where they've gone to one of the specific what I call pillars or building blocks of our digital strategy or digital government, whether it's cybersecurity or aging infrastructure, etc. For the benefit of the many Canadians who are watching, could you take a step back and very briefly demystify our government's digital strategy into four or five key pillars?

Give us an idea of where we were on the path of delivering our mandate before COVID-19, and what the impact of COVID-19 has been on our mandate and our being able to deliver. I'll ask some follow-up questions after that.

Mr. Marc Brouillard: I'm sorry. You're asking in relation to COVID-19 what is the digital...?

Mr. Majid Jowhari: Before COVID-19, there was a mandate. There is a mandate letter for the minister. For you as the CIO, what would you identify as the key building block of our government's digital strategy?

● (1810)

Mr. Marc Brouillard: Okay. That's a bit of a complex answer. I'll try to break it down.

There are various components to the Government of Canada, and all of those components need to be moving forward. Paul Glover can speak more to this, but on the modernization of the infrastructure to support the requirements to connect, we live in an interconnected world. We have to have networks that are efficient and able to talk amongst themselves. Cybersecurity, the topic of today, is an absolutely critical strategic imperative. We must ensure that the information entrusted to us by Canadians is held securely and properly treated.

On information management, again, it's about making sure that the privacy of Canadians is properly entrusted, but at the same time, supporting open government initiatives and making sure that the information that can be made available to Canadians is made available through the open government initiative.

Then we get into the applications and the service delivery and ensuring that those are developed and designed in modern ways, with the digital standards and principles in mind, the first of which being that it's user first, user-centric. If we aren't designing our services with the end-user—Canadians or Canadian businesses—in mind....

Mr. Majid Jowhari: Perfect. That's exactly what I was hoping for. I was hoping that you'd go in and demystify those different building blocks.

Then we have COVID-19. Naturally, that has impacted our strategy or our road map to deliver what we had committed to. Can you quickly talk about the overall impact on our ability to deliver? Where have we had the highest impact?

Mr. Marc Brouillard: Internally, the work that Shared Services has done has been incredible in shifting the entire network configuration from one that is centred on people sitting in buildings talking to the outside to everyone sitting at home talking to the inside. The minister and Mr. Glover talked a bit about the actions that were taken. That was the first pivot.

The second pivot was very clearly the benefits to Canadians and the work that CRA and ESDC did to deploy the Canadian emergency relief benefit as well as others, the wages and things like that. Those were—

Mr. Majid Jowhari: I'm sorry to interrupt. Very quickly, where do you think our vulnerabilities are going forward, based on the original strategy we had?

Mr. Marc Brouillard: I'm not sure I understand. The vulnerabilities in response to...?

Mr. Majid Jowhari: It's our response to our ability to deliver our mandate because of the impact of COVID-19.

Mr. Marc Brouillard: Right. I think that it isn't necessarily a vulnerability, rather than a shift—

Mr. Majid Jowhari: It's a risk area.

Mr. Marc Brouillard: It's also a shift in priorities, and there's a natural reason for that. I think those reasons are valid. As we start to plan for the resumption of business and a return to the workplace, going back to those original priorities pre-COVID is going to be the next focus.

Mr. Majid Jowhari: Give me one of the priorities that we have to pay special attention to as we are ramping up and opening up the economy.

Mr. Marc Brouillard: I think that's a bit out of my wheelhouse, because I'm focused more on the internals of government operations.

Mr. Majid Jowhari: Yes, I realize that, but as an internal government we are supporting those initiatives.

Mr. Marc Brouillard: Absolutely. Ensuring that the departments responsible for that have the infrastructure required to deliver those services is a key priority. That's absolutely what we're focusing on.

Mr. Majid Jowhari: I have 30 seconds left. Do we have the capital resources and the funding to be able to deliver that? If not, where should we focus on getting those resources?

The Chair: Give a very short answer, please.

Mr. Marc Brouillard: The short answer is that it's part of the planning process and the prioritization that we have to look at as we move forward.

Mr. Majid Jowhari: Thank you.

The Chair: Thank you very much.

[*Translation*]

Ms. Vignola, you have the floor for six minutes.

Mrs. Julie Vignola: Excuse me. The interpretation was cut off, so I didn't hear everything.

In the departmental plan, Shared Services Canada noted that computer-related threats were constant. Earlier, it was said that there are 2 billion daily attacks against various government services. At least that's what I heard.

First, what resources does Shared Services Canada have to prevent these attacks?

Second, is there collaboration with other police services, such as the SQ?

Third, where are these attacks coming from? Are they coming from internal sources in Canada or from external sources?

I'll stop with three questions. I'll see later about the rest.

My questions are for either Mr. Brouillard or Mr. Jones.

● (1815)

[*English*]

Mr. Scott Jones: Maybe I'll answer the general cybersecurity questions first.

On the first aspect in terms of where they come from, they come from all around the world. This is typical for cyber-actors. There is no unique location.

What we really look at is how to take care of any of the malicious activity rather than the individuals behind it. We work with our colleagues in law enforcement. Certainly, we do work with law enforcement from across the country, including the Sûreté du Québec, and with our partners in the RCMP as well, to make sure that we're trying to address these things.

Primarily, we let law enforcement do their job and we respond to ours, which is to really try to enhance the safety of Canadians in terms of giving them advice on how to protect themselves, and we really hope that our colleagues in law enforcement.... We try to get as much information as we can so they can do their jobs to go after the criminals at the other end of malicious cyber-activities.

Paul.

Mr. Paul Glover: Thanks, Scott.

In response to the question about the resources that Shared Services needs, there are a number of things. It's access to expertise, such as the Canadian Centre for Cyber Security, which is constantly monitoring those things. It's access to technology in the networks and in the data centres.

It's a range of things that work together to make sure of this, including, frankly, the physical layouts of buildings. Oftentimes you need to take a look at internal threats. For example, at the data centres, we make sure that, for people going in and out, it's all properly logged and captured. The ability to remove hardware is something that is deeply and tightly controlled.

It is definitely multi-faceted. We look at threats from all angles. We rely on a lot of the policy, direction and expertise from our colleagues elsewhere, and then work to ensure that we apply best practices to put that into the systems overall, from the desktop through the network to the end data centre, and at every step along the way.

[*Translation*]

Mrs. Julie Vignola: Earlier, we talked about applications. There's a whole host of them and rumours are rife. Some companies would like to have applications to monitor their employees, for example to calculate the number of clicks, the sites they have visited, and so on.

Does the Government of Canada currently use this type of application for its own employees who telework?

[*English*]

Mr. Paul Glover: I'll take a first shot at the member's question.

We do not monitor how long they're on. Those are issues that the department deals with. What we do monitor is the type of traffic, the nature of it from a security point of view, to make sure they're visiting appropriate sites, the nature of the activity. It is at a very depersonalized level. Often, it's not an individual. It's firewalls. It's artificial intelligence, and looking at those things.

It's not exactly the same as individual companies trying to time-track their employees and what they're doing. It's purely from a security.... It's the nature of the communications, the nature of the exchange, to make sure there have been no compromises or threats.

[*Translation*]

Mrs. Julie Vignola: Thank you.

Among other things, there was talk of increased bandwidth, new computers, new structures, microphones and cyber security. To date, what is the impact of these new needs on budgets?

● (1820)

[*English*]

The Chair: Please give about a 30-second answer, if that's possible.

Mr. Paul Glover: Sure.

It's been about $58 million all told. That's tablets and equipment to help people work at home, network upgrades, secure remote access points, specialized equipment and hardware to deal with the volumes of Canadians trying to access new benefits, and increased storage costs and computing costs to deal with those unprecedented volumes. It's everything end to end.

The Chair: Thank you very much.

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

Mr. Matthew Green: Thank you.

It's certainly not every day that you get to put questions to the Communications Security Establishment, so I'm going to go ahead and take that opportunity today, Mr. Chair, through you to Mr. Jones.

In 2018, the federal government launched the cyber centre as a part of the CSE by consolidating cybersecurity expertise from the CSE, Public Safety and the SSC. How many employees work for the cyber centre?

Mr. Scott Jones: Thank you for the question.

At this time we have about 800 employees spread across the traditional mandate of CSE—which was the cryptographic expertise that we brought—the Government of Canada security operations centre, plus the national CERT as well.

Mr. Matthew Green: How many of them came from Public Safety and SSC respectively?

Mr. Scott Jones: Approximately 150 positions were transferred.

Mr. Matthew Green: How were they selected?

Mr. Scott Jones: They were the people doing the functions that existed in those departments. Both departments transferred folks. We integrated them and designed a brand new cyber centre.

Mr. Matthew Green: Thank you.

According to a media report, the CSE is working in coordination with its partners to ensure that COVID-19-related phishing sites mimicking the Government of Canada are removed. Who are those partners?

Mr. Scott Jones: We work with partners around the world in the international cybersecurity community. When we see malicious activity hitting our country, for example, we can make a request to a national computer emergency response team in any other country. We also have contracted to commercial partners. We typically don't give the name of the partners because we don't endorse companies. We have a contractual relationship, but because we also can give them a reputational boost, it tends to be something we're very careful about.

Mr. Matthew Green: That's very well stated. Thank you.

Could you provide some further examples of how the CSE's cybersecurity work is related to COVID-19?

Mr. Scott Jones: Absolutely.

I've already talked about the example of taking down fraudulent websites and working with partners there. In another case, we've also issued many alerts directly to the health care sector. We have cross-sector tables where we've worked with Canadian industry on COVID-19 and the response. These include communications and technology, the health sectors and our provincial and territorial partners, to make sure that we're sharing as much information as possible.

In fact, we've hit all the major critical infrastructure sectors. At the height of this crisis, when this was first starting and everybody was getting on their feet, we had multiple calls a week and directed information to them constantly.

Mr. Matthew Green: This might seem like a frivolous question, but I'm going to ask it anyway because fraud is a concern of mine. It might not be in your portfolio. Are new technologies in place that enable us to better target the old-school phishing scams through telephones, i.e., even as a member of Parliament, I continue to get CRA calls on my government phone that I'm about to go to jail unless I send them money right away.

Are there ways we can fight back against that type of traditional phone scam?

Mr. Scott Jones: I get those same calls as well.

Mr. Matthew Green: That must be interesting. Do you let them know where you work?

Mr. Scott Jones: Sometimes, if I have a lot of time, I'll try to keep them occupied so at least if they spend time with me they don't spend time on another Canadian. In general, this is where I would look to the work that the CRTC and some of our telecommunication partners have been doing to try to deal with this. The problem is that the international telephone system is working off standards written in 1975 in some cases. It's not designed to have security in mind. It was designed for a very few monopolistic telephone operators who were all trusted, so they're trying to adapt to this. That's a challenge we're facing.

We are trying to support them and work with them through some of our collaboration tables, but it is a pretty significant challenge because of the environment, unfortunately.

● (1825)

Mr. Matthew Green: Thank you.

That concludes my questions. I won't take up time for the sake of taking up time, Mr. Chair.

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

Now we'll go to five-minute rounds, and we'll start with Madam Block.

Mrs. Kelly Block (Carlton Trail—Eagle Creek, CPC): Thank you very much, Mr. Chair.

Thank you also to our witnesses for joining us today.

As you noted in your opening remarks, Mr. Jones, these are extraordinary times, which have required us to change the way we work and communicate. While we have risen to the challenge, I believe it is more important than ever that we secure critical infrastructure as we shift government operations to digital and telework.

Also in your opening remarks, Mr. Jones, you noted that the Government of Canada has a strong and valuable relationship with our international cyber partners, and that we regularly share information, which has a significant impact on protecting "our respective countries' safety and security". Maybe this segues just a bit into the answer that you just provided to my colleague Mr. Green.

According to an article in The Telegraph on Saturday, the Prime Minister of the United Kingdom announced that he will reduce Huawei's role in Britain's 5G network in the wake of the coronavirus outbreak. If Huawei is a part of Canada's 5G network, will it pose a security risk to Canadians?

Mr. Scott Jones: It's important to note that right now there's an ongoing security review led by the Minister of Public Safety. We're certainly supporting the cybersecurity elements of that, and we take all the information we have into account. Certainly, something we face is how to secure any network. One of the really important concepts is that we should have zero trust in any equipment we're using. That's the same structure we've taken with the Government of Canada, where we've tried to build in multiple layers of defence. You always assume that a layer is not going to be able to protect it and you add another layer of defence, so that there's always a belt and suspenders or a check and balance, depending on how you want to describe it, so that we can layer security in place.

Then ultimately, some of the other decisions will need to be taken as part of the policy.

Mrs. Kelly Block: Thank you.

Other Five Eyes partners have already made a decision on Huawei and their 5G networks. Is there something different about Canada that dictates why we have not made a decision yet?

Mr. Scott Jones: We've been working to look at this to provide the cybersecurity advice as part of the broader, ongoing review. One of the key aspects for us is leveraging our experience since 2013 of running a cybersecurity review program, which was about building better security with our telecommunications partners from the start. We've been trying to leverage that experience, but provide a definitive and strong source of information to the government to make a decision.

Mrs. Kelly Block: From your perspective, would it even be possible for Canada to make a decision right now on Huawei's involvement with our 5G networks?

Mr. Scott Jones: The 5G standards are evolving. One of the key things for us is making sure that regardless of vendors—no matter where those vendors come from in the world—we're building in security that is agnostic of origin. It's a complicated supply chain for all vendors, and one of the key things for us is ensuring that we're positioning Canada to be protected, regardless of the vendor, wherever Canadians are located, making sure we're building those relationships and security elements in from the start.

Mrs. Kelly Block: I appreciate what you said about always considering that a network is vulnerable.

Is Huawei considered a higher risk vendor when it comes to a 5G network?

Mr. Scott Jones: One of the things we always look for is how products are being built, where they're being built, how they're being assembled, the origin of their components, the ownership of their companies, etc., and that's for any product.

We apply that expertise as part of something you heard talked about earlier today: supply chain integrity. We apply that expertise there, as well. We add on extra mitigation, extra risk-reduction activities, depending on those different factors, to try to bring the level of risk down to an acceptable level.

One of the key things in my job is that you can never fully sleep well at night, because there's always risk that remains. The only way to really reduce your risk down to zero on the Internet and communications is to shut it all off. That's obviously just not viable.

● (1830)

The Chair: Thank you very much.

We will now go to Monsieur Drouin, for five minutes, please.

Mr. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Thank you, Mr. Chair, and through you, I will be asking my questions to Mr. Glover.

I recall almost 10 years ago, 2013 I believe, it was Marissa Mayer, when the whole debate about working from home versus not working at home.... That Yahoo CEO said, "I'm bringing back all the employees to work and nobody is working from home."

In our case, I know that some employees were able to work from home, but now COVID-19 has hit and everybody must work from home. Can you talk to me about ramping up that capacity to allow telework, to allow our public servants to work from home?

Mr. Paul Glover: Absolutely, I would be happy to do that. My apologies if I take up all of your time; just wave and I will stop.

We did a ton of work here. It was truly unprecedented. It started with what we call secure remote access points, to make sure that we were doing this safely.

When Mr. Jones was talking about all the work in terms of COVID, one of the things he forgot to share with you is all the advice they gave us about how to do this safely. That involved setting up secure remote access points for public servants to do that.

We worked with all the major telcos and Internet providers to expand bandwidth and dedicate it in spots where we knew it was weak. We worked with first responders to make sure they had priority access to the lines they needed. It was really multi-faceted.

We realized very quickly that it wasn't just the number of secure remote access points that were relevant. It was also bandwidth. It was how they were working, what they were doing—and they were doing a lot. We had to really increase the bandwidth. We've just about doubled the number of secure remote access points, and we have just about doubled the bandwidth that's dedicated to this as well. There were big, big changes in that space.

The minister spoke about call centre operators, for example. We moved to make sure they had tablets and they had phones, so that they didn't need to go into a physical call centre. We worked with the telcos and the service providers to make sure the technology worked. That was part of the reason, in the earlier days, that we had a few—quite a few, frankly—dropped calls. We worked quickly to correct that, to route those calls to people's homes so they would be able to do that.

We also realized that not everybody needed the secure remote access, so we worked to stand up what we call the government collaboration site. It's Microsoft Office 365 and Teams in the cloud, but not secured. Public servants are still able to work together to collaborate with colleagues on a government-sponsored platform, but it is not secured. They know that. We're then going to roll that back in so that no information is lost.

We tried to give people as many tools and choices as possible to be able to operate. We doubled our video-conferencing capacity. We went from about a million minutes, a million and a half minutes a day of teleconferences, to over five million a day.

It was literally just standing up capacity. It was not just a tablet and Internet, but the telephones that go with it, the video conferencing, the security, the service to store all of the data with CERB and with more people applying. It was really quite comprehensive.

Mr. Francis Drouin: Mr. Glover, I know through the Buyandsell.gc.ca website, for instance, IT services and IT products were identified as priorities for COVID-related issues. Did your organization go to the same suppliers that you would normally go to, or did you provide some innovation within the system to allow...? Maybe there are new products out there that we don't know of yet, or great solutions that were offered through Buyandsell.

How did your department balance "I'm going to go with the people I know" versus "there may be new solutions out there that we still don't know of"?

● (1835)

Mr. Paul Glover: There are two parts to the answer to the member's question.

The first is that we needed to move quickly, so scale and speed mattered and we looked for partners in vendors that were going to be able to do that. To move at the numbers we were dealing with—millions of Canadians logging in simultaneously on day one—had to be a no-fail. We needed to be ready. The systems needed to work, so we had to work with people who could move at the speed and the scale we were looking for. It was not who we knew; it was speed, scale and security.

Because we work from coast to coast to coast, we had to look at our relationships with SMEs. We couldn't get to all the places we needed to get to, so we shifted the business model to allow, for example, trusted partners to be able to configure and install equipment for us. We would audit that and ship direct to reduce the time we were taking. We innovated that way and tried to bring more SMEs, particularly those that perhaps might have been hurting for some business, and we had some. If they could meet our security requirements, we were able to bring them into the ecosystem, so it was that mix.

I will tell you, quite frankly, I received—

The Chair: Very briefly, sir, you're over time now, so finish in the next 16 seconds, please.

Mr. Paul Glover: I received offers for new technologies virtually every day. We worked with partners to try to assess those to find ones that were relevant to us. We have literally been inundated with people trying to provide new services to us and we're trying to work through all those.

The Chair: Thank you.

Mr. McCauley, go ahead, please.

Mr. Kelly McCauley: Thanks.

Mr. Jones, I'd just like to follow up on Mrs. Block's question regarding Huawei. You commented that we have to protect ourselves from all vendors. Do you feel the same way about the other two main vendors, Ericsson and Nokia, for servers, as Huawei, that we have to protect ourselves against them?

Mr. Scott Jones: We look to make sure that we evaluate every individual product and company on its own basis and then we try different mitigations, depending on where it comes from.

Mr. Kelly McCauley: You talked about extra risk reduction. Is there a larger risk issue with Huawei than, say, Ericsson or Nokia?

Mr. Scott Jones: There are different risks. One of the things that we look for is—

Mr. Kelly McCauley: What are the different risks for Huawei, say, than for Ericsson?

Mr. Scott Jones: For example, we look to see where the products are coming from, where they're being built, where the software is being written. In general, for most of this equipment it's not really a physical hardware issue; it's mostly software. Software right now is being written around the world. One of the things we look at is the testing framework that needs to go with it.

Mr. Kelly McCauley: You're putting Huawei on the same level of security risk-wise as, say, Nokia or Ericsson.

Mr. Scott Jones: We would take it into account where we apply different mitigations. One example would be the lab testing program we have in place with a Canadian lab company that does additional testing. That's an additional mitigation measure that we put in place for the existing 4G network.

Mr. Kelly McCauley: Let me ask you a couple of different questions. The minister stated earlier in her comment that it is widely know Zoom is insecure. Many government workers use Zoom. How do you feel about private caucus meetings—Conservatives, Liberals, NDP or the Bloc—using Zoom, if it is widely known to be insecure?

Mr. Scott Jones: Zoom bombing was a phenomenon. We heard a lot about it at the beginning of the COVID crisis. We can do things like using the lobby as we did here, using unique codes and passwords, sharing those things as a way to minimize the number of people....

In terms of the communication itself, we've never assessed Zoom for the protection of sensitive communications, such as those we call protected B in the government.

Mr. Kelly McCauley: Should we not be doing that? The governing Liberals are having their caucus meetings over Zoom, and the opposition and the NDP are discussing confidential government information.

Mr. Scott Jones: We've been working with the House of Commons to find an appropriate balance. Unfortunately, it was security.... No one product has all the features we need plus all the security things we would be looking for, and it really is to strike a balance between using—

Mr. Kelly McCauley: What's your level of inability to sleep at night over something like this? Is it that you sleep soundly or you're up at night with the night terrors over the lack of security for members of Parliament using the prescribed program in the House of Commons?

Mr. Scott Jones: I'm very comfortable with using Zoom for this. I think the way we've worked with the House of Commons to set it up and mitigate—

Mr. Kelly McCauley: I don't mean for committee work that's open to anyone viewing. I mean for private information, such as a caucus meetings, or perhaps cabinet meetings, if they're doing those over Zoom.

Mr. Scott Jones: One of the things we are working on with the House of Commons staff is to provide a solution for caucus meetings, and for electronic voting as well, to make sure that we're adding additional layers of security. That is something we have been working with since the beginning in continuing to enhance security but also maintain the usability. I think that's something we're working to strike a balance on with the House of Commons. We have a team stood up and their full-time job is to work with the House of Commons to support you.

● (1840)

Mr. Kelly McCauley: In your opening statement, you mention that you monitor and protect programs against cyber-threats, including CERB. What is the threat there? Is it duplicate programs? Are people hacking into CERB? The reason I ask is that in a National Post article today there was a concern expressed that people overseas could be applying. Is it a matter of ensuring the VPN users are actually in Canada for applying? What are your concerns about it?

Mr. Scott Jones: Predominantly, we were looking for anybody who would try to impersonate the Government of Canada and, for example, set up a CERB-like site that looks to fake out Canadians, to pretend that it is CERB—

Mr. Kelly McCauley: Your exact words were “against cyber-threats”. That's not a cyber-threat of CERB. That's a phishing or fraud threat. Did you perhaps word it badly, or was that your intent?

Mr. Scott Jones: No, it is a cyber-threat, because they're using that as part of phishing. They use it to lure Canadians into revealing their private or confidential information.

The second piece that we do look for, though, is that is we look to make sure we're ready to defend against denial of service attacks, so that the site remains up and available for Canadians. That's something we work closely on with our partners at Shared Services Canada.

Mr. Kelly McCauley: Okay. This will be my last quick question, I'm sure—

The Chair: Unfortunately, Mr. McCauley, we just don't have the time.

Mr. Kelly McCauley: Thank you, Mr. Chair.

The Chair: We'll now go to Mr. MacKinnon, please, for five minutes.

[*Translation*]

Mr. Steven MacKinnon: Hello again. I'd like to thank you for your efforts.

There is a lot of talk these days about returning to work and preparing for it, even though we don't know how or when we're going to get back to our offices. The Government of Canada has spent a lot of time reviewing its workplace of the future model.

My question is primarily for Mr. Glover. Could you tell us more about the technology side of the office of the future in the public service and from a post-COVID-19 work perspective? I'm obviously talking about the availability of wireless Internet, cloud computing, and other tools.

[*English*]

Mr. Paul Glover: The short answer is that in order to be digitally enabled you need to have access to digital tools. This means that, just like you trust when you use an electrical outlet that it's going to work, in the office place we need to have wired access points that work and we need wireless access points.

We know and understand that increasingly those two things are a reality and that people are moving around, so this is what has been built into the new standard that we have worked on with PSPC. All new fit-ups have wired and wireless access points so employees are able to function. It also allows us to deal with the changing security requirements. On top of that, the networks are changing, and we're moving to what we call “zero trust” so that at any time, on any device, we're able to make sure that public servants are able to work.

In order to be digital, you need access to the tools, so we need to make sure that access and connectivity, like heat and light, are there and are functional, and not too slow, because then this doesn't work. It has to be of a quality, a security and an availability, and that's what's being built into the standard. That's what we're working to establish for all new federal workplaces. Frankly, the harder part is the retrofit, the going back into older existing buildings, but the technology is improving. We've sent a challenge to industry, and we're accelerating the work in that space as well.

Mr. Steven MacKinnon: That's fantastic.

I know one of the things your organization has spent a lot of time assisting with is a pilot project called GCcoworking. For the benefit of colleagues, that is a pilot project whereby employees from different departments can enter an office environment that is closer to their homes or, when they're on the road, have access to all the technology tools and the required security.

Can you talk a little about GCcoworking and the technology enablement you have done there?

● (1845)

Mr. Paul Glover: Essentially, the question is about a fundamental shift. Right now a lot of people feel they come into their office, sit down at the same desk, the same phone. These GC collaborating spaces are not that. They are a set of standard spaces where a public servant can come in, plug in their tablet, get to their network, their phone number pops up and they're able to function. It doesn't require them to go to the same workplace.

The experience from employees who have moved into this space is exceptionally positive. It allows teams to self-organize, to meet where they need to. It allows people flexibility to be closer to home and to better manage the work-life challenges they face. The feedback from employees as we stand up plans to return to the workplace—because we never really stopped working, so it's not a return to work but a return to the workplace—is that those spaces will be extremely important in providing them the flexibility they will need if there are problems with day care, school and other things. They're a great tool. I suspect the feedback from those pilots will be quite positive and there will be a move to accelerate them.

In this new world there will obviously be some cleanliness and hygiene issues we will have to sort through to make sure it is done safely, but from a functionality point of view, that's the concept, that's the model and that's the flexibility it provides employees and teams.

The Chair: Thank you very much.

Mr. Steven MacKinnon: Thank you.

The Chair: We'll now go to our final two interventions. These are two and a half minute interventions, starting with Monsieur Barsalou-Duval.

[*Translation*]

Mr. Xavier Barsalou-Duval: Thank you, Mr. Chair.

Earlier, it was said several times that cloud computing was good for computer security.

I'm not a computer security specialist, but does data or emails from MPs that are stored on their computer's hard drive end up on private companies' cloud servers?

[*English*]

Mr. Paul Glover: Mr. Chair, in response to the member's question, as he alluded to, cloud is just an exceptionally large data centre that is often multi-tenant and allows the vendor to be able to scale up. What is unique about the way the Government of Canada has approached cloud is that we have imposed our security requirements. As Mr. Jones said, protected B is an example. We have physical requirements that they have to reside in Canada. They have physical security requirements. The employees have to be cleared. Where we are able to, we work with security partners to go in and physically audit those security requirements.

[*Translation*]

Mr. Xavier Barsalou-Duval: Sir, my question is whether or not data is being held by private providers. Is there any outsourcing of cloud computing or is it done directly by government or government services?

[*English*]

Mr. Paul Glover: The cloud services providers are running those data centres. That would include the data in there, but again I must underscore that it's done to the standards we impose on them with respect to the storage and encryption of that data. That would include backups, the ability to restore and who would be able to unencrypt that data.

[*Translation*]

Mr. Xavier Barsalou-Duval: Are these suppliers all Canadian or are there some from other countries?

[*English*]

The Chair: Let's have a very brief answer, please.

Mr. Paul Glover: It is a mix. We have the large multinationals, Amazon web services, Microsoft Azure, to Canadian companies like ThinkOn. The key is they're subject to the same requirements. They must operate in Canada, so we are not subject to things like the Patriot Act and others. The data resides solely in Canada, and we have full ability to physically visit, inspect and verify the security claims.

● (1850)

The Chair: Thank you very much.

We will go to our final two and a half minute intervention.

My understanding, Mr. Green, is that you have ceded your time to Mr. McCauley. Is that correct?

Mr. Matthew Green: I have. I'm keenly interested to see where he goes with it.

The Chair: Thank you very much.

Mr. McCauley, you have the final intervention for two and a half minutes.

Mr. Kelly McCauley: Thanks.

Mr. Jones, just back to you, again in your opening remarks, you said, “Finally, it is important to note that the Government of Canada has a strong and valuable relationship with our international cyber partners. We...share information, which has significant impact on protecting our respective countries' safety and security.”

This goes back to Huawei. We're the only one of the Five Eyes that has not banned Huawei from our 5G or the major role. How will this affect us? Do we risk being excluded from the sharing of vital information if we move ahead with something like Huawei?

Mr. Scott Jones: One of the things that we've really been looking at is that we're a net contributor. Because of our defence with the government, we contribute quite a bit of value to the cybersecurity ecosystem in the world. Our partners around the world value that. In fact, we're one of the top one or two contributors in a lot of things, so we do contribute quite a bit, and we get stuff back as well. We look to build on that and the expertise that we have and to continue to build the strong relationships. It's a relationship—

Mr. Kelly McCauley: Do we risk being shut out of such information for using Huawei, when everyone else has banned Huawei for security reasons?

Mr. Scott Jones: We continue to work with our partners. That's a decision that the government will take into account when it makes its decision. For us, we continue to see no change in our sharing.

Mr. Kelly McCauley: Do you think this is going to be a political decision as opposed to a decision made by your department or on information provided by your department?

Mr. Scott Jones: One of the things for us is that we see no change in the sharing between all of our international allies, including what we share with them on cybersecurity.

Mr. Kelly McCauley: If we went to Huawei, you say you believe there would be no change in sharing. We've heard the U.S. threaten to cut us out of information sharing if we go to Huawei. Is that not a concern for you?

Mr. Scott Jones: I can't speak to what other countries have said. For us, we continue to build strong partnerships with our international partners, and that will be part of the decision.

Mr. Kelly McCauley: I know you can't speak for other countries. Is that not a concern for you, as a Canadian dealing in your business, that we will be shut out if we go against our allies' wishes and go to Huawei servers?

Mr. Scott Jones: One of the things for me is to always show that we provide strong value to our allies. Hopefully they'll see that we have really unique cybersecurity information that we share with them constantly.

The Chair: Thank you very much.

Mr. Kelly McCauley: I'm dumbfounded. I'm absolutely dumbfounded.

The Chair: Thank you very much. I'd like to thank all of our witnesses who were here today, witnesses from Shared Services Canada, the Treasury Board Secretariat and, of course, the Communications Security Establishment. Your information, your testimony, has been very helpful and informed.

To Mr. Jones personally, I know that on a number of occasions people talked about the fact that you may have some difficulty sleeping at night, particularly in your position. I would just point out to you, sir, that's why God invented red wine, so perhaps take that into account.

To the rest of you, colleagues, we will meet again this Friday at 11 a.m. eastern standard time. I wish, in the intervening three or four days, that you all keep healthy and safe, and we will see you on Friday.

Have a good evening, everyone.