HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

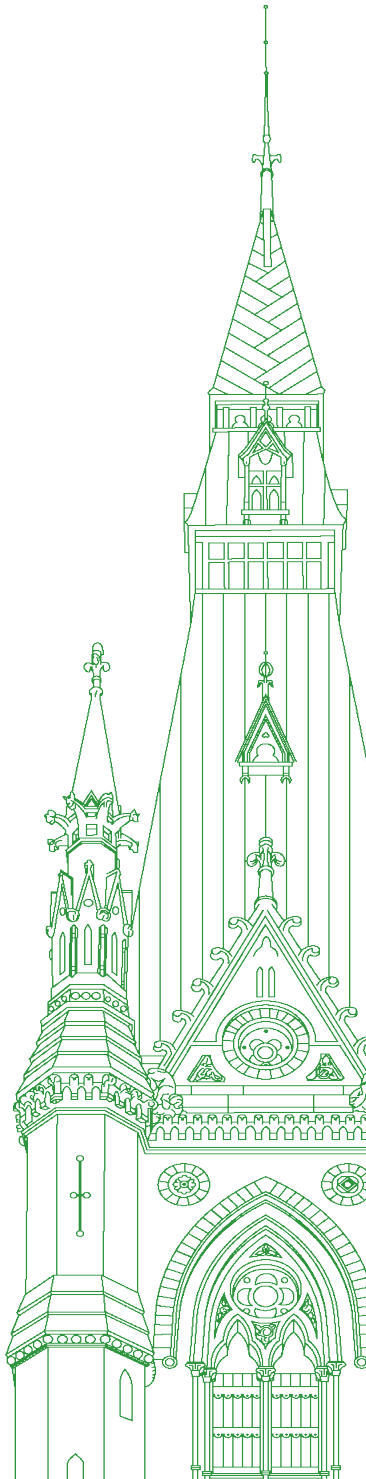
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Accounts

EVIDENCE

NUMBER 056

Thursday, March 30, 2023



Chair: Mr. John Williamson

Standing Committee on Public Accounts

Thursday, March 30, 2023

● (1530)

[*Translation*]

The Chair (Mr. John Williamson (New Brunswick Southwest, CPC)): I call this meeting to order.

Good afternoon, everyone. Welcome to the 56th meeting of the Standing Committee on Public Accounts of the House of Commons.

Pursuant to Standing Order 108(3)(g), the committee is meeting today to study Report 7, Cybersecurity of Personal Information in the Cloud, of the 2022 Reports 5 to 8 of the Auditor General of Canada.

[*English*]

I'd like to welcome our witnesses.

From the Office of the Auditor General, we have Andrew Hayes, deputy auditor general. It's good to see you.

We also have Jean Goulet, principal, and Gabriel Lombardi, principal. Thank you all for joining us.

From the Communications Security Establishment, we have Rajiv Gupta, associate head of the Canadian Centre for Cyber Security. Good day.

From the Department of Public Works and Government Services, we have Paul Thompson, deputy minister, by video conference, and Catherine Poulin, assistant deputy minister of the departmental oversight branch.

From Shared Services Canada, we have Sony Perron, president, and Costas Theophilos, director general of cloud product management and services.

From the Treasury Board Secretariat, we have Catherine Luelo, deputy minister and chief information officer of Canada.

There will be several opening statements.

Mr. Hayes, you have the floor for the first five minutes. It's over to you, please.

Mr. Andrew Hayes (Deputy Auditor General, Office of the Auditor General): Thank you very much, Mr. Chair. We appreciate this opportunity to discuss our report on cybersecurity of personal information in the cloud, which was tabled in the House of Commons on November 15, 2022.

I would like to acknowledge that this hearing is taking place on the traditional unceded territory of the Algonquin Anishinabe people. Joining me are Jean Goulet and Gabriel Lombardi, who led this audit.

Federal departments are increasingly moving software applications and databases into the cloud, including some that handle or store Canadians' personal information. Information stored digitally, whether on premises, in data centres or in the cloud, is exposed to the risk of being compromised.

In this audit, we wanted to know whether the Treasury Board of Canada Secretariat, Shared Services Canada, Public Services and Procurement Canada, Communications Security Establishment Canada and selected departments had controls in place to prevent, detect and respond to security threats to Canadians' personal information in the cloud.

Overall we found that the departments we audited did not always implement and follow the controls the government has set out to protect information that is stored and transmitted using the cloud. These controls include, as examples, encryption and network security requirements. We also found that security requirements and the corresponding roles and responsibilities were not always clear. As a result, they were not consistently implemented. This leaves cloud-based information vulnerable to cyber-attacks, which are increasingly frequent and sophisticated.

[*Translation*]

In addition, we found that 4 years after the Treasury Board of Canada Secretariat first directed federal departments to consider moving information to the cloud, it still had not provided a long-term funding plan for cloud adoption. It also had not provided a way for departments to calculate the cost of moving to cloud applications and operating in the cloud environment.

Without a funding plan and costing tools, it is difficult for government departments to ensure that they have the people, resources, and expertise they need to secure cloud-based information and respond to threats. Having these would strengthen Canada’s cyber-defence capabilities both within individual departments and government-wide.

Finally, we found that Public Services and Procurement Canada and Shared Services Canada did not require cloud service providers to demonstrate their environmental performance or to explain how their services would reduce Canada's greenhouse gas emissions. This is important because Canada has set a goal of net-zero emissions by 2050 and committed to including criteria aimed at reducing greenhouse gas emissions in the government's procurement for goods and services. To date, this has not been done for procuring cloud services.

The government needs to act now, while departments are in the early stages of transitioning to the cloud. It needs to ensure that funding is available and that key security controls to prevent, detect, and respond to cyber-attacks are strengthened. This includes clarifying shared roles and responsibilities for cybersecurity so that the departments involved, central agencies, and cloud service providers know exactly what they should be doing.

This concludes my opening remarks. We will be pleased to answer any questions the committee may have.

Thank you.

● (1535)

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

[*English*]

Next, we'll go to the Communications Security Establishment.

You have the floor for five minutes please.

Mr. Rajiv Gupta (Associate Head, Canadian Centre for Cyber Security, Communications Security Establishment): Hello. Thank you, Mr. Chair, and members of the committee, for the invitation to appear for the study of the Auditor General of Canada's report to Parliament on "Cybersecurity of Personal Information in the Cloud".

My name is Rajiv Gupta, and my pronouns are he and his. I'm the associate head of the Canadian Centre for Cyber Security at the Communications Security Establishment, also known as the cyber centre.

[*Translation*]

The Cyber Centre is Canada's technical authority for cybersecurity, safeguarding Canada with our advanced cybersecurity capabilities and providing a unified source of expert advice and support on cybersecurity operational matters.

[*English*]

I'm happy to be joined by my colleagues from Treasury Board Secretariat, Shared Services Canada and Public Services and Procurement Canada, with whom we work closely on cybersecurity matters.

As part of the cyber centre's operational role, we share cyber-alerts and threat assessments across the Government of Canada to ensure that our information systems remain secure, responsive and well defended. As part of our education role, we work to increase cybersecurity awareness across the government through initiatives like the learning hub.

[*Translation*]

The Learning Hub is based at the Cyber Centre and provides training to improve the cybersecurity of Canada's government and critical infrastructure organizations.

[*English*]

During the 2021-22 fiscal year, the learning hub renewed its collaboration with the Canada School of Public Service, CSPS, to provide a standardized cybersecurity curriculum for all—

Mr. Maninder Sidhu (Brampton East, Lib.): I have a point of order, Mr. Chair. I'm not hearing the translation.

The Chair: I'm sorry, you're not hearing the translation?

I'll just check with the clerk. One second, please.

Mr. Gupta, I'll give you a little time here. Maybe you could back up a paragraph, and slow down just a little, please. Sometimes the interpreters can't keep up. That could be the problem.

Are you hearing the translation from me now? Yes, okay.

We will go over to you, sir. Thank you.

[*Translation*]

Mr. Rajiv Gupta: Thank you very much.

As mentioned earlier, the Learning Hub is based at the Cyber Centre and provides training to improve the cybersecurity of Canada's government and critical infrastructure organizations.

[*English*]

During the 2021-22 fiscal year, the learning hub renewed its collaboration with the Canada School of Public Service to provide a standardized cybersecurity curriculum for all federal public servants. The learning hub and CSPS co-developed an e-learning course to introduce public servants from non-technical backgrounds to the basics of cloud computing. This is a priority topic for the public service as departments continue to migrate their IT infrastructure to the cloud.

Government of Canada organizations are increasingly leveraging cloud computing, which has the potential to deliver agile, flexible and cost-effective IT services. As noted in our 2021-22 annual report, CSE continues to function as a pathfinder for the GC in migrating to the cloud.

[*Translation*]

Indeed, CSE was an early adopter of cloud technology, and we ensured that we were the initial adopters of our own internal advice and guidance.

● (1540)

[*English*]

We were the first department to securely implement several commercial cloud applications, securing them with our cloud-based sensors. We demonstrated leadership by sharing the lessons learned and the relevant advice and guidance with other departments.

As I mentioned earlier, the cyber centre is the operational lead for protecting the GC from cyber-threats such as ransomware and cyber-espionage.

[*Translation*]

We work with federal partners to defend the government's networks and the sensitive information of federal institutions.

[*English*]

While there is no such thing as zero risk when it comes to cyber-threats, we are ensuring that the highest levels of protection are in place. The cyber centre uses autonomous sensors to detect malicious cyber-activity on government networks, systems and cloud infrastructure. We use three types of sensors: network-based sensors, cloud-based sensors, and host-based sensors.

These sensors allow the cyber centre to deter cyber-threats happening in real time. Our classified knowledge of threat-actor behaviour allows us to defend against and block these threats.

We work with our federal partners to ensure that the appropriate safeguards have been applied to ensure the security and the privacy of their information that is hosted in the cloud. As cloud environments continue to evolve, we are making sure that we continue to evolve our tools to ensure that the government's systems are well defended and secure.

[*Translation*]

I would like to thank the Office of the Auditor General of Canada for their report and the committee for bringing us together to discuss this important topic.

[*English*]

Although none of these recommendations outlined in the report is specific to CSE, we welcome them. CSE and the cyber centre take information security very seriously, and this includes the government's data in the cloud. We will continue to collaborate with our federal partners to move forward on these recommendations.

Members of the committee, I can assure you that CSE will continue to work with partners to bolster Canada's cybersecurity, while at the same time ensuring that the necessary protections are in place to respect Canadians' privacy.

Thank you for the opportunity to contribute to this important study, and I'm looking forward to answering any additional questions you may have.

The Chair: Thank you very much.

We turn now to the Department of Public Works and Government Services. I believe that's you, Mr. Thompson.

It's over to you, for five minutes.

Mr. Paul Thompson (Deputy Minister, Department of Public Works and Government Services): Thank you very much, Mr. Chair.

I'm pleased to be here with you and members of the committee to discuss how Public Services and Procurement Canada is responding to the audit of "Cybersecurity of Personal Information in the Cloud".

[*Translation*]

With me today is Catherine Poulin, assistant deputy minister of our Departmental Oversight Branch.

As the Government of Canada's purchaser of goods and services, my department is committed to ensuring that our procurement processes meet the needs of our client departments and agencies.

[*English*]

We appreciate the importance of cybersecurity in all facets of the Government of Canada's work. The government continues to invest in enhancing cybersecurity capabilities. For example, in budget 2023 there is a proposed $25 million for PSPC to work with National Defence and others to establish a cybersecurity certification program for defence procurements in order to further protect Canada's defence supply chain.

Looking beyond Canada's defence supply chain, we know that the use of cloud computing for software applications and databases has the potential to not only improve how we and federal organizations provide services, but also to reduce the cost and maintenance of physical services and applications.

As the government continues its strategy of using cloud computing, it is clear that departments involved will need to work more closely together to manage the security risks in the cloud.

● (1545)

[*Translation*]

With cybersecurity threats and attacks continuing to increase in frequency and severity, my department welcomed the results of the audit of the protection of personal information in cloud computing.

For its part, PSPC plays a supporting role in two key areas.

[*English*]

First, as central purchaser for the Government of Canada, PSPC procures cloud services on behalf of departments and agencies, and has established a supply arrangement with pre-qualified cloud service providers to help streamline the process. PSPC is also responsible for assessing the physical security controls of cloud service providers and their personnel.

In cases where departments procure cloud services directly through our supply arrangement, or through other procurements, we are committed to providing advice and guidance to those departments to help ensure that cloud guardrails are implemented to prevent cybersecurity breaches.

Mr. Chair, while the security of information is an important Government of Canada priority, we at PSPC are also strongly committed to doing our part on another priority, which is promoting environmental responsibility and sustainable development.

The Auditor General's report rightly pointed out that our contracting processes did not require potential cloud service providers to demonstrate their environmental performance or ask them to explain how their services would reduce Canada's greenhouse gas emissions. In addition, even when providers offered that information, there has been no mechanism in place to confirm it was accurate.

The report recommended that PSPC, in conjunction with Shared Services Canada, include environmental criteria when procuring cloud services. Doing so will help contribute to supporting sustainability and help Canada achieve its net-zero carbon emission goals.

Our departments agree with that recommendation and we have committed to taking action by working with our colleagues from Shared Services Canada to address that. This includes requiring suppliers to provide information on their commitments to achieve net-zero emissions, developing clauses in cloud computing service contracts to include GHG reduction targets, and revising the standard contracts for the procurement of cloud services and for requests for proposals.

[*Translation*]

We are also working on incorporating environmental criteria into our existing cloud procurement vehicles.

To conclude, Mr. Chair, I would like to express my thanks to the Auditor General for her report. I believe her recommendations will help guide improvements in our practices around cloud computing services.

Through continued collaboration with our partners, Public Services and Procurement Canada will be better positioned to meet our climate change obligations and ensure the security of the information of Canadians.

Thank you for your attention. I look forward to your questions.

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

[*English*]

Next is Mr. Perron from Shared Services Canada. You have the floor for five minutes, please.

Mr. Sony Perron (President, Shared Services Canada): Thank you, Mr. Chair and members of the committee, for your invitation.

I am pleased to be here today, accompanied by Costas Theophilos, director general of Cloud Product Management and Services, to address any questions the committee may have with respect to the Auditor General of Canada's audit and Shared Services Canada's progress on addressing the recommendations.

Consistent with its commitment to provide modern and secure IT infrastructure, SSC is continuously modernizing the Government of Canada's IT infrastructure. In this effort, SSC has taken an enterprise approach, which means we continue to consolidate, standardize and modernize networks and systems across government.

It is essential that we keep pace with ever-changing technology and increased cyber-threat activity. As such, over the past few years, we have significantly adopted digital solutions, including leveraging the cloud environment. It is essential that we keep pace with these changes.

Cloud adoption is a shared responsibility across the Government of Canada. Shared Services provides controlled and secure access to the cloud environment at the enterprise scale. Precisely, SSC enables cloud adoption by departments and agencies by providing access to critical building blocks, such as supply, secure cloud-to-ground network connectivity, and guidance and expertise.

In that vein, SSC works with departments to migrate their data and applications from aging data centres to modern infrastructures, such as the cloud and enterprise data centres. This accelerates the modernization of applications in an agile, secure and cost-effective way.

Protecting the information of Canadians is a top priority for SSC. This is why a common approach across departments and agencies is important. We are still in the early stages of cloud adoption; therefore, enhancement and maturing of the processes and the protocols are expected.

While there is no such thing as zero risk when it comes to cyber-threats, we are ensuring that the highest levels of protection are in place. It is important to note that all information is stored in Canada, and the most sensitive information is stored in data centres owned by the Government of Canada.

[*Translation*]

We welcome the report and recommendations of the Auditor General. This audit is helping to strengthen the operating framework for cloud services. This is particularly important at a time when reliance on the cloud environment is increasing.

SSC has a role in four of the five recommendations included in the audit.

For recommendation one, SSC is working closely with the Treasury Board Secretariat to strengthen guardrail validation and enforcement and to ensure coordination with departments. Cloud guardrails set the minimum security requirements that departments need for the configuration and the operations of their cloud environment. This includes how data is managed and where it is stored. SSC has begun the automation of the guardrails to assess compliance in real time. This will be tested with pilot departments beginning in fall 2023.

On the second recommendation, the Government of Canada set a minimum-security requirement for securing cloud-based information. SSC is working with departments to validate any outstanding cloud security controls.

On the third recommendation, to address the issue of cloud funding models, SSC is working with TBS to review the way forward as it relates to cloud costing and recovery. It is expected that the proposed cost model will be available in the near future.

And on the fourth recommendation, SSC and Public Services and Procurement Canada will soon release a standard template for cloud contracts that includes sustainability terms for cloud providers.

In fact, SSC has started to include environmental criteria in competitive solicitations under the Cloud Framework Agreement. For example, some processes now include rated criteria, encouraging suppliers to set targets to reduce their greenhouse gas emissions.

Going forward, SSC will include rated environmental criteria in all new competitive solicitations under the Government of Canada Cloud Framework Agreement.

Mr. Chair and committee members, SSC works continuously to manage cloud security risks and to enhance cybersecurity so that Canadians' data and privacy are safeguarded.

Thank you. We will be pleased to take your questions.

● (1550)

[*English*]

The Chair: Thank you very much.

Finally, from the Treasury Board, we have Ms. Luelo.

You have the floor for five minutes, please.

Ms. Catherine Luelo (Deputy Minister, Chief Information Officer of Canada, Treasury Board Secretariat): Thank you, Mr. Chair, and members of the committee. This is my first time appearing at this committee. I've met some of you, but for the others, I'm pleased to be here today.

I've been 21 months in government, having spent about 30 years in the private sector before that so I'm still in my "firsts" as I go through all of these different exercises.

As chief information officer of Canada, I provide overall leadership for the management of information technology, information management and service and digital transformation within the Government of Canada. As you see me sitting here with my colleagues today, we could have another 100 people here with all of the departments. It's a team sport to modernize digital infrastructure in government, and certainly cybersecurity is as well.

We have legislation that we manage out of my department, including access to information and open government, and we have oversight for all of the major technology programs. We have accountability for the GC cybersecurity event management plan—that's a mouthful—GC CSEMP for short.

When it comes to the protection of Canadians' personal information, we set out policies, set cybersecurity requirements, and execute decisions on the management of cybersecurity risks on behalf of the government. This is through the policy on government security, the policy on service and digital and a number of different mechanisms that sit underneath that, such as the digital standards.

I have a couple of key messages in response to the AG's report. We welcome this report, and as noted by the auditor, we're at the baby steps. We are at the beginning of the beginning. This is a beautiful time for us to be getting these findings and have an opportunity to improve. In my experience in prior organizations, a strong audit function really helps technology organizations be better, and I look forward to continued work with the Auditor General on this and other files.

As I noted, we're at the very beginning of the modernization of our technology environment. Only 35% of the systems in the Government of Canada are in a healthy state, and the cloud is a key to modernizing those systems. Cloud migration is one lever—and of note, private and public organizations all around the globe are dealing with this. I worked for several large Canadian companies, and some of the things that we've noticed here are things that we ran into in that environment.

The Government of Canada takes the protection of Canadians' information very seriously, and as Sony noted, not all services will be in the cloud. That is not our plan. We are going to have the cloud, and we are going to have enterprise data centres, and that is partially from a financial perspective and partially from a utility perspective. Cloud guardrails, a standard set of controls, are going to evolve over time. The threat landscape changes. The environment technically changes, so we'll be tuned to that. We will continue to strengthen oversight and compliance mechanisms for cloud use across government to make sure there's very clear guidance and compliance.

Since the Auditor General's report, I want to talk about a couple of areas of progress. We have updated our cloud roles and responsibilities document, and a corresponding matrix, and published it internally, so that our team members have access to that. In November 2022, we updated the Government of Canada cybersecurity event management plan. This is the plan that we put in place to respond to enterprise government cybersecurity incidents. This was first published in 2015, and we continue to test, review and tune that plan. That's normal practice with any type of a cybersecurity plan. In fact, about four weeks ago, we completed an “on guard”, which is a simulation that we run across government. It included a cloud component as part of that review, so we are starting to test our response to cyber incidents in the cloud.

In January, we also published an updated cloud strategy that had been in the works for several months. We've changed the language from “cloud first” to “cloud smart”, and that really identifies the fact that we are not always just going to go to the cloud, but are going to balance the decision-making on a number of factors, including financial.... Cloud first was exactly the right strategy for the government to move forward. We needed to start directing people into new technology, so it got the ship moving in the right direction, for lack of a better way of saying it. We have about 800 of our applications in the cloud. That's still a very small percentage of overall systems that we have across government.

● (1555)

Of note, in January, I issued guidance out of my office on the classification of personal information in the cloud and, in coordination with many of the people around this table, came to a decision that we are going to designate some high-value assets—personal information being an example—and some systems that would have an additional set of controls put in place to protect them even further. Our benefits delivery modernization program, which houses a lot of Canadians' data, is a good example of where we'll be deploying on that.

Finally, on continued development of a cloud costing model—and Sony talked about that already—we're looking to have that ready for publication in summer or fall. We've done a lot of work on that already. That is going to help departments make informed decisions about moving to the cloud, and not just the cost of moving to the cloud but the cost of operating in cloud. Both of those things are very helpful to understand. That will fulfill our responsibilities as it relates to recommendation 4.

In closing, our ultimate goal is to provide Canadians, Canadian businesses and all service users with the high-quality and efficient service that they expect in a digital age. Cloud is going to be a part of that. We will be regularly managing our progress on achieving this ambition, and cloud is an important part of that plan.

Once again, Mr. Chair, thank you for your invitation to speak to you today. I welcome any questions you may have.

The Chair: Thank you very much.

I'm just going to say a couple of words at the top.

This I think is one of the most important reports and work that government can do, because we're not just dealing with dollars and cents or policies that members and civil servants deal with all the time. We're in fact potentially dealing with the identity of Canadians, which is in some cases invaluable. I appreciate the work that you do here today. I hope the Auditor General's office will continue to prioritize this review to ensure we always have standards that keep the identity and information of Canadians safe.

I'm going to ask two quick questions, just to help other members.

Mr. Hayes, I know that there is at least one recommendation that is not public. Is there just one or is there more than one recommendation that you felt was important not to make public in this report today?

Mr. Andrew Hayes: Thank you.

There was just one recommendation.

The Chair: Thank you.

This is a general question, but I think I'm going to direct it to you, Mr. Perron, because I think you might know the answer. Is it the law currently in Canada that Government of Canada information has to be held within Canada?

Mr. Sony Perron: Yes.

The Chair: It is the law?

Mr. Sony Perron: It is the policy. I don't think it's a law. It's a policy that in fact falls under Catherine's authority.

The Chair: Thank you. I'm sure there will be questions. I just wanted to set the table for that, because there was some discussion about it.

Ms. Kusie, you have the floor for six minutes, please.

[*Translation*]

Mrs. Stephanie Kusie (Calgary Midnapore, CPC): Thank you very much, Mr. Chair.

I thank the witnesses for being with us today.

[*English*]

Monsieur Perron, on the proposed costing model that you indicated will be available this spring of 2023, would you be able to table with it the committee when it becomes available, please?

● (1600)

Mr. Sony Perron: Thank you, Mr. Chair, for the question.

This is a product that we are working on with multiple departments. We're under the leadership of the Treasury Board Secretariat. There is nothing to hide. It's something that we'll share with the departments because it's a tool, so I assume that we will be able to share it with this committee when the product is ready for distribution.

Catherine may want to add to this.

Ms. Catherine Luelo: That would be something we'd be happy to share.

Mrs. Stephanie Kusie: Thank you so much.

Will the results of these tests with pilot departments occurring in the fall of 2023 be available to be reviewed by parliamentarians and in particular by members of this committee, please?

Mr. Sony Perron: Mr. Chair, I think the member of Parliament is referring here to the automation of guardrails verification. We'll have to find a way to share that with you. What it is, basically, is that right now there are 12 guardrails. My team, following the wise advice from the Auditor General, has taken to checking not only once at the beginning but on an ongoing basis that these guardrails are maintained. It will be more a monitoring than a one-time exercise.

We are monitoring compliance of each department right now. It's just that it's not automated. It's people who belong to Costas' team who basically undertake the manual work to regularly verify around 200 instances of cloud to make sure the departments, when using this, follow the standard. Often it is only enabling a function, but if they move them, the switch to the left, this is not working anymore, so we need to make sure they maintain that, because all of this is protecting the system.

My answer is that we can come back to this committee or share with the clerk the results of our review, for sure.

Mrs. Stephanie Kusie: Thank you.

Madam Luelo, do you think the Government of Canada is matching cloud adaptation standards as seen abroad?

Ms. Catherine Luelo: I think we are experiencing things that are very similar to what other organizations do at this stage of our maturity. We are less than 10% in the cloud. I think we are adopting what are standard best practices, and I think we are learning unfortunately a lot of the same lessons that organizations learn, which is.... One of the key findings of the Auditor General's report was that we have great standards and guardrails in place, but the application of them was inconsistent, which is why the automation is so very important.

Mrs. Stephanie Kusie: Was there an international comparative analysis completed?

Ms. Catherine Luelo: Not that I'm aware of, but I might ask my colleague, who has been around the table a little longer, if there was an international benchmark done. There is not one that I'm aware of.

Mr. Sony Perron: What I know about that—and maybe our colleagues from the Centre for Cyber Security will have views—is that we often compare our practice here in Canada to the standards of the Americans on cybersecurity. We do comparisons, but again, I'm not sure we have a report that will do a broader scan.

Mr. Rajiv Gupta: I would like to add as well that in terms of our assessment of the CSPs, the cloud service providers, we do look at international standards such as ISO FedRAMP in the United States, as well as SOC 2 Type 2 reports, which are required in terms of the assessment process. We make sure that we're very harmonized with the international standards and the U.S. in that space.

Mrs. Stephanie Kusie: Thank you.

Mr. Hayes, in your audit, you mentioned that one security weakness was that contract security clauses were “unclear” and not standard. At the government operations committee, we found that in some instances contractors were able to start work on the project without a security clearance in place.

Were those the types of issues you found with Shared Services and Public Services and Procurement Canada?

Mr. Andrew Hayes: In terms of the roles and responsibilities, we were concerned that unclarity led to questions about who was on first, who was going to be dealing with issues when there was an event. We did also identify that the monitoring and oversight could be improved both by Shared Services and by PSPC.

Mrs. Stephanie Kusie: Expanding upon that, Mr. Hayes, what security measures for IT contracts were recommended by your organization?

Mr. Andrew Hayes: I won't get into the details of some of the information that we weren't able to include in the report, but what we identified was that for the guardrails for the security requirements that are in place, they should be implemented in their entirety, and ongoing monitoring should be happening as well.

Mrs. Stephanie Kusie: You also recommended in your report that cloud contracts need to have the “security requirements” clarified within the federal government. Who do you think should be taking on that role?

Mr. Andrew Hayes: In my view, this is a role for the Treasury Board Secretariat to provide guidance and policy.

Mrs. Stephanie Kusie: Thank you, Mr. Hayes.

Ms. Luelo, you mentioned that currently less than 10% of government information is on the cloud. Do you think we should be halting storing more information on the cloud until the recommendations of the Auditor General are implemented?

● (1605)

Ms. Catherine Luelo: Just to make a point of clarification, it's 10% of systems, not data. It's a little different.

Mrs. Stephanie Kusie: Pardon me. It's 10% of systems. My apologies.

Ms. Catherine Luelo: No, no, that's okay, but it's important that nuance.

I think we can continue course and speed. We have actually quite aggressively moved on the Auditor General's findings already, as I outlined in some of my remarks, and we will continue to tighten things as we move along.

There is always, as part of putting a new system into production, i.e., into the cloud, a released production activity list you go through to make sure that things have been met. We'll be disciplined in making sure that for cloud migrations, we pay very close attention to that, to ensure that we're managing that risk.

[*Translation*]

Mrs. Stephanie Kusie: Thank you very much.

Thank you, Mr. Chair.

[*English*]

The Chair: That ends your time, Ms. Kusie. Thank you.

Ms. Bradford, you have the floor for six minutes, please.

Ms. Valerie Bradford (Kitchener South—Hespeler, Lib.): Thank you, Mr. Chair.

Thank you to all of our witnesses. I think this is one of the few occasions where we have practically more witnesses than we actually have committee members. It's good to a see a full house today.

I'm going to start with a question for you, Mr. Hayes.

What percentage of the government departments that you assessed were deficient regarding their security event management plans as it pertains to cybersecurity and personal information in the cloud?

Mr. Andrew Hayes: We looked at three departments. We weren't looking across the entire government. Because it's not a representative sample or anything, our results can't be extrapolated across the government, but the areas we identified in our report related to three departments.

Ms. Valerie Bradford: Did your audit find that any information had been compromised?

Mr. Andrew Hayes: We didn't look into that degree of specificity. We were looking at the testing of their plans and the implementation of their plans.

Ms. Valerie Bradford: Mr. Gupta, what work is being done to ensure that Canadians' personal information is safe as we shift to more digital forms of storage?

Mr. Rajiv Gupta: On an ongoing basis, we're assessing the threats to cloud service providers. We're providing threat assessments on those. We're providing advice and guidance for cloud service providers, including for the government and Canadians, in terms of how to secure your cloud systems. On an ongoing basis we're seeing how the threat landscape is changing in accordance with technologies and we're making sure that our advice and guidance and information are up to par.

For the government we're also deploying cyber-defence services to make sure the technologies we deploy for the government are actually taking into account the new threat factors we're seeing from both classified and unclassified sources, and we're making sure that those technologies are implemented on our servers.

Ms. Valerie Bradford: Mr. Thompson, how does the Government of Canada ensure that cloud service providers meet the Government of Canada's security requirements?

Mr. Paul Thompson: Thank you, Mr. Chair, for that question.

I would just note that we have a physical inspection regime that has our employees doing the site inspections for cloud service providers as well as personnel security screening. Those are the two main activities that PSPC does to ensure that the cloud service providers are meeting their expectations.

Ms. Valerie Bradford: This question is for Mr. Gupta or Ms. Luelo.

Why is the government shifting from a cloud-first strategy to a cloud-smart strategy, and what does that mean operationally?

Ms. Catherine Luelo: I'll take that one and then Rajiv can add something if he wants to.

The reason we're shifting from cloud-first to cloud-smart, first of all, is that using the cloud allows us to stand things up very quickly. Where we would take potentially months to stand up an environment in which we can start building a new system for Canadians or migrating a new system for Canadians, we can do that in hours or days in cloud, so there's a huge opportunity to move more quickly to deliver service to Canadians.

We needed to get the government going in a direction because we were all data centres, and in fact SSC had an issue around the fact that they had some very old data centres. Before we just picked up and moved to a data centre, we said let's start moving some of the stuff into the cloud. As part of that, many of the things we've learned were pointed out in the Auditor General's report, including the fact that we need more maturity around our cost model. That is why we went into more of a cloud-smart model, so that we are really going to put that financial lens on migration to consider whether it's more efficient, when you put all things together, such as speed and cost, to have it in the cloud or to have it in an enterprise data centre.

So that was really the shift, and we'll continue to tune that as we go forward. As I noted in my remarks, there will never be a world in which we will be fully in the cloud, and that situation is consistent with those of many large organizations across the globe.

● (1610)

Ms. Valerie Bradford: Thank you for that. Building on that, what are the cost comparisons between managing cloud services within the government and using third party providers?

Ms. Catherine Luelo: That's the work we're undertaking right now, and it's not a one-to-one answer, because there is a cost and a benefit to speed, and there's a cost with buying computing from Amazon Web Services or Microsoft Azure versus having all of the infrastructure that Sony needs to put in place to physically operate a facility with servers and all the things that we need to host on premise.

So we really needed to do what we've done, to move some of our systems over to the cloud in order to have some real-life examples around the cost and the benefit of a cloud environment versus the cost and the benefit of an enterprise data centre, but I would say that the theory that it is less expensive to go to the cloud is not a good theory. It is also not a good theory to say that you can get the equivalent amount of agility from a data centre environment that you can get from a cloud environment. We've seen that throughout COVID and how we've been able to use cloud to move very quickly on some things.

We need to balance all of those things to come up with the right economics because it takes staffing to do things in both environments and that has costs associated with it as well.

Ms. Valerie Bradford: With the adoption of a hybrid work model in the public service, employees will need to access personal data remotely, regardless of their location. Is there a big difference, for the purpose of employee access, between cloud and on-premises data centres?

Would Mr. Perron like to answer?

Mr. Sony Perron: Thank you, Mr. Chair, for the question. That is a very good one.

We are using the cloud as a commercial solution. Catherine mentioned the name “hyperscaler”, which offers cloud. When they have been certified and we have approved utilization, they are integrated into our network. The traffic—whether it's a service, program or application in the cloud or running into a data centre—still comes to our network. The monitoring tools that a cybersecurity centre provides, and the enhanced monitoring we have on the Government of Canada networks, still apply to what we call the “workload”—let's call it the “applications”—that runs in the cloud, in the same way it would in the enterprise data centre.

It's why the security requirements, or the assessment done before we approve a hyperscaler to provide these services.... The validation of the guardrails or security control is so important, because it's one more option we have for hosting applications. Catherine explained really well the agility that comes with the cloud, but we have to do it in a safe way. We cannot lose the level of security we have built around the traditional [*Inaudible—Editor*] just because we are using a new [*Inaudible—Editor*]. We find a way to integrate that. We are never done with this. The guardrails we have today will continue to evolve and be perfected over time.

However, I think what the Auditor General reminded us about.... Did you know, now, that 200 instances of the cloud are organized and configured in line with these guardrails? Frankly, this raised the alert for us. We put the team on checking this. I was very glad to receive a report, last spring, that we were in a good place, in terms of compliance. The few departments that had challenges were notified and, with the support of the CGCIO, we got them to address it. However, this is an ongoing watch. We always have to make sure nothing is being changed and that the level of security remains there.

It's why automation is important. Human intervention in five instances is one thing. When we are at 200, 400 or 500, it will become almost impossible to have our eyes on everything, all the time. Automation is the way for us to get an alert if a guardrail is being changed by a department user. When I talk about the department, there is a small number of people who can change these. For various reasons, someone may decide to—or by mistake—change one of the configuration elements. We need to be alerted, so we can address that in a timely manner.

This is no different from when we were running data centres, before. It's just a different way to apply these guardrails.

The Chair: Okay. Thank you.

You are way over the time. You were wise not to interrupt. Committee members know that, when we have a good question, I like to hear the answer.

I'm sorry that Mr. Fragiskatos is not timing me today, because he would have to give a lot of time to the Liberal bench.

Anyway, that was a good question and a good answer. Thank you.

[*Translation*]

Ms. Sinclair-Desgagné, you have the floor for six minutes.

Ms. Nathalie Sinclair-Desgagné (Terrebonne, BQ): Thank you very much, Mr. Chair.

I thank all the witnesses for being here today. Indeed, it's important to talk about the topic at hand.

I will begin directly with a question to Mr. Hayes.

Clearly, the Office of the Auditor General is sounding the alarm not only on cybersecurity, but beyond that, as we know that cybersecurity raises security issues that exceed the cloud world.

In fact, you've sounded the alarm on two fronts. First, it's about cyber threats, so the damage we could suffer. Secondly, you pointed out a potential lack of resources and guidance that we would normally see from Treasury Board.

Did I understand your report correctly?

● (1615)

Mr. Andrew Hayes: We found deficiencies and have made recommendations to Treasury Board about them.

Ms. Nathalie Sinclair-Desgagné: That's fine, thank you.

I know that some information was not included in the report precisely because it was sensitive. Of course, we don't want to divulge the flaws in our system to unwanted parties.

Do you have any hypothetical examples you could give to inform the committee today?

Mr. Andrew Hayes: I'm thinking, for example, about the importance of following up on requirements. That's an example of information that we didn't include in the report, along with other details.

The recommendations that we made to the department were to do the things that are in the policies.

Ms. Nathalie Sinclair-Desgagné: What department are you talking about, specifically?

Mr. Andrew Hayes: Public Services and Procurement Canada.

Ms. Nathalie Sinclair-Desgagné: Who do you think should do this follow-up?

Mr. Andrew Hayes: This is something we have to do. It was important for us to put a note in our report that we made that recommendation, so that we could...

Ms. Nathalie Sinclair-Desgagné: No, excuse me. I'm talking about the deficiency you raised about the lack of follow-up.

Mr. Andrew Hayes: Yes. This was regarding Public Services and Procurement Canada.

Ms. Nathalie Sinclair-Desgagné: All right, thank you.

I'm going to ask Ms. Luelo now about Treasury Board and the lack of guidance that has been found regarding the security measures that should be in place for all departments that want to store potentially sensitive information in the cloud.

When the Office of the Auditor General sounded the alarm, did you not see fit to slow down the process of storing information in the cloud, waiting until you had sufficient security measures in place before continuing?

[*English*]

Ms. Catherine Luelo: Thank you for the question. In fact it is interesting because while the Auditor General's office was doing their assessment, a lot of work was under way. I walked you through some of the items. We had updated our GC CSEMP, our roles and responsibilities, and our policy guidance around Canadians' information in the cloud. We are kind of arriving at a destination together since we already had work in progress to remediate a lot of the things that were rightfully pointed out in the audit because we had reached a certain critical size and had therefore been doing that reflection ourselves.

Certainly there were things the Auditor General pointed out, but none, in my opinion, that are not well enough along—in terms of the improved guidance we're providing or the improved monitoring that is in place—that would cause us to slow down our progress. I would just note that our progress is very slow when you compare it to that of other organizations I've worked for. We move at a very slow pace. I would consider it a manageable risk.

[*Translation*]

Ms. Nathalie Sinclair-Desgagné: So, as I understand it, you have continued to store potentially sensitive information in the cloud.

You say you have updated everything, including your policy. After that, do you follow up to make sure the policy is being enforced across all departments?

[*English*]

Ms. Catherine Luelo: We're actually just in the process. At the beginning of April all of the departments across government will be sending in their annual plans on service and digital. It would be good for us to check those to make sure they have implemented within their plans some of the guidance we've been providing.

The second thing is for some of the larger programs that are going on. I noted our benefits delivery modernization program. We are working very closely with them as they are building out the system. They have not put data into a production environment in the cloud. I think all of the checks and balances are in place, but certainly, to Sony's point, automating this is very important. When you put humans into the equation to measure whether there's compliance, that's not a sustainable model. We will be doing regular checks with the departments, and we will continue to do the cyber-event management program. We just completed one. We do those on an annual basis. It's my belief that we have enough checks and balances in place, including, when we turn something over into production, a checklist that we go through that allows us to manage that risk.

● (1620)

[*Translation*]

The Chair: Thank you very much.

Mr. Desjarlais, you have the floor for six minutes.

[*English*]

Mr. Blake Desjarlais (Edmonton Griesbach, NDP): Thank you very much, Mr. Chair. I too want to thank the witnesses for being present with us today, and I want to thank the Auditor General's office for this really important audit.

This brings to mind particular questions amongst Canadians with respect to the confidence they have in the kinds of safety and security mechanisms there are for their personal information. I think these are some of the most critical things governments across the world are dealing with as we transform our systems into digital ones. I have learned quite a bit and I'm sure my colleagues have as well with respect to the nature of how those are being operated in the government. It was a surprise to me in many ways to hear that it's only 10% of those systems. We're really at the very start of this in some ways. I think it's incredibly important for us to get these initial aspects right. I believe this may be the first or second audit in relation to personal information when it comes to the cloud. I'm not certain whether there was one prior to this. This may be the first. Is that correct, Mr. Hayes?

Mr. Andrew Hayes: This is the first one we did that was focused on this area.

Mr. Blake Desjarlais: Thank you very much.

In some ways, we've come together with many different departments. I'd say that, oftentimes, when different departments are tasked with doing one big job, there's an issue of trying to figure out who's in charge of doing that work—in particular, the other aspects of what may not be the focus of the departments. Because of the broadness of engaging several ministries and departments, there are things that sometimes slip. Some of those things, which I think the Auditor General points out, were among some of the findings under “environment”. From paragraph 7.59 onwards, to the conclusion, there are recommendations on environment.

I noticed that, in particular, of course, Treasury Board has a mandate to ensure there are sustainability plans and environmental aspects pertaining to the work of government. It's noticed, in the report, that Public Works and Government Services was not active in the requirement to see the contracts between some of the cloud service providers to maintain information or data collection on environmental outcomes.

I just want to better understand how that process is going. This audit is a bit older, so we've had some time. I think the department has accepted the findings of the Auditor General, so I suppose my questions are for Paul.

In relation to that, what progress can you report regarding Shared Services' and PSPC's collaboration to further align the approach to the cloud procurement?

Mr. Paul Thompson: Thank you very much for the question.

I'm happy to indicate that we have now made modifications to the terms and conditions, so the supply arrangements used for cloud service providers, as of next week—as we begin the new fiscal year—will be modified to include the new requirements with respect to greenhouse gas emissions. This pertains to the broader set of procurements, but also to cloud procurements.

I'm happy to say this will be in place starting next week, so any new call-ups against those supply arrangements, or any new activity, will be subject to these new greenhouse gas emissions requirements.

Mr. Blake Desjarlais: If I understand that correctly, the 14 contracts that are currently in operation won't have those requirements.

Mr. Paul Thompson: It will be for any new call-ups against those contracts—any new activities done by these pre-qualified suppliers that are qualified for these new activities under these existing arrangements. It would require them to comply with these attestations on greenhouse gas emissions.

Mr. Blake Desjarlais: The process these providers would have to go through, in terms of declaring their greenhouse gas emissions.... Is that similar to, or consistent with, how the Canadian government collects that data, to date?

● (1625)

Mr. Paul Thompson: Thank you for that question, too. It's a good question, because we're actually changing a broader set of procurement instruments.

At the same time, there was an announcement, a couple of months ago, I believe, on broader requirements for procurement. This fits into the requirement for all procurements above $4.5 million to require this attestation, based on recognized standards for tracking greenhouse gas emissions and having a plan in place towards net zero.

Mr. Blake Desjarlais: To follow up on that, it's my understanding that your department also accepted the recommendation to look at standardizing the templates, moving forward. What's the progress on those standardized templates for these contracts?

Mr. Paul Thompson: On that one, too, I'm happy to report we have standardized contract language. A working group has been established, which is noted in the Auditor General's report. It was established over the course of the audit. We now have, essentially, a single window to work with departments and ensure we have standard language. My colleague Sony Perron's team and mine worked very closely on these new aligned instruments.

Mr. Blake Desjarlais: Who currently monitors the environmental impact of digital services within the government?

Perhaps it's a better question for Catherine.

Ms. Catherine Luelo: I do not know the answer to that, but I will refer back to the committee with a better answer than what I'll give you on the fly, here.

Thank you. It's a good question.

Mr. Blake Desjarlais: Thanks for that. Any supply of written documents on that would be helpful, as well.

Ms. Catherine Luelo: Yes.

Mr. Blake Desjarlais: I'll move on toward some of the other representatives, in relation to training.

It's my understanding that the—

Perhaps it's actually still for the member from Treasury Board.

There has been mandatory training, within the civil service, to look at sustainability and aspects of environmental declaration for information, in terms of how the government either pollutes or doesn't pollute.

How do you ensure there's actual compliance by other departments you partner with to report that information?

Ms. Catherine Luelo: Again, it's a wonderful question, but as the chief information officer of Canada, that's not within my purview. I will make sure that I go back to our greening government folks, who will have a very good answer for you on that.

Thank you.

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

I'll turn to our second round.

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

Mr. Michael Kram (Regina—Wascana, CPC): Thank you, Mr. Chair.

Thank you to all the witnesses for being here today.

I'll start with Ms. Luelo from the Treasury Board.

Why is the Government of Canada migrating data and systems to the cloud?

Ms. Catherine Luelo: The Government of Canada is migrating systems and information to the cloud for a couple of the reasons I outlined.

One is it gives us speed and agility. We've seen some of the challenges we've had in meeting service levels to Canadians. Our hope is that we create digital environments that are elastic and changeable in a different way from some of our old, more monolithic systems, if I can use that word.

The second thing is that it gives us a platform for a more modern toolset, which is a really important way for us to attract digital talent into government. I've talked often and loudly about the digital talent gap in Canada, but particularly in the Government of Canada. Part of our attracting great talent into the government to work on this mission-critical work that we do is having modern tools for those professionals to use.

Mr. Michael Kram: Your first answer was speed. Is that speed in implementing a project from start to finish or speed in other ways as well?

Ms. Catherine Luelo: Yes. It's the speed of implementing new projects, and also the speed of changing systems. Imagine introducing a new policy or program. Some of the exceptional things that were done throughout COVID were done in ways that were extraordinary. In a normal organization, where you have a good cloud footprint, you're able to stand up and build things in a much quicker fashion than in our traditional environment.

I would also note that there is an advantage to using these large-scale organizations whose full-time day job is running these environments. There are benefits for security, generally keeping things modern and not getting behind that cloud environments provide to us. I think it's a dual purpose.

If any of my colleagues would like to comment...but I think got that okay.

● (1630)

Mr. Michael Kram: Okay.

On page 15 of the report, it said that there was no costing model in place. Is there a cost-benefit analysis done before every IT project?

Is that safe to say?

Ms. Catherine Luelo: There's a cost-benefit analysis done on every project. Part of that cost-benefit analysis is what type of posting Sony provides, whether it's the cloud or the data centres.

Because we are very much at the beginning of the beginning in the Government of Canada, I would say we were not fully appreciative some of the costs of moving to the cloud, so we found it more difficult to make the move. In some cases, we did not take the opportunity to simplify and reduce the platform of what we moved to the cloud, so that increases your cost. Also, we did not have good visibility on what it costs to operate and run an environment like the cloud, because we relied on the Shared Services group to run all the data centres. It's very difficult to compartmentalize how much it costs to run Stats Canada versus CSE, versus ESDC.

Part of the great opportunity of having done a small component of this is now we have some real-world data. The other cool thing about the cloud is that we can now take environments that are in there and we can simplify and decrease them. As our consumption goes down with a cloud provider, our bill goes down. There are advantages as we start to tune and calibrate that will be reflected in cost savings.

Mr. Michael Kram: Is it safe to say that for a cost-benefit analysis for a particular project, the time savings up front in setting up a new data centre would have been included in the cost-benefit analysis for a particular project?

Is that fair to say?

Ms. Catherine Luelo: That's fair to say.

Mr. Michael Kram: Would it ever be the case that there is a project whose sole purpose is to migrate data to the cloud?

When you have an old legacy system and you're looking to redevelop it from scratch, would investigating the cloud as an option come to consideration?

Ms. Catherine Luelo: There are two scenarios that we would look at, and I'll turn to my colleague from SSC to complement the answer.

One is that we're moving something old into the cloud. Very simply put, that would include the thing the system does and the data that allows the system to do the thing it does. The second thing is that we could be standing up a net new system.

There are two reasons why we would move to the cloud. One is to get out of an old data centre and manage that risk. The second is that we're building something net new, which we did during COVID and will continue to do. It made more sense to do it in the cloud, because we could turn up an environment—which is where you build something—in days versus months.

The Chair: That is your time, Mr. Kram.

We'll turn to Ms. Yip now. You have the floor for five minutes, please.

Ms. Jean Yip (Scarborough—Agincourt, Lib.): What are the benefits of storing information digitally for service delivery to Canadians?

I'll open that up to anybody.

Ms. Catherine Luelo: If I understand your question correctly—please forgive me if I don't, and re-ask it—the benefits of having a digital service experience for Canadians could probably be best exemplified by the fact that we have Canadians who need to apply in a physical, paper format to get their passports renewed, versus having the opportunity to do that in a fully digitized format, which is what we aspire to.

What it allows for is agility and speed for the person receiving the service, and it reduces the amount of paper and number of forms that government employees need to process. There's an environmental side of that, as well, that I think is obvious.

I don't know, Sony, if you want to add to that.

Mr. Sony Perron: If I can, Mr. Chair, digital is not an option. It's where we host that data, whether it's a data centre that is controlled by the Government of Canada, or it's the cloud, or in between. The reality is, a lot of the work we are going to do going forward will be hybrid. We are going to leverage traditional data centres for some aspects of the business or the process, and we are going to leverage the cloud for some other aspects. All of this needs to be tightly connected.

The business case that is being done at the beginning is about how we optimally leverage the various hosting options. The cloud, as Catherine said, brings that option to scale up. If there is a peak in demand—think about the tax season or the passport season or the demand at the border—these systems can take much more demand if they are in the cloud, because they can ask for more computing. When there is a peak, we pay more, and when there is a lower demand, we pay less.

If it's run in a traditional data centre that I operate, I need to build a farm of servers to be able to be ready to take peak times, so it might not be cost-effective. When we do the business analysis of that, we also have to look at the cycle that some of these programs or services are going through.

This is when we get to figuring out what is the best digital hosting option. Sometimes, it's a bit in the cloud and a bit in a data centre. It really depends on the business and the type of operation. Catherine gave some examples. Each one has its own cycle and its own demands.

That data needs to be hosted somewhere and the application that computes that data needs to be hosted somewhere, so in each case, we're doing a business case.

● (1635)

Ms. Jean Yip: Thank you.

Ms. Luelo, in answering Ms. Sinclair-Desgagné's question, you mentioned that the pace remains slow. Why is that?

Ms. Catherine Luelo: I think, first of all, there are funding constraints. We are trying to manage the highest risk systems within government first, and those are big, complex systems. We're talking about immigration systems. We're talking about benefits delivery systems. Those aren't things you do quickly. They take time to do, so that's some of the built-in slowness to the system.

I would also say, putting my private sector hat on for a minute, we are highly risk-averse in government. I think part of the conversation in the digital space needs to shift to the risk of not moving a little more quickly and the risk of doing nothing, if I could be so candid as to say that.

There's a pacing element around the complexity of our systems that is normal and appropriate, and then there is a general heaviness of process and heaviness of risk aversion in the digital space that we need to tackle from a cultural perspective.

Ms. Jean Yip: What can we do to move this cultural perspective to go a little faster to maybe keep up with the private sector?

Ms. Catherine Luelo: That's an excellent question. Thank you.

I think there are things happening right now within the government in some of the committees that help manage this that are trying to move out of the way some of the systemic barriers that exist. We have things around skills and around decision-making, so I do feel we're making some progress there. I think from an overall MP perspective and ministerial perspective, it's just to support the fact that Canada is falling behind globally in digital government delivery and we can't continue to operate with the number of humans we have doing the things we have them doing.

I think as we talk about new policies and programs—and this is the advice I give to the minister whom I have the privilege of supporting—we have to ask the questions around digital-first delivery, and that includes having great digital tools for the public servants who work so hard every day to serve Canadians.

The Chair: Thank you very much.

[*Translation*]

I now yield the floor to Ms. Sinclair-Desgagné for two and a half minutes.

Ms. Nathalie Sinclair-Desgagné: Thank you, Mr. Chair.

When it comes to cost-benefit analyses, I am really in familiar territory. I have some questions about that.

First of all, a true cost-benefit analysis involves a fairly detailed risk analysis. Can you confirm that such an analysis was done?

If so, how is it that systems were implemented, only to find out that they had significant gaps and deficiencies in the end?

[*English*]

Ms. Catherine Luelo: Yes, certainly risk assessments were completed. I can confirm that, and my colleague from SSC is also confirming that.

I think we're also learning about the robustness of those risk assessments as we move to the cloud: Should we ask different questions? Should we look for different information? Certainly with respect to some of the findings by the Auditor General around the implementation of the guardrails, the two big lessons we take away have to do with automation and making sure we have put in place a good compliance framework.

● (1640)

[*Translation*]

Ms. Nathalie Sinclair-Desgagné: You say that the government is very risk-averse and therefore a risk analysis was done, but that seems contradictory to the fact that significant gaps and deficiencies were found.

Was the cost of a total government computer shutdown factored into the analysis? This is one of the risks we face, in the event of cyber-attacks. If a true cost-benefit analysis was done, I would be really surprised if the risks of a complete system shutdown were taken into account, since you still proceeded to put the system in place in an automated, cyber way, to put it that way since I don't know the exact terms so well.

Finally, I am very surprised by all of this. There is a contradiction there and I would really like to have a clear answer about that.

Ms. Catherine Luelo: Thank you very much for the question.

[*English*]

The risk aversion I'm pointing to is that it is normal for organizations that are moving through modernization to learn lessons, and we are learning some lessons. What I want to avoid is our pulling back and saying we're going to stop because a couple of things weren't done properly. We're learning from those; we're implementing, and we were thoughtful about not doing our big systems first. For example, the old age security, EI and CPP systems will come later and we will have taken the opportunity to learn from some of the smaller systems that we've moved to the cloud.

I would say your question about a whole-of-government shutdown is absolutely something that is constantly on the minds of those on this team when we think about cyber—and Sony said that very well. The cloud still allows us to have all of the protections that the Centre for Cyber Security provides. This is a unique asset we have for the Government of Canada, one that makes me feel very comfortable—a different type of asset from what I had when I worked in the private sector.

So although we have learned some things, the incredible support that we get from the cyber centre is a “compensating control”, if I can say that.

The Chair: Thank you very much.

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

Mr. Blake Desjarlais: Thank you, Mr. Chair.

I just want to mention this, before I continue: Catherine, your attendance here is quite impressive. Oftentimes, at this committee, we don't get as frank answers. It allows the MPs to do the work of this place—in particular, our committee. So really want to thank you for your honesty, because it allows us to do the work that, I think, is very important to making good recommendations in our report.

You mentioned a few things in your previous answers that I want to follow up on. One is the issue of capacity. It's the issue of talent acquisition, in particular the talent gap we have in digital services in Canada.

Could you describe what you mean by that and what that gap looks like? Is it among the IT service folks? What are you talking about when you say there's a capacity gap there?

Ms. Catherine Luelo: I would like to talk about this for 40 minutes, but I will do it very quickly, because I know we're tight for time.

We have anywhere from a 25% to a 30% vacancy rate in technical jobs in the government. That is relatively consistent, by the way, across Canada. We are seeing particular pinch points in cybersecurity, cloud computing and architecture. There are a few areas in which we are competing with companies all across Canada.

We need to do a better job of lighting up what technology people in this country do for Canadians. No one gets to do what we do. It is my mission to go out and have many more people come in and do a tour of service within government doing digital work. First of all, I think there would be a different understanding of the complexity within government and the things we need to do. I say that with all humbleness, having worked for 30 years in the private sector. I looked across and said, “What's going on in there?” I came into government and said, “Oh, my goodness, this is very complicated.”

I think it would also be great to have people from government go out into the private sector and learn what it's like to have quarterly shareholder meetings and some of the metrics that drive industry and a lot of the innovation in our country. That is a huge issue, not just for the Government of Canada but also for Canada.

● (1645)

Mr. Blake Desjarlais: I will respond quickly and try to get one more question in.

Actually, I invite you to supply our committee with a written response on the capacity recommendations you may have. I think that's an important piece. Forty minutes is a long time, but we might be able to do it in a written response.

Ms. Catherine Luelo: I'll make sure, yes.

Mr. Blake Desjarlais: Thanks so much.

John, is it two minutes and 30 seconds that I have left?

The Chair: I'm afraid your time is up, Mr. Desjarlais.

Mr. Blake Desjarlais: Well, it was a good answer.

The Chair: Yes, you squeezed a lot into that time.

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

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

I echo Mr. Desjarlais' comments. It's refreshing to come to any committee and get forthright answers and not a word salad—so far.

Mr. Hayes, Mr. Goulet and Mr. Lombardi, thanks for the report. I appreciate everything you've put into it. I want to start with the three of you.

In paragraph 7.16 in the report, you comment that the requirements for security in clouds were not followed, but you only audited three departments. Do we need to do a wider audit, if you've come up with these concerns from just the three departments you audited?

Mr. Andrew Hayes: Some of our findings relate to the central agencies' rules and the oversight, monitoring and implementation support. I think that, if the central agencies are addressing the weaknesses we found, and filling the gaps we found, we should see some better implementation.

We are planning on following up on this report on a faster basis than we would normally do, because of the fact that these are early stages and there's work to be done.

Mr. Kelly McCauley: With the central agencies.... We've seen, in other reports.... Someone in this regard actually took one of my lines, in asking about “who was on first". We've seen the departments say, "I'm not responsible.” Well, everyone's responsible, but they are saying, “We're not accountable.” In this very serious report with follow-up needed, who should be the main department that's accountable or in charge of ensuring that everyone falls in line and follows the rules, and also addresses the security issues?

Mr. Andrew Hayes: My apologies for taking your line. I think it was me who stole it, today.

Voices: Oh, oh!

Mr. Andrew Hayes: In terms of accountabilities, I'll say that departments have to be accountable for the information entrusted to them. The roles and responsibilities of the central agencies are relatively straightforward. Treasury Board provides the policy direction. It gets to the point, though—when there's an event, and the roles and responsibilities are not clear—where there might be delays, or there might be something missed along the way...or in monitoring and ongoing supervision. Who's looking at that? If there is no clarity, somebody might not actually do it.

Our point is that everybody should know exactly what they should be responsible for doing, all of the time.

Mr. Kelly McCauley: Okay.

In the next paragraph down, paragraph 7.17, you state that the government must take “immediate action”. What is immediate with respect to this report? We've seen other reports where nine years down the road we're still waiting for it. What is “immediate”? Is it one month, one year, six months...?

Mr. Andrew Hayes: We were pleased to see the time frames that were put in the responses to the recommendations. From our perspective, those are reasonable time frames to take action. Obviously, we are dealing with an ever-evolving and very dynamic field, so there has to be constant vigilance with this.

I don't know if I said that—“constant vigilance”. It was under my breath there.

Mr. Kelly McCauley: Thanks. I wasn't going to use that term, so you can have that one.

Ms. Luelo, thanks for your comments. Your direct nature today is very much appreciated. You mentioned that departments are delivering plans to you in April. Who's deciding whether those plans are acceptable? Is it you? Do they then go back to the minister or the deputy minister to say, “This is not good; resubmit”?

Ms. Catherine Luelo: That is correct. They are reviewed. I have portfolio leads within OCIO who have accountability for groupings of departments so that they're able to review them not just on an individual basis but as they compare with their colleague cohort group.

Mr. Kelly McCauley: Is there a due date in April for these?

Ms. Catherine Luelo: I believe it's April 6, but it might be April 3.

Mr. Kelly McCauley: Would you be able to provide to the committee, when they show up, which departments have met the acceptable level?

Ms. Catherine Luelo: I'd be happy to do that.

Mr. Kelly McCauley: Wonderful.

Ms. Luelo or Mr. Perron, who are the companies we're using for hosting cloud?

● (1650)

Ms. Catherine Luelo: I will let Sony answer that. Just for pure cloud services, we have eight service providers, if I have that number correctly.

I'll let my colleague from SSC answer that.

Mr. Kelly McCauley: Maybe you can just submit that to us, Mr. Perron, because I want to ask one last question.

With regard to the "on guard" tests you talked about, do you have the results or the conclusions from those tests?

Ms. Catherine Luelo: We do those on a regular basis. Since I have been with the government, we have done two. We just finished the second one, and I'm expecting the report in the next number of weeks. Typically—

Mr. Kelly McCauley: Is that something you could share with the department, maybe not the exact reports but perhaps—

Ms. Catherine Luelo: With the caveat of "anything that does not expose risk publicly", yes.

Mr. Kelly McCauley: Fantastic.

Thanks very much.

The Chair: Thank you.

Mr. Perron, are you agreeable to...? Mr. McCauley asked for a document or a response. I don't know if you caught it.

Mr. Kelly McCauley: I'm just looking for the name of the companies. I can get it from the public accounts, if you haven't got it.

Mr. Sony Perron: Mr. Chair, it would be a great pleasure to respond to this.

The Chair: I appreciate it. I just wanted to get acknowledgement of that.

We turn now to Mr. Fragiskatos.

You have the floor for five minutes.

Mr. Peter Fragiskatos (London North Centre, Lib.): Thank you very much, Chair.

Thank you to everyone for being here.

I want to look at the issue from a big-picture perspective, if I can put it that way. In looking at the report, one of the key findings, obviously, is this: "Information stored digitally, whether on-premises in data centres or in the cloud, is exposed to risks of being compromised."

I understand the importance of getting into the technical details and the minutiae, if I can follow what Mr. McCauley has asked at this meeting and at others. It is important for MPs to delve into the details that way. But I also think of it from the perspective of constituents, who want to understand this and what's being done in response in general terms as well. What is being done to address this fundamental challenge, which I see as being one of the key findings in this report?

That's for whoever wishes to take it.

Mr. Sony Perron: Maybe I can start.

This is a statement that is true in Canada. It's true everywhere in the world. It's just a pure fact that when you are in a digital world, everything is always at risk. We need to start from there. Otherwise, we won't be doing our job.

I think in Canada, for the Government of Canada, we have an infrastructure that can stand a lot. We have the process to handle these situations where there might be something detected through early intelligence but also detected on our system. We have a way to easily contain, address and remediate, but we will never be done. This is what I was saying a bit earlier. I think the point the Auditor General made at the beginning of the report is very important. Everything is at risk, and we need to always validate and enhance our safeguards.

I'm sure Catherine and Rajiv can add to this.

Mr. Peter Fragiskatos: Before they do, though, there's never going to be 100% protection. I think that's important for us to understand. That's true of not just the Canadian approach but what other democracies are finding as well, that a complete fail-safe system is not possible. That's fair.

Mr. Sony Perron: Exactly. I think it's the departure point of all work. If we work with too much security, believing we have everything in place and there will not be risk, we will be surprised pretty quickly, because the threat actors are very creative. This is where the Canadian security establishment and the cybersecurity centre are bringing us the intelligence and the signal for what we need to prepare next all the time.

Mr. Rajiv Gupta: I would agree. The premise of that comment, I assume from the report, was that we had guardrails in place and these sorts of things, but they really have to be put in place and used to have that real-life implementation and a practical result in terms of protecting the system. It's very important to have those in place. Putting the right security controls in place is very important in moving forward.

I think it's been said, but we're continuing to advance our advice and guidance on how to properly protect against the threats. We are probably the only country—that I know of—that has cloud-based sensors and a security organization monitoring the cloud environment. Though these threats exist in the cloud, they exist on premises as well. That's something that I wanted to point out. It's very important for us to keep that in mind.

Mr. Peter Fragiskatos: Mr. Perron used the phrase "threat actor". How do we keep up with threat actors?

What are the approaches that are used to constantly be monitoring the new tactics and techniques of those who would try to cause problems to our systems? How do we keep tabs on them?

● (1655)

Mr. Sony Perron: Someone was saying, “Who's first?” In fact, it's a team sport here, and sometimes with a team, there isn't a first.

However, there is a primary role for looking forward and identifying what new issues can be—which we have to prepare for, work on and anticipate—and this belongs to the Canadian Centre for Cyber Security. They are looking forward and they are bringing to the operator—which is me, or our organization—the intel. “Here's what you need to do and fix, because we believe this will be a new risk that we didn't contemplate in the past.” It's very important, and the integration with the policy lead in how we deal with this is critical.

We have this in Canada. We are lucky. We need to invest in this all the time, because we have to practise. It's good that we are doing tests, but real life also tests our ability to work together.

Mr. Peter Fragiskatos: Thank you, Mr. Perron.

The time is limited. I was going to ask about collaboration between departments, to pick up on what you were getting at, but suffice it to say I think collaboration and dialogue are taking place.

Let me ask another question, which relates to human resources.

Are you able to recruit the best and brightest into the public service to carry this out? I know there's a huge interest among young people—

The Chair: Mr. Fragiskatos, I'm going to wait for an answer. Your question has gone over, but I want to get an answer, so I'm not cutting off the answer.

Mr. Peter Fragiskatos: No problem.

Are you able to find people? Tell me about that.

Ms. Catherine Luelo: Currently, we have a cybersecurity posting that's up right now, and we are incredibly pleased with the number of applicants we've had. The Canadian Centre for Cyber Security is an employer of choice. Lots of tech folks want to work there.

The thing we are struggling with is the ability to onboard people into the system and the security clearance requirements, particularly in the cybersecurity roles. We're looking at efficiencies within the security screening policy, which I also have as part of my portfolio, to see what we can do to remove friction from the system to bring in new public servants, while making sure, particularly in the space of cybersecurity, that we are not creating any risk with those new employees. That's incredibly important.

The Chair: Thank you very much.

We're now starting our third round, which will probably be our last round, given the time, but that's still six individual members asking questions.

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

Mr. Michael Kram: Thank you, Mr. Chair.

I'd like to circle back to the auditors now.

There were a few pages in the report about “Promoting environmental responsibility and sustainable development.”

Mr. Hayes, I believe you mentioned this in your opening statement as well. Help me understand.

If I have a whole bunch of files I want to save to one cloud service, another cloud service or an in-house server, how could the environmental impact or carbon footprint be significantly different between one and the other?

Mr. Andrew Hayes: It depends on the type of services you're going to be getting.

I'm going to put a hypothetical out there. In the cloud context, if you think about an analytics service that might be very high-powered, it uses energy. How is the company that's providing that service dealing with the environmental aspect of the service it provides?

What we're asking for is for information to be provided to the government, so that they can have a clear picture of what they are procuring and whether there are environmentally preferable options. It's basically for them to go in with eyes wide open.

Mr. Michael Kram: Okay.

Maybe I will come to the representatives from the department.

I'd like to read a quote from the report. At the bottom of page 19 of the report, it says: “Although the departments requested information from providers about their environmental commitments and the status of their operations, they did not require it or confirm its accuracy when provided.”

I was wondering what information was provided and what differences there were from one option to another.

Mr. Sony Perron: Mr. Chair, that applies only to the establishment of the cloud framework agreement, where we have eight qualified vendors. We had asked initially when they were qualified—among many things we were validating—what their environmental commitment was and if they had a net-zero commitment towards 2050. We have done that. We have that in the books for seven of the vendors that were qualified at the end. What we don't necessarily have is an attestation, and I think we are working on getting that, so that it's not only a case of “I said”, but we also need to be able to demonstrate the results.

Like the team from the Auditor General looked at, not all the workload and not all the applications that we are putting in the cloud are consuming and having the same demand on the infrastructure. We need to be able to compare this if we do it in the cloud versus running this through an enterprise data centre: Do I consume more energy and do I produce more gas emissions? What will be the difference? This is something that without the addition of the clause in the contract we will not be able to do, and this is where we need to go, because otherwise, if you ask me five years from now if we're consuming less or more and producing less or more if it's in a data centre or in the cloud, I would not have the data and, frankly, if we want to advance towards these targets, we need to have it.

We are really at the beginning here. What is in the cloud is really tiny. A lot of departments are using the cloud right now for experimentation, so it's not major computing that is there. Some departments are more advanced than others, but a lot of the work we do in the cloud is really small. This is going to change in the future, and it's why we need to put these controls in place.

● (1700)

Mr. Michael Kram: Okay.

On page 18 of the report, the auditors identified this as “a missed opportunity”. Is that language maybe a bit strong? If such a tiny percentage of the data and applications has been moved to the cloud, is “missed opportunity” a bit strong? Would “potential opportunity in the future” maybe be more accurate?

Mr. Sony Perron: Well, Mr. Chair, I cannot really comment on the decision to use these words or not. I would say that you're probably right in your allusion that the potential in the future is more important than what we have done so far and in the past, but if we don't take the steps now....

Changing these clauses and including these means that my team—and Costas was part of that—is engaging with the industry on how we can do this and getting their views about how this could work, because we do not want to invent requirements and clauses that will not work for them, that cannot be built and that cannot be met in the future. There was a fair bit of work in the last few months between us and PSPC to really make sure that those who provide cloud services gave us their views about it: Would this work?

That's why we're really close to being able to release these new practices: because the industry told us that this is the right way to go, that they can comply with these requirements.

Costas, I don't know if you want to add anything.

Mr. Michael Kram: I think I'm out of time anyway—

Mr. Sony Perron: Okay.

The Chair: That is your time, Mr. Kram.

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

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): Thank you very much, Chair.

I too want to thank the witnesses for being here today.

In fact, Mr. Perron, I think I remember sitting at OGGO, the operations committee, back in 2016 and talking about Shared Services and the fact that there were still servers in closets in some departments. Am I right?

Mr. Sony Perron: It would have been my predecessor, Mr. Chair, saying that, but that is right.

Mrs. Brenda Shanahan: There we go. We've come a long way since then.

Certainly, the demands for service delivery to Canadians and for protecting data from international threats and cyber-threats and balancing that with costs are very important considerations. On the aspect of service delivery, something I found very interesting in the 2023 budget was that we're moving toward automated services, such as allowing Canadians to complete their tax returns in an automated fashion. Is this something, do you feel, where we're up to the job and able to provide this service?

Mr. Sony Perron: This is a question that would probably be better addressed by the Canada Revenue Agency.

I have to say that digital enablement is essential. In this day and age, if we want to provide agile services and deal with peak demand, we have to be digital. We have to ride the right infrastructure. Right now, a lot of the infrastructure at the Canada Revenue Agency depends on what we call “mainframe”. This was the best thing you could have, when the cloud did not exist. Now, the cloud can bring the kind of high-computing capacity and high velocity we only had with the mainframe, in the past. The mainframe is a supercomputer running in a data centre.

I think the cloud—if we stick with the theme of the audit, here—provides us with much more opportunity to do this. Sometimes, it's not only with a big program. Think about the Canada Revenue Agency. It probably has the largest programs that depend on technology in the Government of Canada. Now, with the cloud, we can have that kind of velocity for something that is way smaller, as well...and analytical work. There is great potential there.

Are we up to it? Catherine said we have a lot of challenges with talent and multiple priorities in the Government of Canada, but I believe we have done the foundational work. Hopefully, we'll have fewer servers hidden in closets.

What I want to avoid, early on, in the work we are doing on the cloud.... There are cloud instances out there that we, around this table, are not aware of. We need to manage this, as an enterprise, so we don't get into the mess that existed in the past, in terms of how we distributed the data centre and servers everywhere. We have done this cleanup. There is a lot of work still to do. We have to be very organized in the way we leverage the cloud, so we don't create this.... We leverage and build expertise. We are organized. We have common rules, so we don't expose ourselves. If there is an incident somewhere, we know what is out there and how to take back control, so we avoid the damage and consequences of incidents.

It's about being organized at the enterprise level. The players around this table are essential to make this happen.

● (1705)

Mrs. Brenda Shanahan: That's excellent.

Catherine, do you want to jump in there?

Ms. Catherine Luelo: I think it's a great question.

We don't have a choice. Canadians expect it. In every other part of their day-to-day life, they are engaging digitally with companies all over Canada.

I think—to Sony's point—we're up to the challenge, but we have a very big hill to climb. I think what we're talking about, here, is getting the right foundations in place and not being afraid that we've learned a few things...to push on, but push on in a smarter, better and more organized fashion.

Mrs. Brenda Shanahan: That's excellent.

I appreciate that you've been conscious of the cost-benefit analysis. It's already been brought up in this meeting.

I'd like Canadians to understand what the threats are that we're facing.

Mr. Gupta, how many cyber-threats and threat activities against us would you say we experience on a day-to-day basis?

Mr. Rajiv Gupta: The threat against the Government of Canada has been high for a long time. We always talk about the blocks we're doing, as the Government of Canada. In terms of activity, we say it's four to seven billion blocks per day. Those are a lot of reconnaissance activities and other sorts of threat, but the threats are still there.

We enumerated those international cyber-threat assessments, as well. Really, the sophistication of cybercrime has increased in the past few years. Nation-states are still there. We named China, Russia, Iran and North Korea as the primary countries we're worried about. We still have the sophistication of the state-sponsored threat actors, but we also have the rise of cybercrime in this space as well. That has proven to be very lucrative, I would say, from a ransomware perspective and others. It's really fuelling the threat in that space.

It's very important for us to learn from those threats, which we do on a daily basis. We are the national [*Inaudible—Editor*], so we see what's happening across Canada, to a certain extent. We also work with our partners to make sure we're taking everything we're learning from those threats and baking it into advice and guidance. We work with our partners, here, to make sure we're putting the best recommendations out, and also building that into our security analytics and the types of defensive solutions we use for the government.

We couple that, of course, with what we've learned from our signals intelligence. CSE is fortunate, in that we have the cyber centre, and also our foreign signals intelligence, which tracks cyber-threat actors around the world and gives us the intel we can use to inform our advice and guidance for Canadians.

The Chair: Thank you very much.

[*Translation*]

Ms. Sinclair-Desgagnés, you have the floor for two and a half minutes.

Ms. Nathalie Sinclair-Desgagné: Thank you, Mr. Chair.

Another aspect of a best-practice cost-benefit analysis seems not to have been included in the process, and that is concerning. According to the report, “Public Services and Procurement Canada and Shared Services Canada did not include environmental criteria in their procurement of cloud services.” Normally, really good cost-benefit analyses include environmental and social impacts.

Has this recommendation been addressed? Following the release of the report, have you begun to assess environmental impacts in contracts with companies?

Mr. Sony Perron: Thank you for the question.

As I mentioned earlier, Shared Services Canada and Public Services and Procurement Canada are committed to working with industry to determine how best to require the information necessary to assess the environmental impact of service proposals in future bids for cloud services. The consultations are complete and in a few weeks, in April, the criteria will be incorporated into the contract vehicles we have for competitive bidding.

● (1710)

Ms. Nathalie Sinclair-Desgagné: Can you give us examples of criteria that will be incorporated into it?

Mr. Sony Perron: Mr. Theophilos, do we have any details regarding the criteria that have been added?

[*English*]

Mr. Costas Theophilos (Director General, Cloud Product Management and Services, Shared Services Canada): Thank you for the question.

Just to answer that directly, the answer is that it's in alignment with Canada's commitment to reduce greenhouse gas emissions and the net zero—

[*Translation*]

Ms. Nathalie Sinclair-Desgagné: I'm sorry to interrupt, Mr. Theophilos, but I'd like to know what the criteria are, specifically.

[*English*]

Mr. Costas Theophilos: With regard to the accuracy of what they are providing, companies like Google provide their commitments on greenhouse gas emissions for their operations publicly. Seven of the eight providers that we deal with in the cloud space at Shared Services Canada have met or exceeded those targets in a public fashion. We're following up with the eighth.

[*Translation*]

Ms. Nathalie Sinclair-Desgagné: Could you please send us a list of the criteria that will be added to the contracts to evaluate the environmental impact of the proposals? More importantly, can you provide us with an implementation date for these new contracts for which environmental assessments will be conducted?

Mr. Sony Perron: As far as the second part of the question, the implementation of these contracts will be in early April. So, we are there.

In terms of the clauses that will be added to the contracts and to the calls for tenders, I'm sure Shared Services Canada or Public Services and Procurement Canada will be able to provide that information to the clerk in the next few weeks.

Ms. Nathalie Sinclair-Desgagné: Thank you very much.

The Chair: Thank you very much, Ms. Sinclair-Desgagné.

[*English*]

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

Mr. Blake Desjarlais: Thank you, Mr. Chair.

I believe it's our final round, so I want to offer my thanks to all the witnesses here today.

Thank you for your service. I think it's important that Canadians understand the value of digital infrastructure. You've been very patient with us, knowing that we're not experts in this field. I want to thank you for your accessibility in this discussion.

I do want to return to trying to understand the signals intelligence that was mentioned a few times. One fact that was submitted today, if I'm correct, and I can't remember which witness mentioned this, was that we are the only country currently utilizing signals information. Is that correct?

Mr. Rajiv Gupta: No, I would say that's not correct. It might have been a reference to cloud-based sensors, which is kind of our definition; we made up the term—

Voices: Oh, oh!

Mr. Rajiv Gupta: —so it's probably easy to say. At the same point in time, we haven't seen the analogous type of capability through the partners we work with, so I would caveat it as such.

Mr. Blake Desjarlais: I see. Okay.

What is that, exactly?

Mr. Rajiv Gupta: Basically, one of the guardrails, which is very important, is that as a government entity stands up a cloud tenancy, we have to be baked in from the start to be able to get telemetry. We get log analysis and other sorts of data that help us analyze from the start of the instantiation of this tenancy. Back at CSE we can actually look at this data and detect threats right across the board on an enterprise scale. It gives us a common enterprise monitoring standard for cloud and gives that visibility of the cloud tenancies right from the start.

Often mistakes happen early on, when people don't know how to configure their cloud tenancies right, so being baked in was very important.

Mr. Blake Desjarlais: Yes. No kidding. I can see that's a massive piece to ensuring that we have the proper safeguards.

I think one thing you mentioned earlier as well, I think in response to a question from Mr. Fragiskatos, was that in relation to the threat present to Canada, it was high. What can we do in terms of our recommendations to ensure that we can reduce that? What would you say your biggest recommendation would be for Canada to ensure that we can actually try to control this threat? I think that's a scary thing to Canadians when they hear that.

Mr. Rajiv Gupta: I'm sorry. What was the threat that was high...?

Mr. Blake Desjarlais: I think the question by Mr. Fragiskatos was in terms of the risk present to Canada, and you mentioned that the threat to Canada was quite high in terms of cybersecurity for information.

Mr. Rajiv Gupta: Oh, we've seen a high level of threat activity against the Government of Canada. Risk is different from activity. What we have seen on an ongoing basis, for the greater than a decade that I've been doing this job, is that there is a lot of threat activity against the Government of Canada. We are an interesting target for a lot of countries and a lot of cybercriminals. That has always been at a very high level.

Mr. Blake Desjarlais: What can we do to limit this risk?

Mr. Rajiv Gupta: You know, we are a prosperous country. We have things that other countries want. We have opportunities for cybercriminals, so I think that is a lot of the motivation. At the same point in time, we want to make ourselves a hard target and bake in the defences we have in order to make sure that cybercriminals don't make money off us and state-sponsored threat actors don't get the information they want.

Continuing to up our defences is probably the best way to do that.

Mr. Blake Desjarlais: That means investment.

Mr. Rajiv Gupta: Yes—as we have in the past as well with our cyber-defence services.

The Chair: Thank you very much.

Two more members will be asking questions.

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

● (1715)

Mr. Kelly McCauley: Thanks, Chair.

Mr. Hayes, I want to go back to you. In paragraph 7.19, you mentioned that you can't report some findings publicly “because doing so [would] reveal vulnerabilities” and pose a national security risk—which is fine—and said “we...reported them directly to the departments”.

Do you have assurances from the departments that these items will be addressed? Also, are these departments reporting back to you that these issues are being addressed?

Mr. Andrew Hayes: Yes. The departments responded to us on our recommendations, and we will be going back in to follow up to make sure that they are addressed. That was one of the reasons we wanted it in the report: so that it was completely transparent and you could ask us whether we have done our job.

Mr. Kelly McCauley: Is there a timeline on when they have committed to address this issue?

Mr. Andrew Hayes: Based on the recommendation we made, there was an importance to act immediately. At this point in time, I don't think there was a specific time frame in the response, but we will be looking at whether or not actions have been taken.

Mr. Kelly McCauley: Are you able to explain the nature of the issue?

Mr. Andrew Hayes: It was a monitoring and oversight kind of issue from the central agency perspective.

Mr. Kelly McCauley: Okay.

One of my colleagues in the House had an Order Paper question about data breaches. It came back with, like, 2,400 pages of data breaches suffered by the government. This was in November 2021, a year and a half ago. Could any of these data breaches be directly linked to perhaps some of the shortcomings that you've identified in our security around it?

Mr. Andrew Hayes: I'm not in a position to say that. I guess what I would say in response is that the importance of preventing, detecting and acting is one of the points of emphasis from our report. Part of being in a position to be able to do that is making sure that the controls that have been established are being put in place and the monitoring and oversight are being done effectively. That is the posture that needs to be taken.

Mr. Kelly McCauley: Okay.

Ms. Luelo, you mentioned that we need to spend more money to stop falling further behind. How much? Have you identified this solely for TBS or are you speaking on behalf of Mr. Perron, who needs more money as well, or department wide...? How much money?

Ms. Catherine Luelo: In terms of a dollar value, from an overall government perspective I think the digital spend that we do is substantial, and the largest issue we have is around delivery against the work that we've committed to do. I would suggest that it is less about spending more money on digital and more about being more focused and prioritized in which digital work needs to go, applying the right resources to it and—

Mr. Kelly McCauley: I'm sorry. Did I hear wrong? I thought I heard from you that we need to invest more and spend more money to stop falling further behind.

Ms. Catherine Luelo: We need to invest more consistently. The funding model.... The way that government funds, at least to my understanding—and I'm by no means an expert—is on annual rolling basis or a programmatic view. It is also done in a very decentralized way, and that is where I would say we have challenges.

From a spend perspective, to just double-click on what Rajiv said, we do need to continue to spend in the cybersecurity, and we do need to be able to spend on skills. All of that together is the spend envelope, but we do not have a forecast, if that's the question you're asking.

Mr. Kelly McCauley: Okay.

Let me just ask you this. The main estimates just came out. Was there satisfactory money in there for what we need to do from your department?

Mr. Rajiv Gupta: From a cyber centre perspective, budget 2022 did provide a significant amount of money to CSE.

Mr. Kelly McCauley: Enough...?

Mr. Rajiv Gupta: From a cloud perspective, a lot of the monitoring we do is directly proportional to the transition or migration of departments to the cloud. As the departments migrate to the cloud, our needs will potentially grow, but currently we are able to monitor....

Mr. Kelly McCauley: I have just one last question. I'm not sure, but maybe it's for Mr. Perron

The data centres have been discussed at OGGO meetings for seven years. I remember Mr. Parker coming in and describing the data centres.

Explain this to me in simple terms. Are we migrating some of the data over to the cloud? If so, are there money savings that should be experienced in the data centres, or is this apples and oranges?

Mr. Sony Perron: Thank you for the question, Mr. Chair. It's very complicated, but I think I will start the answer.

When we close legacy data centres and bring these workloads into an enterprise data centre, yes, there are savings, because the scale and infrastructure in the enterprise data centre give us better reliability and security.

● (1720)

Mr. Kelly McCauley: In moving it over to the cloud, is there...?

Mr. Sony Perron: Usually, to make it—

The Chair: Give me one second, Mr. McCauley.

You're past your time. I'm going to let Mr. Perron speak, but, if you interrupt, I will cut the time.

Mr. Perron, I know you said it's a complicated answer, so you have the floor for about 30 seconds.

Thank you.

Mr. Sony Perron: We try to avoid what we call “lift and shift” by taking a workload from a legacy data centre and bringing it to the cloud. There is an element of modernization, and there is a business there. I think, as my colleague explained a bit earlier, the analysis of each case depends on the effort we'll put into the modernization and how we are going to spread.... I think I can provide you with more, if you are interested.

In the last supplementary estimates C, we had savings in PSPC, which funded its transfer back to SSC. That's because we are consuming less space and closing legacy data centres. Thus, there are savings with the consolidation—at least within the infrastructure.

Thank you.

The Chair: Thank you very much.

Mr. Sidhu, you have the last five-minute round. The floor is yours, sir.

Mr. Maninder Sidhu: Thank you, Mr. Chair.

Thanks to the witnesses for being with us here, today.

I know cybersecurity is something our government is very seized with. Many different departments and ministers are involved.

Mr. Gupta, you mentioned we need to continue to invest in cybersecurity. Cybersecurity is included in our recently announced $2.3-billion Indo-Pacific strategy. I'm not sure whether you're able to shed a little more light...in terms of allies or friendlies that are doing a good job and from which we can learn best practices.

Are there countries we can look to, when we talk about cybersecurity?

Mr. Rajiv Gupta: Certainly, we work very closely with our Five Eyes alliance. We have a very good understanding as to what they're all doing.

At the same point in time, as a cyber centre, we work with like-minded allies around the world, as well, and try our best to learn from their best practices, in order to make sure we're up to speed. We'll be growing that into the Indo-Pacific, as well, to build further allies and relationships in those places.

Mr. Maninder Sidhu: Wonderful.

Is there something that stands out to you that the U.S., Australia, the U.K. or one of these countries is doing, perhaps, which you think we can bring to Canada?

Mr. Rajiv Gupta: Obviously, we do a lot of information sharing and help each other out. That's very important. I think, from a government perspective, we're fairly well positioned, in terms of how we have built up our ecosystem. We'll continue to learn in the critical infrastructure space as we go forward. It's a bit of [*Inaudible—Editor*].

Mr. Maninder Sidhu: Thank you.

Ms. Luelo, you mentioned there are roughly 800 services under cloud management at this time. You said that's a very small fraction. How many programs are there that need to be brought in?

Ms. Catherine Luelo: At this point, part of the work we're going through is analyzing what that right number is going to be. I can say that 50% will go to the cloud and 50% will stay in data centres, but we have not defined that completely, yet. I think that's a reasonable proxy. Again, not all systems are equal.

There is flexibility in the cloud, where we can stand things up, then roll things down when we don't need them any longer. That's a little different from the traditional data centre. Part of that will be informed by the financial modelling work we're going to do, because we want to make sure we're getting the best value for Canadians.

Mr. Maninder Sidhu: Thank you for that.

In terms of cost efficiencies, I know that, when we're looking at a server room, the equipment ages and there's more maintenance. I'm guessing that's one of the reasons why we're looking at the cloud for longevity and savings.

Is that your approach?

Ms. Catherine Luelo: Yes, very much so. It's not needing to buy, install and keep updating our own equipment. That is the accountability of a cloud service provider. It puts us on a path of ever-fresh modernization, which would be a very good path to be on.

Mr. Maninder Sidhu: Mr. Chair, how much time do I have?

The Chair: You have two minutes.

Mr. Maninder Sidhu: Okay. I'll give our witnesses here some time, since this is the last round.

Minister, you got cut off. Is there something you want to highlight before we end today?

Mr. Sony Perron: Mr. Chair, to continue on the last question, we have some use cases where we are doing it. There is pathfinder work here around the cloud. There are things we never did that we are doing. We never take a risk with the quality, the security, the privacy—this is always attached—but in terms of the business, we are experimenting to some extent, so it's why starting small is very important, namely, to learn and scale up.

We are working with one of our clients with whom we have a cycle where there is peak time. We are building an infrastructure, and then after a while we have to dismantle it, because it's not needed anymore. We are working with them on what the business will look like next time, because we are going to rely more on the cloud and less on the traditional infrastructure, and we are doing the cost assessment on that.

In the future, we will be able to answer a bit more these kinds of questions about how this would work.

From my perspective, one of the benefits of the cloud is the ability to go fast and to scale up and scale down. It's not the Government of Canada's obligation to decommission.... They installed all of that equipment that has been running there for a year or two. We don't have to buy this. What we are going to pay for is service.

Of course, it's a different model, because we're not going to spend capital; we are going to spend operating...on this. There will be a blip in our spending, but we will not have to invest in the infrastructure and then the installed infrastructure.

There are lots of business cases where this will make sense, but we start at a small scale, learn how it works, find the challenges we have to deal with and adjust. This is the model that paid off. I'm really glad that one of the first pathfinders was the CSE. This is where we learned a lot. This team is highly preoccupied by the security, so it was right to start on the cloud journey with an organization that has so much attention on security, because we needed to learn. We need to feel secure to put anything else in the cloud, so starting with the right use case is very important.

● (1725)

Ms. Catherine Luelo: I just have one last comment. I hope today this committee saw a little bit of the team play that's going on within government on this really important file. It does take a community to deliver digital in government. We are behind; we need to accelerate.

We're going to learn from the things that the AG pointed out. Like we said, we're very supportive of that work, and we will continue to learn as we go along this path.

I really hope that if there's nothing else productive that you take away from today's session, you take away the fact that we are working on this as a collective community.

The Chair: Thank you very much.

I just have a couple of brief questions.

Mr. Gupta, I'm not looking for a long explanation. Are data centres more secure than clouds generally?

Mr. Rajiv Gupta: We provide the controls to make sure they could be equivalently secure, but then at the same point in time you have to look at staff and skill set and having the availability, and perhaps some of the scale that cloud providers might have to apply to the problem. It's more of an operational question.

The Chair: Okay, so you're saying they can be made equivalent.

Mr. Perron, I get the impression that you're partial to the cloud because there are efficiencies. You can scale up, you can scale down, and you pay for what you use. Is that a fair assessment?

Mr. Sony Perron: It is a fair assessment.

It goes faster. If I'm asked to put together 25 servers, I will take days, weeks, to procure and install. This could be there tomorrow night if we use a hyperscaler.

The Chair: You believe that there are cost savings. Is that correct? I don't want to put words in your mouth.

Mr. Sony Perron: Mr. Chair, there are not cost savings in all instances.

There are cost savings if we are taking what Catherine described as a “smart” model or approach, or some type of.... I could use the word “workload”. It's easier to describe, rather than “data application”. There are cost savings, but we need to do the detailed analysis before we go there, because it's difficult to just go in and go out. You cannot change your mind if you build into a data centre. If you want to amortize investment, you need to be there for a while.

If we go in the cloud, we also need to learn not to stay locked in with a vendor, and have that velocity. Catherine was really blunt with the committee before, so I will be on this one. I said to the hyperscaler that these companies have not given us the right price still. Organizing together as an enterprise, being able to procure with this consolidated demand from the Government of Canada, we can get a better price from them; so we are not at the end of measuring savings, because we haven't necessarily had the best price yet.

The Chair: Thank you.

My last question goes to Mr. Hayes.

The report seems to suggest to me that, in fact, the budgeting has not been adequate. I'm going to give you the last remark on that, just to flesh that out a little bit, because you didn't get lots of questions on that. I'm curious to hear it, because it sounds like a big enterprise with so many different departments working together.

Mr. Andrew Hayes: Thank you very much for that. That is an important point I did want to emphasize if I got the chance.

What we really wanted to get at with the recommendation about the costing model, the funding framework, was really about allowing departments who are onboarding onto the cloud to see, not just the short-term costs, but also the medium and long-term costs, because a big department can absorb additional costs down the road that might be there because of the need to increase skills or tools or oversight, but it's a lot harder for smaller departments. What they have to do sometimes might be to reallocate from other places, and that puts other programs or security at risk.

This a big part of that cost-benefit analysis. If you don't know your short, medium and long-term costs then you don't really have the clear picture. I think we're all on the same page on the importance of that, and this will be something that will help to identify which things should be moving to the cloud and which shouldn't.

● (1730)

The Chair: Thank you very much.

I'll now excuse all of the witnesses. I appreciate your coming today.

The meeting is adjourned.