HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

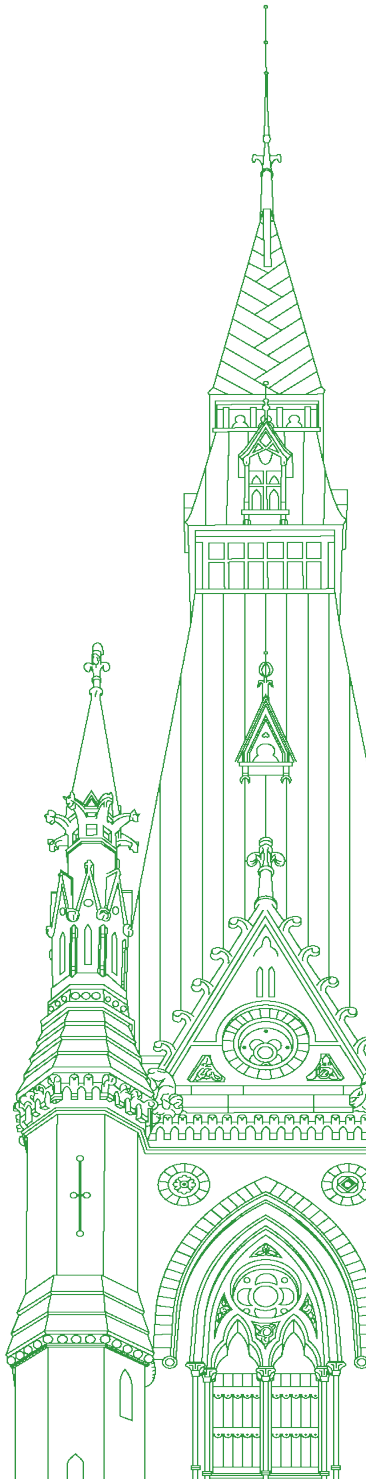
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Accounts

EVIDENCE

NUMBER 022

Monday, January 26, 2026



Chair: John Williamson

Standing Committee on Public Accounts

Monday, January 26, 2026

● (1100)

[*Translation*]

The Chair (John Williamson (Saint John—St. Croix, CPC)): Good morning, everyone.

I now call the meeting to order.

[*English*]

Welcome back from the Christmas recess. I hope everyone is rested and ready to go.

The weather is not getting us down too much, although I understand it's worse in Toronto.

Jean Yip (Scarborough—Agincourt, Lib.): Yes. We have 45 centimetres of snow.

The Chair: Have they called in the army yet?

Jean Yip: No, not yet. We're very proud of being so efficient.

[*Translation*]

The Chair: Welcome to meeting number 22 of the House of Commons Standing Committee on Public Accounts.

[*English*]

Today's meeting is taking place in a hybrid format, pursuant to the Standing Orders. Members are attending in person in the room and remotely by using the Zoom application.

I want to thank all of our witnesses for coming here in person today.

Before I begin, I would like to remind participants of the following points. Please wait until I recognize you by name before speaking. Comments should be addressed through the chair—well, that's more if we have a debate of any sort.

[*Translation*]

Pursuant to Standing Order 108(3)(g), the committee will begin consideration of the cybersecurity of government networks and systems, taken from the fall 2025 reports of the Auditor General of Canada and referred to the committee on Tuesday, October 21, 2025.

[*English*]

Let me introduce the witnesses I just thanked for coming in today despite the ugly weather.

From the Office of the Auditor General, we have Andrew Hayes, deputy auditor general, along with Jean Goulet, principal. It's nice to see you.

From the Treasury Board Secretariat, we have Dominic Rochon, chief information officer of Canada, and Po Tea-Duncan, the chief information security officer of the Government of Canada. It's nice to see you as well.

From Shared Services Canada, we have Scott Jones, president. It's good to see you again, Mr. Jones. We also have Patrice Nadeau, senior assistant deputy minister, connectivity and security services branch. It's nice to see you as well.

From the Communications Security Establishment, we have Caroline Xavier, chief. It's nice to see you again. We also have Rajiv Gupta, head of the Canadian centre for cybersecurity.

Thank you all for coming in today. I suspect we'll be using the full two hours, given the number of esteemed witnesses we have here today. Each unit department will have five minutes.

Mr. Hayes, I'll get you to open things up for five minutes, please.

[*Translation*]

Andrew Hayes (Deputy Auditor General, Office of the Auditor General): Good morning, Mr. Chair.

Thank you for the opportunity to appear before the committee today to discuss our report on cybersecurity of government networks and systems, which was tabled on October 21, 2025.

I'd like to begin by recognizing that we are meeting on the traditional, unceded territory of the Algonquin Anishinabe people.

With me today is Jean Goulet, the principal director who was responsible for the audit.

The central responsibility for protecting government information technology systems and operations is shared by the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada. These organizations work together and with departments and agencies to prevent data theft and limit disruptions to systems that deliver programs and services to Canadians. We found that while the government had tools in place to protect and defend its networks and systems against cyber-threats, there were gaps in cybersecurity defence services, monitoring and response during active attacks.

● (1105)

[*English*]

Only 42% of federal organizations are required, by Treasury Board policy, to use the cybersecurity defence services offered by Shared Services and the Communications Security Establishment. Others have opted in, but this inconsistent use of services undermines the federal government’s ability to protect critical information and manage risks.

We also found that coordination among the three organizations was too slow during active cyber-attacks. For example, poor coordination delayed the government's response during a major attack two years ago. This extended the time during which the attacker had access to public servants' personal information.

Protecting federal networks and systems also requires analyzing the potential vulnerabilities of all government IT devices, including laptops, smart phones, and servers. We found that Shared Services and the Communications Security Establishment did not have a comprehensive inventory of all government devices. Without up-to-date information, the federal government risks being unable to quickly respond to a changing cybersecurity landscape.

Malicious actions, external events, and attacks targeting the Canadian government’s digital systems are frequent and more sophisticated. A coordinated and comprehensive approach to the government’s cybersecurity posture, better collaboration and a current inventory of IT devices are key to safeguarding Canadians’ information.

[*Translation*]

Mr. Chair, this concludes my opening remarks. We would be pleased to answer any questions the committee may have.

Thank you.

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

Mr. Rochon, you have the floor for five minutes.

[*English*]

Dominic Rochon (Chief Information Officer of Canada, Treasury Board Secretariat): Thank you, Mr. Chair.

I'm pleased to speak about the Auditor General's performance audit of the cybersecurity of government networks and systems, which is report 5 of her fall 2025 reports.

I'm pleased to appear today with my colleagues from Shared Services Canada, the Communications Security Establishment, the Office of the Auditor General and, in particular, Po Tea-Duncan from my office, the Government of Canada's chief information security officer.

Mr. Chair, protecting the government's IT infrastructure from vulnerabilities and responding to cybersecurity threats is critical to protecting Canadians' data and the services the Government of Canada provides them. As Canadians increasingly access government programs and services online, network security is more important than ever.

The Treasury Board of Canada Secretariat is named in two of the recommendations in the audit. The first such recommendation is that TBS, in consultation with the Communications Security Establishment, ensure that federal organizations implement the Communications Security Establishment's cyber-defence sensors on all their IT endpoint devices so that their associated vulnerabilities can be identified and remediated.

The second recommendation is that Treasury Board Secretariat, Shared Services Canada and the Communications Security Establishment re-evaluate their cybersecurity incident management practices to enable better coordination and timely access to required critical information when responding to cybersecurity incidents affecting federal organizations.

[*Translation*]

The government is committed to reducing cybersecurity risks in order to protect its systems and, consequently, Canadians’ information, and to ensuring the continued delivery of secure and reliable digital services. The Treasury Board Secretariat welcomes the Auditor General’s recommendations and will continue to work with Shared Services Canada and Communications Security Establishment Canada to implement them.

With regard to evaluating our cybersecurity incident management practices to improve the rapid communication of critical information, the Treasury Board Secretariat, in collaboration with its partners, regularly reviews our operational framework, the Government of Canada Cybersecurity Event Management Plan.

The lessons learned from cyber simulation exercises, also known as “tabletop exercises”, enable the TBS to identify improvements that are then applied to the plan to ensure its effectiveness.

The Government of Canada, like all public and private sector organizations, faces ongoing and evolving cyber-threats. To maintain a strong cyber-defence posture, the Treasury Board Secretariat, in consultation with Communications Security Establishment Canada, will work with federal organizations to ensure that the centre's defence sensors are installed on all endpoints, whether they are devices, servers or workstations.

We will achieve this in part through a tool that quickly identifies information technology endpoints where no sensors are deployed. This will enable us to subsequently detect, assess and prioritize vulnerabilities to be addressed on IT devices on government networks.

● (1110)

[*English*]

Of note, Mr. Chair, to enhance the government's cybersecurity, budget 2024 provided $11.1 million over three years, starting in 2024-25, for the Treasury Board Secretariat to begin implementing a whole-of-government cybersecurity strategy. This included measures to support the rapid identification, assessment and management of vulnerabilities across the enterprise, the formation of a purple team that will emulate techniques used by malicious threat actors to proactively test and audit any security gaps, and the creation of a program to improve cyber-assurance and risk evaluation for the Government of Canada enterprise.

Network cybersecurity is vital for the government to protect Canadians' data and services, ensure national security, maintain economic prosperity and uphold public trust in an increasingly digital world. We agree with the Auditor General's recommendations and, along with our partners, are taking action to address her concerns.

Thank you. Following my colleagues' opening remarks, I will welcome the committee members' questions.

The Chair: Thank you very much.

Up next is Mr. Jones, please, for five minutes.

[*Translation*]

Scott Jones (President, Shared Services Canada): Thank you, Mr. Chair, for the opportunity to discuss the Auditor General's Report on the Cyber Security of Government Networks and Systems.

Before we begin, I would like to acknowledge that we are on the traditional, unceded territory of the Algonquin Anishinabe people. I'm here today with Patrice Nadeau, senior assistant deputy minister for SSC's Connectivity and Security Services Branch.

Shared Services Canada, or SSC, welcomes the Auditor General's findings and is working to address the issues raised. It's important to underline that the Auditor General found that the government had tools in place to protect and defend its networks and that the government's cybersecurity plan was sound and comprehensive.

As the provider of IT services to departments and agencies, SSC plays a pivotal role in this work.

[*English*]

Indeed, SSC blocks about 6.5 trillion cyber-threats annually, which is an average of 18 billion a day. This ensures the uninterrupted operation of government services. We do that through a state-of-the-art enterprise infrastructure and modern commercial cybersecurity solutions that defend government systems against a wide range of cyber-threats. SSC uses multiple layers of defence and prevention, including firewalls, network defences, anti-denial of service measures, anti-virus and anti-malware tools, encryption, virtual private networking and robust identification on authentication services.

We have an excellent partnership with our colleagues at the Treasury Board Secretariat and the Communications Security Establishment. This collaboration is absolutely vital, as the Auditor General underscored, and we continue to improve it. We regularly conduct post-mortems on cyber events to identify ways we can always do better. Together, SSC and CSE's Canadian centre for cybersecurity provide sophisticated cyber-defences that go beyond commercial capabilities. Our work offers one of the most sophisticated cyber-defences in the world.

Cybersecurity is a space that is evolving fast, and we work continuously to keep on top of it. That said, there is more to do, as the Auditor General rightfully underscored. We share the Auditor General's concerns about organizations that are outside of SSC's enterprise internet service. As the threat environment changes rapidly, that is a model that clearly needs to evolve. This is why SSC is now working to provide connectivity and security services to 43 small departments and agencies. It is on track to complete this work by the end of March 2027.

The Auditor General also highlighted a project called endpoint visibility, awareness and security, or EVAS for short. This is one of the tools SSC is adding to its cybersecurity environment. EVAS will automatically identify network-connected endpoints, such as desktops and servers, and verify that they meet security requirements. Unlike our semi-manual service system, EVAS is automated and enables real-time vulnerability and impact assessments. EVAS will also provide automated response to cyber events. While there were delays to this project, our organization has learned a number of lessons. This project has turned a corner and, since implementation began in July 2025, over 36,000 deployments have been completed.

The Auditor General also highlighted our project to develop a security information and event management system, or SIEM for short. I want to assure you that we are on track to award a competitive contract for this project in early 2026. Further, SSC is currently operating an interim SIEM capability, which allows SSC and our partners at the Canadian centre for cybersecurity to manage priority needs and supports an effective response to cyber-threats.

Since SSC's creation, we have shifted the government's business model from one that is siloed and decentralized to a government-wide enterprise approach. This not only reduces costs but strengthens overall security Government of Canada-wide. It is easier to monitor, patch and fix one system than 45 separate ones—and it is easier to invest in one system than in 45 separate ones.

We are not done. SSC is streamlining the management of devices and software by centralizing procurement and operations. This achieves considerable efficiencies and reduces the potential for inconsistencies in security policies. We're also continuing to reduce duplication by replacing additional siloed back-office tools with standard, government-wide tools. Legacy systems are also more vulnerable to cyber-threats, as was pointed out in another Auditor General review. Moving off legacy systems improves our cybersecurity posture.

● (1115)

[*Translation*]

In short, everything we do to consolidate and modernize IT systems is essential to improving cybersecurity.

Reports from the Auditor General are also an important tool to hold us accountable and allow us to improve our operations. Cybersecurity is an evolving field with actors that don’t follow our rules. Continuous improvements are key to protecting the GC’s IT systems.

Thank you for the opportunity to speak on this important file, and I look forward to answering your questions.

Thank you.

The Chair: Thank you, Mr. Jones.

Ms. Xavier, you now have the floor for five minutes.

Caroline Xavier (Chief, Communications Security Establishment): Thank you.

[*English*]

Good morning, Mr. Chair and members of the committee.

[*Translation*]

Thank you for inviting me to appear today to discuss the Auditor General of Canada’s report on the Cyber Security of Government Networks and Systems.

[*English*]

As mentioned, my name is Caroline Xavier, and I am the chief of the Communications Security Establishment, also known as CSE.

I'm joined today by Rajiv Gupta, head of the Canadian centre for cybersecurity, also known as the cyber centre, which forms an integral part of CSE.

[*Translation*]

We are pleased to appear alongside our colleagues from the Treasury Board Secretariat and Shared Services Canada, with whom we work closely on cybersecurity.

[*English*]

Today I will provide a brief overview of CSE and our cyber centre, and then share how we are responding to an increasingly complex threat landscape, one that includes cyber-threats, risks to economic security, violent extremism, foreign interference, disinformation campaigns and more.

[*Translation*]

Before we begin, I want to acknowledge that we are on the traditional unceded territory of the Algonquin Anishinabe nation. We acknowledge that this nation has been on this land since time immemorial.

CSE is one of Canada’s key security and intelligence agencies, and a stand-alone agency reporting to the Minister of National Defence.

[*English*]

As part of our mission, we provide vital foreign signals intelligence on a wide range of threats to help the Government of Canada make informed decisions and safeguard Canada's interests, while strictly following Canadian law and privacy standards. We also defend Government of Canada networks and systems of national importance against malicious cyber activity targeting Canada's digital infrastructure.

Through the cyber centre, we serve as the national and technical authority for cybersecurity, providing a single, trusted source of expert advice and guidance for Canadians and organizations across the country. By integrating cybersecurity, signals intelligence and foreign cyber-operations, CSE is uniquely positioned to strengthen Canada's overall defence and security.

The integrity of Canada's cyberspace is foundational to our country's future. It underpins our digital economy, protects personal safety, and strengthens national resilience.

In 2024-25, CSE produced more than 3,300 foreign intelligence reports and responded to over 2,500 cyber-incidents affecting federal institutions and critical infrastructure partners. We also issued over 330 pre-ransomware notifications to more than 300 Canadian organizations, early warnings that helped prevent serious harm.

As the threat landscape evolves, so do we. Our world-recognized cyber-defence sensors program provides real-time detection of malicious cyber activity across Government of Canada networks and cloud environments. This program is available to all federal departments and agencies, and to Crown corporations upon request. It enables our experts to block and neutralize threats before they cause harm.

While many federal organizations manage their own IT infrastructure, they can leverage CSE's sensors program and the cyber centre's expert guidance to strengthen their defences. Today, most federal institutions use at least one of our sensors. We also continue to deepen our engagement with Crown corporations, critical infrastructure operators, and provincial and territorial partners.

CSE welcomes the Auditor General's report and supports its recommendations, particularly those aimed at strengthening sensor deployment and improving incident management coordination. As my colleagues have highlighted, we are working closely together to expand the deployment of cyber-defence sensors across federal networks and refine incident response protocols.

● (1120)

[*Translation*]

These efforts build on significant progress already made to modernize and secure the digital systems that deliver essential services for Canadians. Cybersecurity is a shared responsibility, and collaboration remains at the heart of our approach.

Mr. Chair and members of the committee, the threat environment is dynamic, but our commitment is unwavering. Together with our partners, we will continue to protect Government of Canada systems, Canada’s critical infrastructure and digital systems, ensuring Canadians can rely on secure and trusted services.

Thank you once again for the opportunity to appear before this committee.

[*English*]

We welcome your questions and look forward to continued dialogue.

Thank you.

The Chair: Thank you, all, very much.

We'll now begin our first round of questions, which will consist of three members with six minutes each.

Ms. Kusie, you'll kick us off this year. Thank you.

Stephanie Kusie (Calgary Midnapore, CPC): Earlier this month, the Prime Minister announced a new Canada-China strategic partnership. On many fronts, this concerns me, but specific to this meeting, I'm concerned about Canada's cybersecurity and the protection of our private information.

In 2024, I was informed by IPAC through the FBI that I had been the target of a cyber-attack orchestrated by the PRC. I had been targeted because of my status as a member of Parliament. As the Canadian government begins a new economic relationship with the PRC, I'm concerned with how our government assesses these new strategic partnerships with non-democracies on the world stage.

Madame Xavier, can you please share with this committee what measures your agencies and departments are taking to ensure cybersecurity and the protection of sensitive data as we enter new agreements with governments like the PRC?

Caroline Xavier: As mentioned in my opening remarks, CSE holds multiple mandates within one agency, one being the foreign intelligence collection that we do, to be able to ensure that decision-makers have the information they require to make decisions. That is something we've been doing for almost 80 years. The other part of our mandate is the cybersecurity or cyber-defence part of our mandate, and one other part of our mandate is the foreign cyber-operations mandate. Having all those elements within one agency really helps us to ensure that what we learn from foreign intelligence data collection can be used in the defence of Canada and vice versa. All the billions of incidents that we protect against in the defence of Canada allow us to learn about threat actors who maybe have potential interests in Canada. That then feeds what we can do on the foreign intelligence part of the mandate. In addition to that, in foreign cyber-operations, we're able to take actions in cyberspace, in the foreign cyberspace, to ensure that we continue to protect Canada.

We operate under cabinet-approved intelligence priorities that are reviewed on a regular basis. As it is now, our mandate includes protecting Canada's critical infrastructure and democratic institutions. Whether they are nation states or cybercriminals, that is part of the mandate that we operate on a regular basis, 24-7, 365 days a year. We remain committed to being able to ensure that we do our jobs effectively. I am pleased and proud of the fact that we lead an organization that puts out world-class cyber-defence. The work that we do together with our partners both at Treasury Board and SSC allows us to continue to protect Government of Canada systems.

● (1125)

Stephanie Kusie: Thank you very much for that extensive answer.

You mentioned that you have protected against billions of negative interactions, negative interceptions; however, it is apparent to me, from the experience I had as well as that of several other members of Parliament, that the most cunning of evil operators are still able to penetrate the system, which is very concerning to me.

You mentioned the implication of other decision-makers. Are there ministers who have given you direction specifically, and who would those ministers be, please?

Caroline Xavier: Again, thank you for the opportunity to clarify.

Our intelligence priorities are driven by the cabinet of the Government of Canada. Our intelligence—

Stephanie Kusie: Which cabinet members are they, please?

Caroline Xavier: The full cabinet endorses the intelligence priorities of the Government of Canada—

Stephanie Kusie: Who provides the direction, please?

Caroline Xavier: The full cabinet provides the direction, led by the Prime Minister of the country. As a result, we've published the intelligence priorities so Canadians have an opportunity to understand the priorities we have. The priorities are fairly broad, and we are able to work to those priorities in the work we do.

Stephanie Kusie: Thank you very much, Madame Xavier. I'm not getting a lot of good, clear information in terms of what those priorities are and how they're implemented, but thank you.

Mr. Hayes, your report from October is not the first to focus on cybersecurity. As the importance of technology continues to grow, I'm sure it will not be the last, unfortunately.

Do you believe that hostile actors like the PRC could attempt to act on the security gaps that you mentioned within this report?

Andrew Hayes: There's no doubt that the government faces attacks every day. Indeed, they're stopping billions and trillions every year. I think the message from our report is that vigilance and rigour need to be at the top of the mind of every government organization.

To us, one of the big findings in our report is that not every federal organization is required to use the services that Shared Services Canada and the Communications Security Establishment Canada provide. That is, in our view, a missed opportunity.

Stephanie Kusie: Thank you for that.

Monsieur Rochon, over the past year, the government has placed a focus on artificial intelligence and the use of it both within and outside of government. With AI comes a world of opportunity, but also a world of unknowns.

How can Canadians be confident that their confidential information will be secure and private if your department can't even get federal organizations to follow the existing rules and policies surrounding cybersecurity?

Dominic Rochon: Thank you for the question, Mr. Chair.

Let me just say that the challenge remains that.... The Financial Administration Act, section 7, grants Treasury Board authority to apply general administrative policies, such as the policy on government security and the policy on service in digital. Those policies are applicable to departments and agencies that fall according to a certain schedule. That's how the legislative framework is set up and, therefore, we cannot impose on agents of Parliament or Crown corporations—

Stephanie Kusie: That's not very efficient or effective if you can't impose—

The Chair: Ms. Kusie, I'm afraid that is your time. We will certainly come back to you.

Stephanie Kusie: Thank you, Chair.

The Chair: Next is Ms. Yip.

You have the floor for six minutes, please.

Jean Yip: Thank you. Happy new year.

Thank you to our witnesses for coming in on a slight snow day here in Ottawa. I'll just note that Toronto has 45 centimetres of snow. It's rare that we out-snow Ottawa.

Voices: Oh, oh!

Jean Yip: I'm going to direct this question to all three organizations. How is your organization working on improving collaboration among all three of you? What steps have you taken that will help to protect Canadian national security?

Mr. Jones, would you like to go first?

Scott Jones: Sure. Thank you for the question.

I think there are a few areas where we're making progress.

The first thing is that there's been a base of collaboration for over a decade as we've built up this robust system of defences, and those are relationships. As much as I'm supposed to be leading a technology organization, effective cyber-response is about building those relationships and the trust, because a lot of times it's a judgment call until you know for certain. That is the first thing.

The second piece is that we are exercising. Mr. Rochon talked about the purple team and some of the other pieces that have been put in place lately as exercises. One of the consequences of having a robust defence mechanism is that.... When I first started working on cybersecurity with Mr. Gupta about 14 or 15 years ago, we were having incidents happening every day that we were responding to. Now our systems take care of a lot of these things proactively, and these big incidents that we've talked about don't happen often. You have to continue to practise so that those muscles stay able to work.

Those are a couple of the things we're doing.

The third thing is that in every single incident there's always something that we can learn from. We do a full after-action review that's led by my colleagues at Treasury Board. I'll let them speak to this, but that's very important. Even when it goes very well, what could have been done better? What could have been done more quickly? What could we learn from this?

There always has to be one, and sadly, with cybersecurity, there usually is a first victim. Our goal together is to make sure there's never a second.

● (1130)

Dominic Rochon: Maybe I can elaborate.

It is indeed a team game. As Madame Xavier pointed out in her opening remarks, there's no one entity in cybersecurity. We form a tripartite in terms of protecting systems across the federal enterprise.

At Treasury Board Secretariat, we put in place rules. Indeed, we've promulgated a cybersecurity enterprise strategy for the federal government. We provide advice and guidance. Also, as Mr. Jones just alluded to, we have a Government of Canada security event management plan that is indeed followed, so that when there's a critical incident we understand roles, responsibilities, etc.

As the Auditor General pointed out, there are some shortcomings with regard to that coordination. Despite the fact that we meet regularly and we're constantly coordinating, there are certain things that we can do better. Last May, we put in place for the first time a simulation exercise at the executive level, touching several departments and agencies. Drawing from the lessons learned from that exercise, we're going to be updating our security event management plan, among other things. We also keep our policies and our strategy evergreen. We learn, as Mr. Jones just pointed out, from any critical incident.

In terms of our coordination efforts, they go from managing the policies to the direction and the guidelines. It's also a partnership with every department and agency. Each has to have a designated person responsible for cybersecurity and for making sure that they understand and interpret our rules and are putting them in place.

Mr. Jones and his organization are responsible for connections to the Internet and all of the infrastructure side of things. Then we have the special sauce, if you will, of the cybersecurity centre led by Mr. Gupta, which, above and beyond putting in place sensors, is doing all sorts of monitoring and connecting with the rest of the Communications Security Establishment to make sure we stay on top of the threat.

Caroline Xavier: The only other thing I would add is the fact that, as I said earlier in my remarks, all that we do to provide advice, guidance and direction is definitely fed from an intelligence perspective. That is helpful, in addition to the learnings we are taking from all incidents that are occurring. As a learning organization, we strive to always do better. As was mentioned by Scott, we continue to apply those learnings. I would also add that as a tripartite, and in the way in which government has organized us in the cyber-defence space, we are the envy of many in terms of how this functions.

This is why I'm pleased about the fact that we have the sensors that we have to be able to be automated and be able to act on our behalf 24-7. We can then dive deeper into them when major incidents happen.

Jean Yip: Why are we the envy of others?

Caroline Xavier: It is primarily because of the fact that Shared Services Canada does a great job of coordinating all that it does with regard to providing a centralized service to many of our government departments. Anybody getting the shared services is then protected by the sensors, because that is part of the standard rollout when it comes to working for the Government of Canada and the Government of Canada systems that Scott Jones protects.

Scott, feel free to add more there. We've heard that, for example, the U.K. Parliament has touted the Government of Canada's world-class sensor system as one of the sensors it recognizes as being world-class.

The Chair: Thank you, Ms. Yip.

That's about your time. I'll give you a few extra seconds next time.

[*Translation*]

Mr. Lemire, good morning. You have the floor for six minutes.

Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you, Mr. Chair.

I would like to take this opportunity to wish you a very happy 2026. I believe it will be a very promising year for the public accounts. At least, we hope so.

Thank you to all the witnesses for your participation, and I apologize for the delay. Parliament sometimes calls on us. It’s part of our job.

I would first like to mention that the Royal Canadian Mounted Police, Public Safety Canada, Global Affairs Canada, the Financial Transactions and Reports Analysis Centre of Canada, and the Canadian Centre for Cyber Security issued a notice on July 16, 2025, stating that hostile agents deployed by the North Korean government could pose as information technology workers.

Ms. Kelly Hutchinson, a digital government and procurement strategist with the Compass Rose Group in Ottawa, pointed out that the North Korea case was just a drop in the ocean of this problem.

For his part, Aaron Shull, research director at the Centre for International Governance Innovation, pointed out that Canada’s reliance on outsourced labour from abroad, coupled with inconsistent security and identity checks, could create real avenues of attack by gaining access to sensitive data, thereby enabling espionage. He even mentioned the possibility of inserting malicious code into government systems and software.

Ms. Xavier, from the Communications Security Establishment, I would like to know your thoughts on the comments made by Ms. Hutchinson and Mr. Shull. Does outsourced labour abroad constitute a risk that should be thoroughly analyzed in a cybersecurity strategy?

● (1135)

Caroline Xavier: Thank you for the question.

It is important to emphasize, as we did in our cyber-threat assessment published in October 2024, that we recognize that we face cyber-threats from states. One of the states that was named is China, but we also named the Democratic People's Republic of Korea in our assessment, as well as Russia and others.

So, yes, we support the advisory that was issued, because it was issued in collaboration with us and the Communications Security Establishment, which includes the Canadian Centre for Cyber Security. This type of advisory is a way for us to ensure that we are all on the same page and that we can provide good advice and guidance so that the Canadian government can be prepared.

However, when we issue such an advisory, it is not just to protect the government. We also want to ensure that Canadians and critical infrastructure operators are aware. When it comes to cyber-threats, it is not just the government that is targeted when someone wants to harm Canada.

Sébastien Lemire: Obviously, we are very vulnerable to the United States, and signing an agreement with China to import Chinese vehicles is not going to help us keep our data at home.

That said, my next question is for Mr. Rochon or Mr. Jones.

The government hires many self-employed workers and contractors. Ms. Hutchinson's question is an interesting one. What is the government doing to authenticate individuals and ensure that they are who they say they are, in an era where identity fraud is facilitated by deepfakes and other tools? What measures have you put in place?

Dominic Rochon: We have implemented security measures. Subcontractors must be authorized to work for the federal government. They go through different levels of verification depending on what they will have access to. There are rules in place to justify and certify their presence.

In short, the problem is that the threat will always be present. It is impossible to guarantee at all times that we have covered everything, so we put rules in place. We have implemented a mandatory course that all public servants must take each year. We have implemented a vulnerability management program where we are looking at the risks and following up on them. We have set up both a red and blue team of various cybersecurity professionals, as I mentioned.

Ms. Tea-Duncan, would you like to elaborate on these points?

[*English*]

Po Tea-Duncan (Chief Information Security Officer of the Government of Canada, Treasury Board Secretariat): Thank you for the question.

The purple team allows us to effectively test in advance some of the techniques of bad actors. It helps us to put in place the right detection and protective measures to make sure that we are all staying ahead of the cyber-threats.

Part of the policy on government security ensures that departments and agencies are putting in place the right baseline security controls. Cybersecurity is all about layers of controls—such as cyber-sensors that are put in place on end points in the network—but it's also about the protection of data within our information systems. That's outlined under the policy on government security.

● (1140)

[*Translation*]

Sébastien Lemire: One of the things we realize about front companies is that companies claim to be indigenous, but ultimately they are not. Because of subcontractors, you never know who is actually doing the work, especially when it is sent to India or other countries to be done at low cost. You realize that you are extremely vulnerable. We send them our data. Is there a mechanism to ensure that the work is done by people from Canada, in Canada? Does this exist, or is it acceptable for gateways to be provided all over the world?

Dominic Rochon: That's an interesting and difficult question.

Each department and deputy minister is responsible for determining how to implement its programs. At the Treasury Board Secretariat, we are putting guidelines in place so that they are aware that risks exist. We need to look at the nature of the work and the systems they will have access to. If they have access to systems, that's where we, who are here before you today, have a role to play. There are also issues from the perspective of equipment supply chains.

For all these things, we have rules in place, as well as procedures for follow-up. Ultimately, it's also a team effort in the sense that each department must ensure that it follows our rules, and we must be aware of access to our systems and the nature of the work done by these departments.

Sébastien Lemire: Thank you, Mr. Rochon.

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

We will now begin the second round of questions.

[*English*]

It consists of five members with various times.

[*Translation*]

Mr. Deltell, you have the floor for five minutes.

Gérard Deltell (Louis-Saint-Laurent—Akiawenhrahk, CPC): Thank you very much, Mr. Chair.

Good morning to all my colleagues.

Happy new year 2026 to everyone here and, of course, to all Canadians who follow our work.

Ladies and gentlemen, thank you very much for being here and thank you very much for serving our country, your country, in a situation as delicate as cybersecurity.

Mr. Chair, we Conservatives have very serious concerns about cybersecurity, particularly with regard to the Beijing regime. My colleague Mrs. Kusie, who is a career diplomat, shared her personal story earlier. I have been spared so far, as perhaps many people here have, but no one is ever safe from this.

Ms. Xavier, in response to my colleague Mr. Lemire's question, you mentioned cyber-attacks and cyber-threats from states. Spontaneously, the first country you identified was the Beijing regime. Could you tell us more about that?

Caroline Xavier: Thank you for the question.

I did not necessarily mention the Beijing regime first on purpose. I just wanted to mention that in our cyber-threat assessment published in the autumn of 2024, which is valid for two years, we clearly stated that we see certain states taking an interest in Canada. Yes, we name China, but we also name other actors such as Iran and Russia, among others.

With regard to our assessment of cyber-threats at the time, we certainly said that China is indeed a very sophisticated and capable actor. However, that does not always mean that, even if it is a Chinese actor, it is necessarily linked to the state. We know that there are also cyber-criminals. In fact, in the same publication, we said that the actions of cyber-criminals are also significant in terms of cyber-threats to Canada and around the world.

We have published several other documents in which we have said that we have seen actors. This is part of what we do to try to ensure that Canada and critical infrastructure are aware of how to protect themselves.

Gérard Deltell: As you said, there are actors, but they are not necessarily linked to the state. However, when we talk about a totalitarian state, it is difficult to view these actors as autonomous. Rather, we see them as actors directly linked to the state, particularly the Beijing regime. You may have noticed that I am careful not to identify the country so as not to stigmatize Canadians who come from that country. For us, the problem is the Beijing regime, not its citizens.

In this regard, I cannot ignore the fact that on this side of the House, we are very concerned about the Prime Minister's visit to the Beijing regime last week. All of our grievances and contentious issues regarding security and human rights seem to have evaporated. That is unfortunate, and we are very concerned about this approach. That is a political point of view, and I have no right to question you on that.

Mr. Rochon, earlier, in response to a question from a colleague, you said that it was a team effort. You have three entities here in Canada, namely the Communications Security Establishment, Shared Services Canada and the Treasury Board Secretariat.

Mr. Goulet, do you feel that these three entities work in coordination or in isolation? This is not a question of blame, but rather one of efficiency. With technology evolving at breakneck speed, do you feel that improvements could be made to ensure that information is shared more widely?

● (1145)

Jean Goulet (Principal, Office of the Auditor General): Thank you for the question.

I can say without hesitation that we observed a very high level of co-operation between the entities. That said, it doesn't mean there's no room for improvement. We mention this in our report, particularly with regard to various projects that were delayed but are nonetheless very important for the country's cybersecurity needs. The three entities definitely co-operate well with each other.

Gérard Deltell: Mr. Rochon, what do you think could be improved? What other entities could be improved to ensure that you are more effective?

Dominic Rochon: Thank you for the question.

I'll start by saying that improvements can always be made, especially when it comes to information sharing.

We have highly skilled people working in all three organizations. We don't always think to bring everyone together to solve the problem. Under our policies, if an incident occurs in any department, the Canadian Centre for Cyber Security is immediately notified. From there, it will launch its investigation. I think improvements need to be made to bring everyone together so that we are all aware. There are also issues we haven't mentioned yet today with respect to access to privacy. If personal information is incorporated, the Privacy Commissioner must absolutely be brought back into the equation. It's a matter of honing those responses, conducting exercises to ensure that everyone understands their role and responsibilities and that everyone works together.

The Chair: Thank you very much.

[*English*]

Mr. Osborne, you have the floor for five minutes, please.

Tom Osborne (Cape Spear, Lib.): Thank you, Mr. Chair.

I think we need to keep the fact that canola farmers or fisher people in Atlantic Canada can trade with a country separate from cybersecurity. I'm not sure the two are connected. We do need to strengthen not only cybersecurity but economic trade.

I think this is the first time I've ever uttered the words.... There was a security threat in Newfoundland and Labrador against the Newfoundland and Labrador Health Services. I was the chair of the cabinet committee on that, so I have some understanding, but this is the first time I've ever said that publicly, because we were advised never to say it. As parliamentarians, we're probably a target for bad actors. I will say that there are bad actors, both nation-states and very well-organized organizations, that profit.

Keeping in mind the balance between the public's right to know what's happening and our nation's security, I think we have to be careful in the questions we ask here, because the work that you undertake is very serious business. We do need to ensure that we address the weak links.

I have two questions. Mr. Rochon, I'll direct this question at you.

With regard to the purple team, how are we ensuring that this group of professionals is able to stay ahead of a system that changes very quickly—hour by hour, maybe minute by minute, as quickly as we put defences in place to protect our information security and our cybersecurity measures—as bad actors are working to try to get around those measures?

● (1150)

Dominic Rochon: Therein lies the rub. The challenge that we have on a daily basis is staying ahead of the sophisticated threat actors.

One of the members today mentioned artificial intelligence. As much as we're excited about the use of artificial intelligence for good, you could imagine that malicious actors are going to be using artificial intelligence for bad.

I'd like to distinguish between the purple team...which is still very much in pilot project format. It's something that we've just launched. We were relying on departments and agencies to self-report that they had put in place all the measures and defences that we've advocated in our policies and our cyber strategy and our vulnerability programs, etc. The purple team is going in without a department or an agency knowing about it, checking in on them and seeing if those defences are actually up to snuff. We do so in partnership with Shared Services Canada and the CSE, of course, which have the expertise and understand where those vulnerabilities might be. As those things come to light, we are able to test and discover those gaps further.

To your question specifically about how we stay ahead of the sophistication, I think that would be better suited for my colleague, Mr. Gupta, who I think releases annually or every two years the cyber-threat report. CSE is constantly looking at the sophistication that's occurring and is tailoring their services and their defences and their sensor work to counter that.

Rajiv Gupta (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Actually staying ahead of the threat is very important to us. It does change all the time, and as we lock down certain areas, other areas become the target of threat actors. That's exactly what we see on a daily basis. To stay ahead of the groups, yes, we have the purple team. Treasury Board brings in first-class industry experts to come in and see if we detect them and if others detect them as well, which is an important exercise.

The chief mentioned earlier the collaboration right across CSE and with our Five Eyes partners. We are tracking threat actors right around the globe all the time, trying to figure out what their next techniques are going to be and what exploitation efforts they're going to conduct, and we are implementing defences for this.

We host innovation workshops with the best in industry right across Canada and around the world. For example, GeekWeek, which is hosted annually, includes members of critical infrastructure—banks, telcos, etc.—as well as security companies and cloud service providers. We all come and try to figure out what those next challenges will be.

We do this on the classified side as well, with basically the best cyber-defenders in the world trying to figure out what those threats are and how we can circumvent them. It's intelligence-informed, definitely, and staying at the latest edge of technology in being able to find threats that are out there from a threat intelligence perspective, but it's also building the latest technologies as well.

You mentioned AI. It's very important for us to put out advice and guidance on how to secure AI and how organizations can safety adopt AI, but we also make extensive use of AI internally as well, making sure that we can scale, just as threat actors are scaling as well.

We're on the edge for technology development, but we're also consuming threat intelligence from ourselves, from commercial entities and from our partners to make sure that we understand what's there. We may still find some gaps and subsequently find something new, because that's the world. It's changing all the time.

The Chair: Thank you very much.

That was your time, Mr. Osborne. I believe we'll come back to you later.

[*Translation*]

Mr. Lemire, you have the floor for two and a half minutes.

Sébastien Lemire: Thank you, Mr. Chair.

In her many reports, the Auditor General highlighted the massive use of subcontractors in IT, who can access sensitive information without the required security clearances or training. Ottawa spends nearly $1 billion a year on IT services. In 2022, the number of IT subcontractors was around seven. So I think there's a huge vulnerability there.

Mr. Jones, you might be the best person to answer my question, but obviously any of you can answer.

I think we are quite vulnerable to foreign interference. We would need security guarantees. What are the security guarantees required by the government? Are checks done so that companies to whom you award a contract have the work done by people from that company, and not by subcontractors? How are you going to adapt your methods for awarding contracts to avoid using foreign workers located in countries at risk, with which there are diplomatic tensions? As the world order changes, the list of countries we can trust is quite limited.

● (1155)

Scott Jones: Thank you for the question.

I can only speak to the hiring of subcontractors and contractors by Shared Services Canada.

First, to access the Shared Services Canada system, you have to get an account from us. So we have to verify the identity of the individuals who will have access to our systems and our information.

Second, we are constantly evaluating the systems for verification, and for keeping and securing information, so that individuals can only access the information they need to do their job.

Our own security processes apply before giving an account or an ID card to access our facilities, but also to verify someone's identity and the country in which that person works.

Finally, there is also the procurement process. The contract contains clauses that require information, as well as security clearances related to Public Services and Procurement Canada's security program.

Sébastien Lemire: Thank you very much.

The Chair: Thank you very much.

[*English*]

Up next is Mr. Kuruc.

You have the floor for five minutes, please.

Ned Kuruc (Hamilton East—Stoney Creek, CPC): Hello, everybody.

Thank you for coming today, and happy new year.

My first question would be for Ms. Caroline Xavier.

In an earlier quote in a document, you said, “the rise of AI-enabled cyber threats poses significant challenges to our democratic process.” What countries would you identify as bad actors for that?

Caroline Xavier: I believe the quote you are referring to is from our document on threats to the democratic process. Almost every two years we put out a publication called “Cyber Threats to Canada's Democratic Process,” where we assess what we learn from a global perspective and what are the threats that could be of concern, especially if there is going to be a general, municipal or provincial election. We look at it purely in terms of the cyber-threat activity targeting these elections. In general, we tend to see action such as DDoS attacks, mis- and disinformation, manipulation of online systems and things of that nature.

Ned Kuruc: I'm sorry, but I have limited time.

Are you saying that it's global and there are no specific countries that you would pinpoint?

Caroline Xavier: What I was going to say is that in “Cyber Threats to Canada's Democratic Process” we have highlighted that Russia and China have the most cyber-threat activity attributed to them in terms of targeting foreign elections. It is important to note that this is on a global stage.

Ned Kuruc: Thank you very much. I appreciate your answer.

My next question is for Mr. Gupta.

You were quoted as saying, “Malicious actors are increasingly leveraging AI to enhance the scale and sophistication of their activities—including those that threaten our democratic institutions.” Could I get your expert opinion on which countries those would be?

Rajiv Gupta: I would refer to the exact same document that the chief mentioned, “Cyber Threats to Canada's Democratic Process”. That's from a democratic perspective. At the same time, AI is democratizing this capability, and I think that more and more countries will continue to stand up the ability because it's easier for countries to take advantage.

Ned Kuruc: Would you agree with the chief, then, that China and Russia would probably be the two main...amongst others, obviously?

I fully respect that it is a global issue, but I'm trying to pinpoint a few things. As Conservatives, our party has always had concerns about these issues. I want to commend you both for doing a great job, first and foremost. Now, as the Prime Minister looks to make new trade deals, it seems he's aggressively moving very quickly towards China. More importantly, it's China, but for more important communication methods, let's call it the Chinese Communist Party. That's the real concern, as opposed to China and Chinese people. It's the Communist Party that governs that country.

As a Conservative, I and many of my colleagues here are advised not to use things like TikTok, which 99% of MPs don't use for security reasons, which I'm sure you know all too well. Canadians can't buy Huawei phones. The previous government addressed that, and I agreed with that.

Now there's a big concern about Chinese EVs. Not only will it be a threat to the auto sector in Ontario, but also on a security level, Mr. Gupta, how do you feel...and what would you address? Is there a threat in bringing 50,000 Chinese EVs into our market?

● (1200)

Rajiv Gupta: From a security perspective, EVs are similar to other technology platforms. We've given out advice and guidance in terms of the increasing digitalization of critical infrastructure in general. I think that's something we need to keep a view on right across the board, because everything is becoming connected to the Internet.

With respect to EVs, we have supply chain guidance, and we have national cyber-threat assessments. We have all those things that we publish regularly on our website, and we continue to communicate these threats to Canadians. The supply chain is in one of the documents we have there as well. We also have advice and guidance as to secure communications of vehicles that we post as well. There is all that advice and guidance. I think it was mentioned earlier that you need layered defences, but you need to understand exactly what situation you're actually deploying the technologies in and what mitigations you put in place. We recommend.... For applications that are perhaps not as secure as you'd be considering, there are mitigations you can put in place, such as turning off Bluetooth and doing different sorts of things, so—

Ned Kuruc: Would there be a heightened risk, though? We can't use TikTok and Huawei, and some of our journalists and MPs have to use burner phones when they go to visit the Chinese Communist Party. Is there a higher threat in those EVs, or is it standard?

Rajiv Gupta: Right across the board, we assess risk as a number of different elements. Part of it is the supply chain, so you do look at the laws of nations as it comes in, you look at technology and the quality and implementation of software, and then you look at legal and reputational risks as well. That's our typical assessment of products. Putting all those things together gives you a general risk. You'll have products that are developed in certain ways that will have vulnerabilities based on technical deficiencies. You'll have—

Ned Kuruc: But the same is—

The Chair: Thank you. That is the time, I'm afraid, Mr. Kuruc.

Ned Kuruc: Thank you very much. I appreciate your answers.

The Chair: Up next is Ms. Tesser Derksen. You have the floor for five minutes, please.

Kristina Tesser Derksen (Milton East—Halton Hills South, Lib.): Thank you so much, Mr. Chair.

Welcome, everyone. It's great to be back.

I certainly take my colleagues' concerns to heart with respect to trade agreements with foreign countries. I know it's not anything new. I know the Conservative government back in 2014 under Stephen Harper negotiated the FIPA with China without any public debate, and quite quietly and efficiently.

It's something that's been brewing for a long time. It's something we have to keep our minds to if we're going to diversify our trade. It's something that I'm glad we have a team like you in place to help guide us through.

Getting back to the report, I want to note the staggering numbers. That's really what caught my eye at the start. We're talking about trillions of different interactions from a cybersecurity perspective. I want to maybe have you comment on the levels of threat, because I know not all of them are actual attacks. I presume many of them are innocuous, not to make light of cybersecurity threats. Could one of you—whoever feels best placed to answer—just comment on the hierarchy of characterization of the threats? There are incidents, events and then attacks.

Rajiv Gupta: Sure, I can begin.

The internet “weather” is active. You're being hit non-stop by reconnaissance. This is basically the equivalent of people coming by and wiggling your doorknobs and trying your windows. That is happening non-stop—millions of times a second. That's just so you're aware of that. Mr. Jones talked about some of the protections in terms of blocking that initial set of reconnaissance, as we call it—basically those doorknob turnings or window checks. Those are happening non-stop, so those blocks happen. Those are in the trillions.

There are the protections that we have in terms of known threats. For anything that we know about that's a threat, we actually put in blocks to try to block those things from happening. That gets into billions of blocks, as well.

Then there will be other threats that actually get through. They run through analytics. We start to find out that this thing plus this thing plus this thing makes it look suspicious and worrisome. What do we have to do with that? Then you're into tens of thousands. Some of that is actually handled by automated analytics that block things as we're sleeping, 24-7.

Within our security operations centre, which is tier two for the Government of Canada, we're looking at close to 180 different departments. From all of that automated machinery that's happening and blocking millions of things a day, we get down to maybe a few hundred alerts that actually have to be looked at by humans. We look at those and triage them. Then, every single day, if we look at 1,100 incidents for the Government of Canada, we have about six or seven of those that turn legit.

Every single day, we're actually working on real, legit incidents with our partners here, as a team. When you say that cybersecurity is a team sport.... We see each other too often—weekends, evenings, all the time. Every single day, there are about six or seven things that we're actively chasing that become legit incidents. They are typically mitigated, but sometimes they go further than others and we have to work hard together to be able to prevent them.

● (1205)

Scott Jones: Perhaps I could just jump onto what Rajiv said.

We're not used to calling each other “Mr.” and “Ms.”, because we've worked together so closely for the last 20 years.

Pat can talk about this in a little more detail, but there isn't a minute that goes by when there's not a government department under a denial-of-service attack. Pat's team right now will be mitigating that with our automated defences. You almost never notice them because of the defences and what we've layered in.

As we go through, this is where we talk about the best available commercial defences. Shared Services Canada is responsible for deploying that, making sure we maintain that, keeping it up to date and continually modernizing the commercial side of things. When it gets past those—there are threat actors that are able to get past that—that's when we turn to our colleagues at the Canadian centre for cybersecurity and the Communications Security Establishment.

That's what I would say is the “secret sauce” of the Government of Canada. It's the fact that we have this continuum. It is not separate things. It goes together. I think one of the key points in the Auditor General's report is that you bring this together and you bring a comprehensive approach to cybersecurity. Not a minute goes by when we are not suffering some sort of denial-of-service attack from all around the world.

Kristina Tesser Derksen: Thank you so much. You're quite right. I noted that in the Auditor General's report, the strategy was found to be “sound and comprehensive”. Congratulations on that.

I believe, though, that the critique from the Auditor General is that we have these tools and systems in place, but the uptake from all organizations is not 100%. I want to move into a question surrounding that.

Are there policy obstacles to these departments taking advantage of these tools? Is it a logistical issue? I know there might be a perception that it might infringe on the independence of a particular agency. Could you comment a little more on that? How can we resolve that issue?

Scott Jones: Absolutely. Thank you for the question.

I think the first thing is that the Shared Services Canada mandate is specified in an order in council. There are 44 departments that must use our service, particularly on connectivity. That is then optionally provided to a number of other entities, including, if they wish, Crown corporations and others.

As you rightly noted, there are organizations that have opted out, for independence. Primarily, if you look at the judicial branch.... The parliamentary branch has also opted out of Shared Services Canada, for reasons of independence, as you pointed out. They've done other things to compensate for that, but those were the primary things.

Many departments have chosen not to come with SSC. There are a few reasons. Number one is that it does cost more. If you're just going to run standard, commercial Internet access, the commercial defences we've layered on cost money. If you run without those, you're running at risk, but you've made a choice. You might not be able to afford it. That's what the investment in the small departments and agencies is seeking to overcome. It's funding so that they can come on to the sensors that they couldn't have afforded without that type of thing.

It is not a mandatory service. It is an optional service for most departments and agencies that they get to make a choice about. My department works on cost recovery, so they have to be able to pay the bill.

The Chair: Thank you very much.

It is my intention to get through another two full rounds. That will give the government two additional slots and give the opposition two additional slots for each round.

[*Translation*]

The Bloc Québécois will also have two turns for questions.

Mrs. Kusie, you have the floor for five minutes.

[*English*]

Stephanie Kusie: Thank you very much, Mr. Chair.

I'll start by saying that I'm very concerned that this government refers to any cyber-attack as innocuous. This is the security of our nation that is further compromised. I'm very concerned in terms of the new level of the relationship being delivered by this Prime Minister. That's very concerning to me.

Continuing with that, APT31, which hacked parliamentarians, was linked to China's intelligence service, as I indicated in the first round. In light of this finding, how can the CSE provide a guarantee that intelligence shared with China will not compromise Canadian cyber-defence security?

Caroline Xavier: First of all, it's important to recognize that no matter what amount of cyber-defence we put in place—and we have some great-quality defence in place—we can never guarantee zero cyber-incidents. Working in cyber-defence is a team sport. It's one that we're doing with all the people at this table, but in addition, an individual role has to be played when one is doing what needs to be done to protect oneself.

There is no intelligence sharing under way with regard to the CCP or the PRC. We work on a global stage with many intelligence entities as well as international bodies. That is part of what we do in the cyber-defence space because it is so important to learn from others how cyber-defence works.

I won't speak to the intent of the Prime Minister. I'll leave that for you all to discuss with him directly. I would say, though, that the role CSE plays in terms of foreign intelligence collection is very important. Particularly, when decisions are made by government, it could be informed in terms of the intent of others.

Those are the insights we provide in the work we do, in addition to all the learning from the many incidents that happen on a global scale and all the sharing we do with international bodies, including the Five Eyes, and it's the way we function, both domestically and internationally.

● (1210)

Stephanie Kusie: Thank you very much for that response.

I'll also add that former prime minister Harper had the capacity to manage our relationship to the south, a capacity that the current Prime Minister does not have. That's why he's been forced to kowtow to dictators around the world. I just want to make that very clear. Harper had the capacity to manage that relationship. This Prime Minister does not, and that's why he's forced into the hands of dictators, as we have seen throughout this week.

Can you confirm whether any technology produced by Beijing state-owned companies, as my colleague alluded to, will be blocked from being embedded into the Canadian cybersecurity operations? I'm talking about the daily ones as well, of course.

Caroline Xavier: As has been mentioned by my colleagues, part of the work we do is to ensure that any tools we use in the cyber-defence of Canada are tools that we trust and that minimize any of the vulnerabilities we're concerned about. They go through rigorous testing, rigorous assessments, and as part of the procurement contracts, we outline clear conditions that must exist.

No matter what products we will use, no matter which country they will come from, this forms the basis of the work that's required to be done, especially if we at CSE are going to use them, because we want to ensure that we continue to keep our systems secure. Therefore, it matters to pay attention to the supply chain, as mentioned earlier, and to pay attention to who the potential contractors are. They still have to undergo a very rigorous process when it comes to security, personnel security, especially if they're going to work for, and be employed by, the Communications Security Establishment.

Stephanie Kusie: Thank you.

Every one of these 20,000 EVs will be evaluated for potential malware. Is this what I'm hearing?

Caroline Xavier: This is not what I'm saying, Mr. Chair. The question asked was about whether or not we are assessing anything that's going to be used by the Communications Security Establishment. My answer to that is yes. We make sure to assess that.

I would add that, as part of the community you see at this table, our jobs will be to ensure that we give our best advice to government when it comes to whatever systems they are going to use. The other thing I would add is that we work with critical infrastructure sectors, including the transportation sector, and they are the ones who will give the advice, I assume, to the government as to the best way to do the implementation of any electric vehicles.

We have advice out, as Mr. Gupta said earlier, with regard to connected devices, and we stand behind that advice. We'll continue to learn and to improve our advice as we become more informed. This is where Bill C-8 is really important, because one of the sectors in that is the transportation sector. If that bill passes, then we'll have a better understanding of what the vulnerabilities are.

In the meantime, we continue to work and to build really great relationships with the transportation sector, and we have governance bodies that allow us to better understand what's going on there.

The Chair: Thank you very much. That is the time.

Next, we go back to Ms. Yip.

You have the floor for five minutes, please.

Jean Yip: Thank you.

We'll just say that Mr. Harper was not negotiating with President Trump. Prime Minister Carney is a pragmatist, and he's able to see that our economy really needs to be diversified.

Now I go back to the report. I'd like to ask questions of Mr. Jones and Ms. Xavier. This is in regard to the AG's report indicating that there was not a comprehensive, up-to-date inventory of all government IT devices—such as laptops, smart phones and servers—and that, while Shared Services Canada began to work to address this in 2017, the project has not been completed and is expected to continue until, at least, 2027. Why is this important, and why is it taking so long?

● (1215)

Scott Jones: I'll start. Thank you for the question.

I think it's important to note the complex environment we operate in—as I was discussing during one of the last questions—which is the complexity of the number of departments that are involved. A number of entities are responsible for managing their own inventory of goods. The other piece is that, when Shared Services was created, it was a mishmash of technology that was thrown together and handed over to this new agency, saying, “Figure it out.”

The agency didn't invest in its tooling at the beginning. There wasn't money to do that. Really, the money was to just keep it running and hope we could do that. We managed to make some good progress in things like cyber-defence with our colleagues at CSE. That is why EVAS is back on track. We had to work with the vendor. There are some things around needing to make sure the software and the packages we bought were working securely. The pandemic did delay the procurement process.

At the same time, this is a space where the market is evolving very quickly, so we have shifted from a very static project management process that is long-term to a very agile project delivery process that is about rolling out minimum viable product quickly to accelerate that. That's why we've gone from zero deployments to 35,000 desktops so far. It will be at 87,000 desktops by the end of this year, so it's starting to fill that gap. However, there are over 100 departments and agencies we have to work with. That is one of the complicating factors.

The second piece, for us, is how we make sure that information is available to those departments so they can see what their users have. It is an environment that.... There are very few organizations in the world that work the way we do, because of the vertical silos. Mr. Rochon was talking about the authorities, but then we have this horizontal organization that does infrastructure, so there are things we have to work with the vendors on. Those have all been overcome now.

Now it is about—not to trivialize this—lather, rinse, repeat: Get the deployment, get into the department, get it deployed, move to the next one and get it deployed, and do that on a priority basis to get that visibility.

Caroline Xavier: I don't know whether I have much more to add to what Scott Jones has already shared.

We are working hand-in-glove. With regard to the recommendation the OAG provided related to identifying a new platform, this is work we're doing in conjunction with our Treasury Board and Shared Services colleagues. We will, though, even without the platform, continue to at least provide a minimum viable product, as was mentioned by Scott.

Dom mentioned earlier the importance of continuing to build the relationships through tabletop exercises. That's really where it matters. It doesn't matter what systems you have, ultimately, in physically tracking these things if we're not doing a good job of ensuring that we're keeping that communication channel open, which is very much what we've worked on, improved and learned from, in terms of the OAG's report.

Jean Yip: What are the biggest barriers for your organizations to having cybersecurity defence sensors on all the devices?

Caroline Xavier: I don't know whether the Treasury Board wants to take that one. There aren't any barriers....

Dominic Rochon: It goes to one of the earlier questions in terms of whether the barriers are legal or whether they are logistical and financial. Mr. Jones adequately answered it earlier, saying there's a little bit of both.

There's a barrier in that we can impose our rules on those entities that fall under the Financial Administration Act's schedules I and II. Schedule III falls outside of our authorities. As a result, we cannot mandate Crown corporations to use CSE sensors or, indeed, to use SSC services. However, on a voluntary basis, we have reached out to all of these entities. We're looking for them to adopt our cybersecurity practices, because, of course, they're world-leading and why wouldn't you? As a result, little by little we've started to address that gap. That deals with the legal side of things.

On the logistical and financial side of things, again, as Mr. Jones pointed out, we need to understand exactly what the Internet presence is and what the technological presence is of some of these organizations and how they are set up. If they then want us to protect them, what happens if an incident occurs with one of those organizations? It costs time, effort and resources. We need to put in place the appropriate cost recovery mechanisms in order to ensure that we're able to address them.

● (1220)

The Chair: Thank you very much.

[*Translation*]

Mr. Lemire, you have the floor for two and a half minutes.

Sébastien Lemire: Thank you, Mr. Chair.

Ms. Xavier, during the Prime Minister's trip to China last week or about 10 days ago, journalists were asked not to bring their phone, but to use a temporary phone and throw it away afterwards to make sure it wouldn't be used.

When we parliamentarians travel, security checks are a given. Often, we are loaned another device to ensure that the foreign country cannot access our data and all the information we have access to as members of Parliament.

During that trip to China, an agreement was reached to import Chinese electric vehicles. I could pick up my parliamentary phone and connect to the Bluetooth network of a Chinese electric vehicle. Would you recommend I avoid doing so? Would I be putting Parliament's strategic data at risk for the benefit of the Chinese government?

Caroline Xavier: Thank you for the question.

It's a bit difficult to give a concrete answer, because those are hypothetical questions. What I would generally say, like my—

Sébastien Lemire: It's like the TikTok app, which the government asked us to delete from our phones. I've never used that app, but the government still asked me to delete it. We're also talking about Huawei phones, which were banned, and wireless networks. So it's really not hypothetical.

Caroline Xavier: Indeed, but what I was going to add is that, for the examples you mentioned—whether it's TikTok or another application—we at the Canadian Centre for Cyber Security always recommend that people pay attention to all the privacy laws of the country in which they travel. That's what we're talking about.

You specifically mentioned Beijing and China. That said, regardless of where people travel, our advice is to always pay attention to local laws. We have to ask ourselves what they are, whether we're comfortable with the laws and the networks on which data will circulate, because we don't have control over all the telecommunications networks around the world.

So it's a personal question that someone has to ask themselves when travelling, to make sure they understand the laws, problems or challenges that exist—

Sébastien Lemire: I'm talking here about the feeling people have—as elected officials or citizens—about the devices they use and connect to other sources, such as a vehicle.

I own an American electric vehicle and a Japanese hybrid vehicle, so I feel less at risk with those two countries than with China, if I had a Chinese electric vehicle.

Technologically, can countries that might want to acquire my data for strategic purposes do so through a device, for example, if I connect to the Bluetooth network?

Caroline Xavier: As Mr. Gupta said earlier, no matter where you connect, you're exposed to risk. The name of the country doesn't change that, because we're in a digital world. In that world, in terms of cybersecurity, as soon as you are connected to a telecommunications medium, you may be exposed to risk.

That said, in Canada, we work very closely with telecom companies. We have an excellent relationship with them, they work with us and they have a good understanding of the challenges, regardless of the cyber actor. They're doing what they need to do to try to protect the systems as much as possible, especially when you're using their network.

Sébastien Lemire: I have full confidence in telecom companies—

The Chair: I'm sorry, Mr. Lemire, but you will have another two and a half minutes later. I let you—

Sébastien Lemire: —but perhaps not the intermediaries.

The Chair: Mr. Lemire, I have to stop you there. I'm sorry. You will have another opportunity in a few minutes.

Mr. Deltell, you have the floor for five minutes.

● (1225)

Gérard Deltell: Thank you very much, Mr. Chair.

Ms. Xavier, let's continue the conversation about cars.

I drive a car and most of the people listening to us drive a car or an EV. I'm very happy and proud, because I've been driving an EV for two and a half years. I'm quite pleased with it. By the way, I bought a used car, which is half the price, without subsidies or commitments.

Now let's talk about electric vehicles.

The concerns raised by Mr. Kuruc and Mr. Lemire are relevant. What's going to happen? As we now know, EVs in particular are computers with wheels and an engine to propel them. It's a bit like F-35 fighter jets, which are computers with wings and bombs. First and foremost, they are essentially computers.

Have you ever received threats of cyber-attacks, unauthorized access or anything else related to EVs manufactured in Japan, South Korea, the United States or Europe? Incidentally, before we look for cars in China, we could get a few in France. They exist.

Have there ever been any cybersecurity attacks or threats related to electric cars—or any cars, for that matter, since they're all equipped with a computer? Have there ever been threats of attacks?

Caroline Xavier: I can't comment on whether there have been specific threats to electric vehicles. Certainly, based on all the information we have and all the research we do, we know, as you said, that an EV is like a computer. We understand computers and we know they can be vulnerable. Without sufficient layers of security, their vulnerability increases.

We're not a regulator. We will work very closely with Transport Canada and sectors that will implement what is needed to ensure that electric vehicles work properly. We've drafted publications that generally explain how to be cautious with all connected things, whether it's an electric vehicle or a computer. We are cybersecurity experts when it comes to understanding that threats will exploit vulnerabilities when the necessary security is not in place.

Gérard Deltell: Cars have been equipped with computers for about 20 years. To your knowledge, have drivers ever been targeted by cyber-attacks because their cars could be tracked and surveillance cameras could be used for espionage? Are you aware of such situations, yes or no?

Caroline Xavier: I can't say that I'm aware and give you a categorical yes or no answer, because not all threats in Canada are automatically reported to the Canadian Centre for Cyber Security. People are not required to report all incidents to us. It is possible that an incident involving an electric vehicle occurred, but that does not mean that we received information related to that threat. Since we conduct research globally and stay in touch with our international partners, we have a good sense that it is feasible.

Mr. Gupta, would you like to add anything?

[*English*]

Rajiv Gupta: I'm not aware of something reported to the cyber centre. That's how we would measure—

Gérard Deltell: Is that about the cars?

Rajiv Gupta: At the same time, we have done workshops to understand the new technologies. Just like other software.... There are vulnerabilities in all software. As you said, it's a computer on wheels, so there are vulnerabilities.

We would expect them to be targeted. As soon as they are targeted, they will find vulnerabilities, and just as with other software, they will continue to find them. It's just a matter of time, I would say, right across.

We will continue to look at the technologies involved in vehicles and continue to add our advice and guidance. That is something we have done. For example, we did this at a GeekWeek workshop with industry partners, just to understand what those weaknesses are and how to formulate appropriate advice and guidance and make sure that Canadians are aware.

We'll continue to work on that, but the expectation would be that layered software comes with vulnerabilities and exploitation eventually, whether it's cybercriminals, states or whoever. Basically, it's an opportunity just like other digital technologies.

[*Translation*]

Gérard Deltell: Thank you very much for that clarification, Mr. Gupta.

In today's world, cars leave a trail everywhere they go. There are cameras everywhere, so it's possible to identify individuals. It would even be possible to take control, meaning that a foreign power could take control of a vehicle. This has an impact on the daily lives of all Canadians.

Thank you.

● (1230)

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

[*English*]

Next, we'll go back to Mr. Osborne.

You have the floor for five minutes, please.

Tom Osborne: Thank you.

I just want to go back to my previous question. I was hoping to get to another. I talked about addressing the weak links.

On two occasions, we heard of the order in council impacting 44 departments and schedule III, with agencies being asked on a voluntary basis. Talking about weak links on such an important issue as cybersecurity and Canada's sovereignty in terms of national defence, this would fit in, I would anticipate, to some degree.

What are your recommendations to us, as members of the public accounts committee, in terms of going beyond a voluntary basis with the agencies and commissions of government? Hopefully they would take your advice on a voluntary basis and implement best standards, but there's no requirement for them to do so. Do you have advice for us or are there things that we can recommend to ensure they follow, or are required to follow, best practices as well?

Dominic Rochon: I'll mention that this is not a new issue. I believe it was flagged by the National Security and Intelligence Committee of Parliamentarians some five years ago now. It's something that we've been discussing and looking at. The reason we haven't found a specific recommendation to resolve it is that it's complicated—and it's complicated for a couple of reasons.

On the legislative front, if you want to add schedule III entities that have to follow our policies, it becomes difficult for agents of Parliament, for Crown corporations or organizations that don't fall 100% under the federal government purview. Making them beholden to our policies is a difficult thing to do. There are also reasons of national security. There are exemptions to our policies for very good reasons, so sometimes the voluntary route is necessary.

The other aspect that is complicated, which I mentioned as well, is that there's a cost associated with it. There are possibly some very small entities that have a very complicated way of managing their systems or perhaps maybe even an antiquated way—maybe they're using legacy systems. Imposing our cybersecurity sensors and technology is going to come at a cost. In particular, if we go into a small entity and all of a sudden turn on our sensors and find a whole bunch of things that are happening there, it's going to require resources to clean it up. Again, all of this has a significant cost, and it will take away from resources that are being applied already to the 100 departments and agencies that we're already vigilant in looking at. It will pull some of those resources toward some of these smaller entities to try to resolve and close some of these gaps.

This is what we've been discussing now for the better part of several years and trying to come up with the best solution. So far, the best solution has been to reach out to these entities, which we've done. We've written to them. Both my colleagues and.... Po Tea-Duncan, as the chief information security officer, has been writing to these organizations, in collaboration with CSE. In some cases, we've actually figured out a way of deploying our sensors and bringing them inside the tent.

Little by little, we're trying to close those gaps, and that's the best approach that we've found so far.

Caroline Xavier: Because of what Mr. Rochon just shared, I would add that we've actually seen progress in the adoption of the sensors, especially since the NSICOP report. This conversation may potentially also add the opportunity of people wanting to see how important this is.

We've done, I'd say, a full-court press with some of these Crown corporations for them to better understand the value of that. I would say that when a Crown corporation undergoes an incident and shares its experience with its sectoral colleagues, it's something we encourage a lot. All of a sudden, we also end up having more calls, because people start to learn and benefit from the practices of others.

Tom Osborne: Regarding the implementation of the SIEM system into the overall cybersecurity strategy for federal institutions, are there specific goals or milestones that you are looking to achieve?

● (1235)

Scott Jones: There are a few things that we're looking to measure. The first one is cost-effectiveness. I realize this is one of those areas where we would say, “You should spend whatever you need to protect yourself”, but the fact is that we need to maintain it within a budget and to leverage every dollar in the most effective way possible. That's something we're constantly looking at in order to do better.

Part of that is the fact that, because of where we sit, we can leverage the volume of the Government of Canada to negotiate better prices. With some of the things that we've talked about, we've actually significantly reduced the cost because of the volume. Buying 500,000 of something is much cheaper than buying one per unit type of thing. Cost-effectiveness is one.

The other one is that we maintain a tight integration with CSE. If I'm deploying something commercially, I want it to free up CSE's analytical time, so it can concentrate on the way the threat is evolving. At the same time, we want to make sure that we're automating as much as possible, so we look at how much automation we're putting in place and how much tooling we need to be able to increase productivity.

We do not have an unlimited security operations centre to be on top of these things, so with regard to automation and building things in, we expect our vendors to do that contractually. Those are all pieces that we look to leverage for measures.

The Chair: Thank you.

I'm afraid that is the time, Mr. Osborne, but we'll be back to your side for more.

Mr. Rochon, just to clarify, when you talk about entities, were you referring to Crown corporations primarily?

Dominic Rochon: Yes, schedule III is primarily for Crown corporations.

The Chair: Let me pinpoint a question on this.

Would you like to see strengthened requirements for Crown corporations to follow directions from your group?

Dominic Rochon: Personally speaking, that would be a good thing, yes.

The Chair: Thank you.

I will let other members follow if they choose to do so. We're going to begin our fourth and last round. I'm going to cut the minutes down so we don't go too much over. I might have a few questions here from the analysts at the end. The government and opposition members will have four minutes each.

[*Translation*]

Mr. Lemire will have two minutes.

[*English*]

Mr. Kuruc, you will kick us off for four minutes, please.

Ned Kuruc: Thank you.

I want to continue with some questions that I had earlier, but I want to address a few things first. In this panel here, we've heard that former prime minister Harper did trade with China regarding canola. Canola, I understand. Former prime minister Harper did not have AI cyber-threats like we do today, and 50,000 EV cars weren't in question coming into our country. I want to address that. The issue of EVs is a whole other topic.

Today, we're talking about cybersecurity, and that's what we're going to stick to. I have something here from the "National Cyber Threat Assessment 2025-2026". It says:

> The PRC conducts cyber operations against Canadian interests to serve high-level political and commercial objectives, including espionage, intellectual property (IP) theft, malign influence, and transnational repression. Among our adversaries, the PRC cyber program's scale, tradecraft, and ambitions in cyberspace are second to none.

I find it concerning that we're fielding proper questions that Canadians want to know about, and government representatives from the other side are not. This is a real threat. At the end of the day, if the Prime Minister didn't go onto the world stage and tell the whole world he's going to do business with the Chinese Communist Party with open arms, we wouldn't be asking these questions today.

On that, I have a direct question for the chief of CSE. Is Canada ready to have an open arms approach to the Chinese Communist Party on a cybersecurity level, or do we need to have a more heightened or robust...or level up to keep Canada secure?

Caroline Xavier: What I would have said, even before this conversation that's being had today, is that Canada is not immune to the threats of hostile state actors, cybercriminals and hacktivists. This is what our "National Cyber Threat Assessment" has stated—

Ned Kuruc: I would agree with you, but in light of the Prime Minister going on a world stage and virtually signalling that the Chinese Communist Party is where we're going to move forward, things have changed. I'm only speaking on behalf of the people who have called my office. It is a concern. There are many reports.

Even the former Liberal government stated that we can't use Huawei phones and this and that. That was identified. You yourself have identified China as one among many. Surely we have to have a heightened sensitivity based on the direction in which we're going. I'm not asking for concrete answers. I know this just happened a week or two ago, but this has to be formulating in your minds to keep Canada safe. That's why I asked that question.

This is a clear path forward to do business with the Chinese Communist Party, not only on canola—and maybe it will buy our LNG, which we can all get our heads around—but there are severe cybersecurity risks on what Chinese goods we're going to bring in or Chinese Communist Party goods we're going to bring in. Things are changing. You are the expert. I do recognize that, and I thank you, but the calls I'm getting.... Things have changed from two weeks ago.

Are we ready to deal with that? What steps are we taking to better deal with that?

● (1240)

Caroline Xavier: I think being ready as an institution, as a government and as a country is something we always need to be doing, because the threats we see are constantly emerging and pivoting. Part of what we do at the Communications Security Establishment is prepare for that. We analyze that and we take it from what we learned from the foreign intelligence perspective, as well as what we learned from the cyber-defence perspective. The work that I do with my Treasury Board and Shared Services colleagues is really important to ensure that the Government of Canada's systems continue to be prepared to defend against any threat.

It is factual that we see the threats evolving. It's factual that we see the threat actors pivoting and using artificial intelligence on a daily basis to be able to do what they need to do. We see it from cybercriminals as well as state actors.

The defence of Canada is something that I am proud to be part of, being part of the defence portfolio and reporting to the Minister of Defence. It is clear that in the work we're doing in that posture with the investments we've been given, we're going to continue to modernize the IT systems, and we're going to continue to ensure that our data is protected by leveraging information assurance mechanisms and encryption technology to be able to continue to ensure that whatever data we're housing will be protected.

The Chair: Thank you very much. I'm afraid that is your time.

We're going back to Ms. Tesser Derksen, please, for four minutes.

Kristina Tesser Derksen: Thank you very much, Mr. Chair.

I'm really enjoying the conversation. It's great.

I do want to note that none of us is underplaying the security risks that we face as a country, and certainly that all countries do in this changing landscape of technology. I want to address a concern that my colleague Ms. Kusie raised with respect to my use of the word “innocuous”. What I was referring to is that when I looked at the definition of a “cybersecurity event”, the actual definition is, “Events do not necessarily mean a security breach”. An example would be a user, such as myself, “logging in to a system at an unusual time”.

Of course, we have to treat all events as potential attacks—I understand that—but a large number do end up being innocuous. I'm glad that you are hypervigilant even to those innocuous events and making sure that we're properly protected, so thank you for that.

I want to continue along my line of questioning. I was getting into the Crown corporations that are not taking up the tools that are available to them.

I want to ask a question of the witnesses from the Office of the Auditor General, if I could. Some of those Crown corps, as I said, felt that using this was compromising their integrity and independence. I would describe that as a type of mindset, and I'd like to know, from the Auditor General's department, whether you find that this type of mindset is, for lack of a better word, harmful to our ability to properly protect ourselves in a cybersecurity context.

Andrew Hayes: The best way I can answer this question is that when it comes to independence, there are very few organizations that are as independent as the Office of the Auditor General, and we use these tools.

In terms of Crown corporations, I totally agree with my colleagues about the legislative structure. I would note that there are other options in the Financial Administration Act. For example, ministers have the authority to direct Crown corporations, and that's in part X of the Financial Administration Act, so there might be other ways to get at this, but the factors that have been brought up as reasons why other organizations might not be willing to make a move are valid. They have to be overcome. Another example might be that you're using a third party to provide your IT services and it's costly to have them engage with government organizations on things like this. These are things that I think the government has to tackle.

To your question about mindset, absolutely, I think every Canadian expects that the government will do everything that it can. Government organizations across the board will do everything they can to protect information and keep services going.

Kristina Tesser Derksen: Okay. I like your suggestions because—correct me if I'm wrong—I didn't actually see any recommendations in the report about how we would entice these Crown corporations to take up these tools.

● (1245)

Andrew Hayes: We didn't make recommendations directly in the report, because it is a question of policy. However, I think what we are talking about here is the importance of a clear picture across government organizations of what the threats are.

My colleagues might be able to expand on this, but the truth is that the more they have visibility into what's happening at end points and on the networks of all organizations, the better they're equipped to help everyone.

Kristina Tesser Derksen: Okay, that's excellent.

Going back to the Auditor General's team, I noticed in the preamble of your report that you note that “an initiative to set up a cyber security collaboration platform and incident case management tool had not received funding.” Can you expand on that a little bit?

Andrew Hayes: I might have to ask one of my colleagues to expand on that, but I think the challenge, when we provided the report, was that the organization had to seek funding, and that hadn't been done yet. There has been some time that has passed since we finished our report, though.

Scott Jones: This was in the context of us moving forward with the procurement that I mentioned earlier. We're in the process of finalizing the contract for the SIEM, the security incident and event management system. Procurement can always be unpredictable with challenges and some of the other pieces, but that is in its final stages right now to be able to proceed with that. What was highlighted in the report has been moved on from.

On the EVAS side of things, that has been settled, and we're now at tens of thousands of deployments.

The Chair: Thank you very much. Your time is up, I'm afraid.

[*Translation*]

Mr. Lemire, you have the floor for two minutes.

Sébastien Lemire: Thank you, Mr. Chair.

The Minister of Artificial Intelligence and Digital Innovation, Mr. Solomon, introduced a new framework on digital sovereignty. Regarding challenges and risks, it discusses the dangers of having all our data hosted in other countries—particularly the United States, where laws allow authorities to request access to information held by organizations within their borders. It also addresses the issue of dependence on big tech or data management companies.

Obviously, here, we have access to affordable renewable energy and places to house many servers—but the Canadian strategy, clearly, is to make us dependent. Even our computers are affected. I have to replace mine this week, and I'm told that all the data will be sent to the cloud.

Perhaps Mr. Jones is in the best position to answer my question. How will the new strategy affect the choices made by the various departments? People say that the Prime Minister was so clever in not naming President Trump and the United States in his famous Davos speech, but we are making ourselves extremely vulnerable to retaliation by the Americans. I'm not afraid of a tank rolling into Rouyn-Noranda, but I can certainly be afraid that President Trump will order Microsoft to pause all data devices related to Microsoft in Canada. It would paralyze our work as a whole.

Have you given any thought to that impact?

Scott Jones: Yes, absolutely. We've been thinking about this for years. During procurement processes, we add security clauses, and there's also a security assessment process, which is provided by the Communications Security Establishment, to verify the protection of information and grant a level of qualification to cloud service providers.

In addition, we added other levels of security, such as encrypting emails and other communications, to protect truly sensitive information. We also keep the keys to erase what is sent to large suppliers in any country. It's another layer of protection, and it's also effective against cyber threats.

Lastly, it's important to strike a balance between the capabilities of a system and the needs of government and technology users, because the only thing that is absolutely secure is a computer that is turned off. That doesn't work. So we always have to measure the risks we face.

Perhaps my colleagues would like to add something.

● (1250)

The Chair: Thank you very much.

[*English*]

Up next, we have Ms. Kusie for four minutes, please.

Stephanie Kusie: Thank you, Chair.

In December 2022, it was revealed that the RCMP had awarded a contract for radio frequency equipment to Sinclair Technologies, a company owned by Hytera Communications. Hytera is a Chinese telecommunications firm partly owned by the Chinese government. It was blacklisted by the U.S. Federal Communications Commission in 2021 as “an unacceptable risk to national security”. The Department of Public Safety confirmed that the RCMP did not seek a risk assessment from the CSE before awarding the contract.

Can anyone clarify if cabinet has deemed it a requirement to consult CSE before federal departments engage in contracts with foreign suppliers for products used by our security agencies?

Dominic Rochon: Maybe I'll just weigh in here.

Because of some of my previous roles at the Department of Public Safety, I know that this is something that would fall under the purview of the Investment Canada Act, not necessarily something that we would be discussing in terms of the protection of Government of Canada systems and the cybersecurity of our systems. It's more so that there's a distinction to be made, I think, in terms of a lot of the questions that have been asked of us today. I mentioned that this is a team game. One of the members of our team isn't here, and that is Public Safety. They're very much responsible for outward-facing cybersecurity. The team you see before you here today is the team responsible for securing systems within the federal government.

As I think Ms. Xavier mentioned earlier, Bill C-8 is a bill that is advocating for specific cyber-hygiene to be rolled out and implemented in four critical infrastructure sectors: namely, transportation, finance, telecommunications and energy. If that bill comes to pass, I think a lot of the issues asked of us today will be clarified, because you'll have regulators in place that will impose cyber-hygiene in these sectors in the private sector.

My apologies if I didn't address the question specifically, but I wanted to point out that there's a distinction to be made between what's happening in society writ large here in Canada and cybersecurity for that, which falls under the purview of Public Safety, and protecting systems. Obviously, there are links between the two, but I just wanted to point that out.

Stephanie Kusie: Mr. Jones, in April 2017, nearly nine years ago, your organization began developing a security incident and event management application that was to be completed by March 2023. This application had an original budget of $72.7 million. However, this was doubled in 2021 to over $144 million. Further, the Auditor General found that the product was put on hold in June 2024 pending approval of additional funding.

What is the status of this application today? How many millions of dollars has SSC spent on this project? As well, the original budget was greatly underestimated. Why is that?

Thank you.

Scott Jones: Thank you for the question. There are a few elements here. This is the project I was talking about. The contract award is forthcoming in the coming months; the number of months is low.

The second piece is that this was a space where the technology was evolving very quickly because of cybersecurity. The process was designed for a standard government procurement of heavy specifications, award, delivery over a number of years and then final delivery. That doesn't work in an agile environment with technology changing. That approach has been changed to a much more agile project delivery, where you're looking at smaller deliverables that grow over time.

Third, there were requirements that pushed the cost. The primary cost that drove it up was the requirement to hold data for a much longer time period than was necessary for critical cyber-evaluations. That is something we've worked on with our colleagues at CSE: What is reasonable and needed? Sometimes what happens is that.... It was overspecified. That's a simple way of putting it. That was brought back down to bring it back into context.

The money that's been spent has only been on the procurement processes, as we restarted this to prevent spending money on something that was overspecified and that we didn't need, but also to have something that conforms to today's cyber-environment, not 2017's. That was the primary challenge to restart this procurement and get it going. It is now back on track to deliver, but it's important to note that in the interim, the Government of Canada has always had a security incident and event management system in place. It has been in place since prior to the creation of the Canadian centre for cybersecurity, and we continue to fund that.

● (1255)

The Chair: Thank you very much.

That is Ms. Kusie's time.

Ms. Yip, I understand that you'll be sharing your time. I'll let you make the handover, or do you want me to cut you off?

Jean Yip: I will make the handover.

The Chair: All right. You have four minutes. Then I'll have some questions at the end.

Jean Yip: Okay. Thank you.

How will the publication of the guidelines on vulnerability management help resolve the issues identified in the report?

Po Tea-Duncan: Managing vulnerabilities is an important aspect. Under the policy on government security and the policy on service and digital, departments are accountable and responsible for implementing the rules we lay out. To help them with this, the guidelines on vulnerability management will help them manage their own departmental system for identifying and mitigating the vulnerabilities that are in place. Tools like endpoint visibility and awareness will help to identify some of those systems that have vulnerabilities. Once you get the data, you'll be able to identify and put in place the right controls, including patching and addressing those vulnerabilities and gaps.

That's part of the overall GC vulnerability management program, which is a program being put in place as part of the funding that was offered to TBS from budget 2024. We continue to work with our colleagues at the Canadian centre for cybersecurity, as well as Shared Services Canada, to help departments also prioritize which vulnerabilities need to be addressed within our ecosystem.

Jean Yip: I have just a quick question.

Would the new purple team—this is addressed to Mr. Jones or to Mr. Rochon—have the capabilities and resources to deal with a massive cyber-attack and, more importantly, be able to react quickly?

Po Tea-Duncan: The purple team is a proactive approach in terms of testing the controls we have in place. It's a preventative measure.

In terms of a massive cyber-attack, this is what is already in place with the teams within the Treasury Board, as well as the cyber centre, which is the lead for the instant response within the Government of Canada, working with Shared Services Canada, as well as departments and agencies that also play a role in terms of managing and responding to incidents that affect their systems.

Jean Yip: Thank you.

I'll pass it over to Mr. Osborne.

The Chair: That was perfect, Ms. Yip.

Mr. Osborne, you have two minutes.

Tom Osborne: Thank you.

This committee will undoubtedly do a report and perhaps make recommendations. I know that the Auditor General's office said that we could use part X and have ministers provide a direction. That's still not consistent across all ministers, all departments or all agencies. Whereas in most cases this may be an exception, when we make recommendations, should we be recommending that, because we are looking at national security and at the security of our information systems, we have tighter guidelines when it comes to cybersecurity?

As an extension of that, if we are allowing contracts through agencies for IT services where some of them may even use subcontractors, what measures should we look to put in place as recommendations to ensure these are trusted partners?

The Chair: Mr. Osborne, they might actually say that's your job—

Voices: Oh, oh!

The Chair —but I will hear the answers here, so please continue.

Tom Osborne: I'm looking for their opinions.

The Chair: Yes.

Your opinions, please, would be helpful.

Rajiv Gupta: I can start.

In terms of third party risk, it's very important to put those out. We have published recommended procurement guidelines for cybersecurity to be baked into these procurements—things that we would recommend—and that enables everyone. We put those out for government, but also for Canada as well. That's something we work closely on with Treasury Board and Shared Services, to make sure they're baked into all of our contracts, but we recommend them for all governments and procurement.

Dominic Rochon: Yes, the difficulty.... I mean, we keep talking about Crown corporations, but there are also parliamentary entities, judicial entities and shared governance organizations. It is a complex landscape of some of these smaller organizations.

As I said earlier, I personally welcome stronger authority to be able to impose some of the cyber-hygiene that we do impose on core public administration departments and agencies, but I'm conscious of the fact that there are other factors that come into play. We've been trying to resolve that from a gaps perspective. In reaching out, I feel like we've started to get a better understanding of what the landscape is and what some of those challenges are, but I would welcome a report from this committee suggesting perhaps additional authorities to make sure that we close those gaps once and for all.

● (1300)

The Chair: Thank you very much. That is the time.

Before I excuse everyone and end this meeting, I have two questions from our analysts that I'm going to put out there, and we'll look for a response from the relevant authority.

Number one, what is the status of the procurement of the endpoint visibility, awareness and security project?

Number two, has the government established the federal asset inventory of all applications and systems?

Scott Jones: Perhaps I'll take the first question, and then maybe my colleagues at Treasury Board can take the second.

On the enterprise vulnerability visibility project, the contract has been issued and we are now in the deployment stage. That's 37,000 deployments to date. That will accelerate to a much higher number by the end of the calendar year—I don't have the number in front of me, and I don't want to give you a wrong number—and then that will continue to accelerate into the next fiscal year as well.

Dominic Rochon: Unfortunately, the answer to the second question is that we do not have funding to follow through on that second point.

The Chair: Thank you.

Mr. Jones, would you submit the number you didn't want to reference? If you could send it to the committee in the next couple of weeks, that would be great. Thank you very much.

Mr. Hayes, are there any last comments you want to make? Okay, I just saw you.... I never want to be an auctioneer. Any move can trigger a bid.

Thank you to our witnesses for their testimony and participation in relation to the study on the report “Cyber Security of Government Networks and Systems” of the 2025 fall reports of the Auditor General. Thank you very much.

We ran a little over time, so I'll be very quick here.

I want to speak to the subcommittee members off-line right after this committee. That would be Ms. Yip, Monsieur Lemire and Ms. Kusie.

This meeting is adjourned. Thank you.