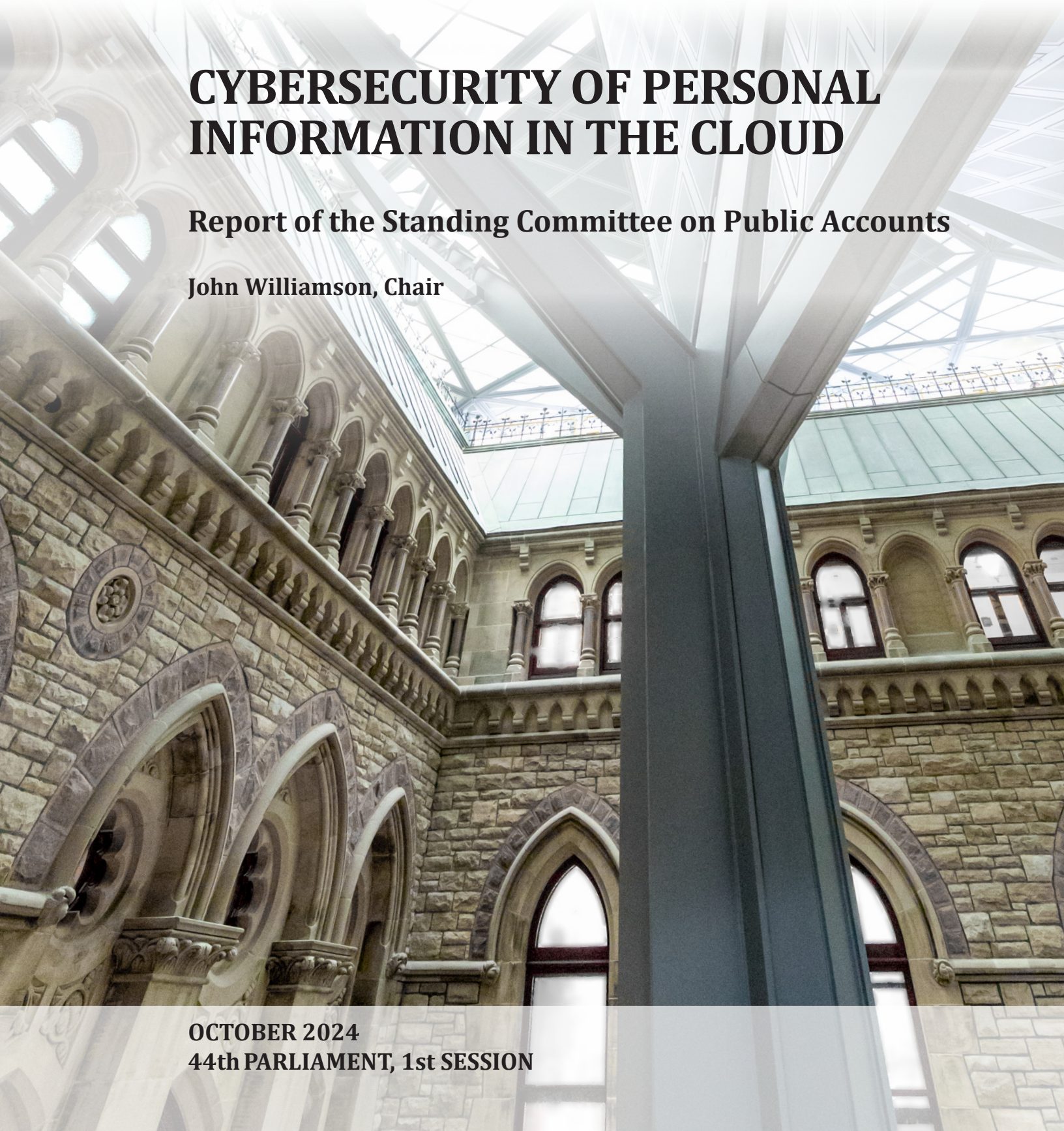
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

CYBERSECURITY OF PERSONAL INFORMATION IN THE CLOUD

Report of the Standing Committee on Public Accounts

John Williamson, Chair



OCTOBER 2024
44th PARLIAMENT, 1st SESSION

CYBERSECURITY OF PERSONAL INFORMATION IN THE CLOUD

Report of the Standing Committee on Public Accounts

John Williamson
Chair

OCTOBER 2024

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON PUBLIC ACCOUNTS

CHAIR

John Williamson

VICE-CHAIRS

Jean Yip

Nathalie Sinclair-Desgagné

MEMBERS

Valerie Bradford

Blake Desjarlais

Iqra Khalid

John Nater

Brenda Shanahan

Jake Stewart

Arnold Viersen

Patrick Weiler

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Peter Fragiskatos

Michael Kram

Stephanie Kusie

Dane Lloyd

Brian Masse

Kelly McCauley

Maninder Sidhu

CLERKS OF THE COMMITTEE

Hilary Smyth

Cédric Taquet

LIBRARY OF PARLIAMENT

Research and Education

Mahdi Benmoussa, Analyst

Dillan Theckedath, Analyst

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

has the honour to present its

FORTY-FOURTH REPORT

Pursuant to its mandate under Standing Order 108(3)(g), the committee has studied Report 7, Cybersecurity of Personal Information in the Cloud, of the 2022 Reports 5 to 8 of the Auditor General of Canada and has agreed to report the following:

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

CYBERSECURITY OF PERSONAL INFORMATION IN THE CLOUD

KEY FINDINGS OF THE AUDITOR GENERAL OF CANADA

- There were weaknesses in departments' controls for preventing, detecting, and responding to cyberattacks.
- The roles and responsibilities for ensuring cloud cybersecurity were unclear and incomplete.
- The Treasury Board of Canada Secretariat did not provide departments with a costing model or funding approach for cloud services.
- Public Services and Procurement Canada and Shared Services Canada did not include environmental criteria in their procurement of cloud services.[1]

1 Office of the Auditor General of Canada (OAG), Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, At a glance.

Summary of the Committee's Recommendations and Timelines

Table 1—Summary of the Committee's Recommendations and Timelines

Recommendation	Recommended Measure	Timeline
Recommendation 1	The Treasury Board of Canada Secretariat should provide the House of Commons Standing Committee on Public Accounts with a progress report on A) how requirements for guardrails in cloud service provider contracts that stem from supply arrangements established by Public Services and Procurement Canada have been implemented; and B) how it has clarified responsibility for the initial validation and ongoing monitoring of cloud guardrail controls and what processes are being followed.	31 January 2025
Recommendation 2	TBS should provide the Committee with a progress report on how it has ensured that the Government of Canada Cyber Security Event Management Plan applies to the evolving cloud environment and shared responsibilities. Moreover, the progress report should show how the plan will be reviewed and tested at least annually and how it is to be updated; it must also include the procedures for following up annually with departments to ensure they have finalized, implemented, and are regularly testing their own security event management plans.	31 January 2025
Recommendation 3	TBS should provide the Committee with a progress report on A) How it is documenting and proactively communicating with departments their respective roles and responsibilities for designing, implementing, validating, monitoring, coordinating, and enforcing the security controls needed to protect sensitive and personal information in the cloud; and B) What steps it has taken to ensure it is reviewing and updating these roles and responsibilities at least every 12 months.	31 January 2025

Recommendation	Recommended Measure	Timeline
Recommendation 4	TBS should provide the Committee with a progress report on A) their costing model to help departments make informed decisions about moving to the cloud and determining whether additional resources and funding are required; and B) how they are working with departments to help them determine long-term operational funding needs and support access to funding so they can fulfill their evolving responsibilities for cloud operations, including securing sensitive information.	31 January 2025
Recommendation 5	Public Services and Procurement Canada should provide the Committee with a report on the environmental criteria to be used when procuring cloud services in order to support sustainability in procurement practices and contribute to achieving Canada's net-zero goal.	31 January 2025
Recommendation 6	Shared Services Canada should provide the Committee with a report explaining its progress with regard to developing environmental criteria when procuring cloud services to support sustainability in procurement practices and contribute to achieving Canada's net-zero goal.	31 January 2025

BACKGROUND

In computing, the "cloud" refers to computer servers and the software applications and databases that run on them, located in data centres all over the world. Users do not need to own, run, or maintain their own physical servers or software applications; they can use cloud servers and applications on demand, paying for only what they need.[2]

The Treasury Board of Canada Secretariat (TBS) released the Government of Canada Cloud Adoption Strategy in 2016 and updated it in 2018. It directs federal organizations to consider the cloud as the preferred option for delivering IT. According to TBS, the benefits of cloud computing include:

2 OAG, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, para. 7.1.

- economies of scale;
- on-demand services;
- flexibility;
- services governed by contracts; and
- security.[3]

Additionally, the strategy notes that both the cloud service providers and the federal departments that use them share the responsibility for security. Yet, federal organizations remain accountable for the confidentiality, integrity, and availability of IT services and of related information that a cloud-service provider hosts. Furthermore, the TBS Digital Operations Strategic Plan: 2018–2022 "recognizes that to minimize security risks, departments that use cloud services must build cloud-savvy workforces."[4]

Between April 2018 to March 2022, Shared Services Canada (SSC) awarded contracts to 14 cloud service providers; Public Services and Procurement Canada (PSPC) established supply arrangements with them. During that time, many departments started to migrate their software applications and databases to the cloud, and also launched cloud-based applications. Specifically, between April 2018 and March 2021, federal organizations reported total spending of $210 million on cloud services.[5]

Cyberattacks can result in service shutdowns as well as the failure or even destruction of critical infrastructure (e.g., banking or electrical power distribution). Moreover, they can expose personal data, damage reputations, lead to financial costs, significantly disrupt Canadian businesses, government services, and cause hardship to individuals. Geopolitical events, such as war or political unrest, and international commercial conflicts can significantly increase cybersecurity risks.[6]

As federal organizations have begun to move software applications and databases to the cloud, more and more Canadians' personal information is being stored there. To protect personal information in the cloud, "the government has implemented a shared

3 Ibid., para. 7.2.

4 Ibid., para. 7.3.

5 Ibid., para. 7.4.

6 Ibid., para. 7.5.

responsibility model that relies on a number of parties to work together."[7] Table 2 provides information about the roles and responsibilities of TBS, SSC, PSPC, Communications Security Establishment Canada (CSEC), and individual departments.

Table 2—Various Roles and Responsibilities regarding Cybersecurity of Personal Information in the Cloud

TBS	Provides policy and guidance on cloud services, such as that contained in the Government of Canada Cloud Adoption Strategy; coordinates government-wide cybersecurity responses to incidents as outlined in the Government of Canada Cyber Security Event Management Plan.
SSC	Provides other federal departments with access to approved cloud service providers through contracts that it administers. It also manages and monitors most of the Government of Canada's computer servers and data centres and ensures secure cloud access.
PSPC	Provider of common services to government; establishes supply arrangements with prequalified cloud service providers to allow other departments to obtain the software services they offer. In some cases, departments can procure these services directly with these or other providers. For contracts that exceed certain financial thresholds, PSPC establishes and administers the contract on a department's behalf. It also assesses the physical security controls of cloud service providers and their personnel.
CSEC	As part of this agency, the Canadian Centre for Cyber Security provides Canadians with advice, guidance, services, and support on cybersecurity. This includes conducting security assessments of cloud service providers that SSC and PSPC have identified for some of their cloud-based procurement processes. It also monitors cloud security and departmental networks and provides training, advice, and guidance on cloud security. It helps federal organizations implement secure digital infrastructures.
Individual Departments	Departments (i.e., federal organizations) implement their own security controls and monitor information and user activity on their own software applications. They are ultimately responsible and accountable for security risks that arise through their use of cloud services. Departments are required to share information about privacy breaches with TBS and the Office of the Privacy Commissioner of Canada.

7 Ibid., para. 7.6.

Source: Office of the Auditor General of Canada, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, paras. 7.7 to 7.11.

On 15 November 2022, the Office of the Auditor General of Canada (OAG) released an audit that examined whether TBS, SSC, PSPC, CSEC, and selected federal departments had "adequate, effective governance, guidance, and tools in place to prevent, detect, and respond to cybersecurity events that could compromise Canadians' personal information in the cloud. For national security reasons, [the audit] does not name the selected federal departments"[8]

On 30 March 2023, the House of Commons Standing Committee on Public Accounts (the Committee) held a hearing on this audit, with the following in attendance:

> Office of the Auditor General of Canada—Andrew Hayes, Deputy Auditor General; Jean Goulet, Principal; and Gabriel Lombardi, Principal
>
> Communications Security Establishment—Rajiv Gupta, Associate Head of the Canadian Centre for Cyber Security
>
> PSPC—Paul Thompson, Deputy Minister and Catherine Poulin, Assistant Deputy Minister, Departmental Oversight Branch
>
> SSC—Sony Perron, President, and Costas Theophilos, Director General of Cloud Product Management and Services
>
> TBS, Catherine Luelo, Deputy Minister and Chief Information Officer of Canada[9]

Table 3 provides a glossary of the key terms used in this report.

Table 3—Definitions

Supply arrangement	A method used by PSPC to procure goods and services by prequalifying suppliers and establishing the basic terms and conditions that will apply to any resulting contract.

8 Ibid., para. 7.12.

9 House of Commons Standing Committee on Public Accounts, *Evidence*, 1st Session, 44th Parliament, 30 March 2023, Meeting No. 56.

Security control	Any type of safeguard or protective countermeasure used to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets; referred to these as "controls" in this report.
Validate	In the context of validating guardrails, the process of reviewing evidence to confirm that departments have implemented the guardrails as required by the Treasury Board Directive on Service and Digital.

Source: Office of the Auditor General of Canada, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, Definitions.

FINDINGS AND RECOMMENDATIONS

Guardrails Not Validated and Monitored Consistently

The OAG found that "[information] stored digitally, whether on-premises in data centres or in the cloud, is exposed to risks of being compromised."[10]

Cloud "guardrails" are a minimum set of controls that departments must implement to prevent and detect cyberattacks in their cloud environments. For contracts that SSC set up between departments and cloud service providers, it checked whether departments implemented guardrails within the first 30 days. However, it performed only limited ongoing monitoring after that. For cloud services set up by PSPC, no one validated whether departments implemented guardrails initially, and no one monitored ongoing compliance. This inconsistent application of controls across the federal government increases the risk that the personal information of Canadians in the cloud could be compromised.[11]

SSC did not assess some controls effectively and sometimes gave departments passing grades even when they did not implement the guardrails properly. And, although it validated all departments' implementation of the 12 guardrails within the first 30 days of their contracts with cloud service providers, it monitored only two of the 12 guardrails for ongoing compliance. Furthermore, for these two, it verified only administrative aspects (such as those related to billing and reporting), and not whether the guardrails

10 OAG, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, para. 7.16.

11 Ibid., paras. 7.26 and 7.28.

were still in place and working as intended. SSC left the ongoing monitoring of guardrails from a security perspective up to individual departments.[12]

Consequently, the OAG recommended that in consultation with SCC and PSPC, TBS should do the following:

- Extend the requirement for guardrails to cloud service provider contracts that stem from supply arrangements established by Public Services and Procurement Canada; and

- Clarify who is responsible for the initial validation and ongoing monitoring of cloud guardrail controls and what processes they should follow.[13]

In its Detailed Action Plan, TBS stated that it will clarify the process and roles, responsibilities for validating and monitoring of guardrails is extended to PSPC procured solutions.[14] The department also provided the following outcomes that were to be completed by 1 April 2023:

> Published Cloud Responsibility Matrix, that formally identifies who is responsible for validating, ongoing monitoring, performing oversight and compliance of the cloud guardrails controls.
>
> The Standard Operating Procedure for Validating Cloud Guardrails is clarified and extended for cloud service provider contracts awarded by PSPC.
>
> The GC Cloud Guardrails and Directive on Service and Digital is updated to reflect guardrail controls that apply to cloud services including PSPC procured cloud services.

In addition, TBS will:

- establish a score card to report on departments' level of adherence to the GC Cloud Guardrails,

12 Ibid., para. 7.30.

13 Ibid., para. 7.31.

14 Treasury Board Of Canada Secretariat (TBS), Detailed Action Plan, p. 1.

- collaborate with SSC in their efforts to implement tools to automate guardrail monitoring for cloud service providers in the Government of Canada; and

- continue to provide advice and guidance to departments on ensuring that they perform security assessment and authorization activities for cloud-based applications using tools such as the Security Playbook for Information System Solutions which outlines a set of security tasks for consideration when designing and implementing solutions for Government of Canada information systems in cloud environments.[15]

At the hearing, in response to a question about test cases for the automation of guardrail verification, Sony Perron, President, SSC, provided the following:

> 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 [situations] to make sure the departments, when using this, follow the standard.
>
> […]
>
> 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.[16]

Therefore, the Committee recommends:

Recommendation 1

That, by 31 January 2025, the Treasury Board of Canada Secretariat provide the House of Commons Standing Committee on Public Accounts with a progress report on A) how

15 Ibid.

16 House of Commons Standing Committee on Public Accounts, *Evidence*, 1st Session, 44th Parliament, 30 March 2023, Meeting No. 56, 1600 and 1610.

requirements for guardrails in cloud service provider contracts that stem from supply arrangements established by Public Services and Procurement Canada have been implemented; and B) how it has clarified responsibility for the initial validation and ongoing monitoring of cloud guardrail controls and what processes are being followed.

Shortcomings in Cybersecurity Event Management Plans

When cybersecurity events occur, the lead security agencies and individual departments must be able to coordinate and respond quickly. This requires the establishment of cybersecurity event management plans that have been tested and validated (i.e., proven effective through simulation exercises). The federal government's "ability to detect and respond to cyberattacks government-wide relies on the ability of each department to do so at its level."[17]

The OAG found that of the cloud contracts or supply arrangements procured with 14 cloud service providers, "neither department provided sufficient detail about the departments' or cloud service providers' obligations for handling security incidents and privacy breaches, including how quickly either party should respond and who should communicate incidents and breaches (and to whom)."[18]

The Government of Canada Cyber Security Event Management Plan (April 2020), establishes the departments and central agencies tasked with coordinating responses to government-wide events; it covers steps to assess, classify, and escalate events. Per the plan, federal organizations are responsible for continually improving their capacity to respond to cybersecurity events; this "includes testing plans and procedures, implementing lessons learned, maintaining contact lists for individuals who have responsibilities set out in the plan, and training personnel, including cybersecurity personnel."[19]

The OAG found that TBS and CSEC performed lessons-learned exercises and developed a report, recommendations, and an action plan to improve future responses. However, TBS did not follow the requirements set out in the plan for testing plans and procedures and keeping the plan up to date. Specifically, the OAG review of the cybersecurity event management plans for the three departments selected for the audit found the following:

17 OAG, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, para. 7.35.

18 Ibid., para. 7.33.

19 Ibid., para. 7.36.

- Each of the three departments conducted annual tabletop exercises and tests of the security of its applications.

- Each of the three departments drafted plans, but two out of three informed the OAG they lacked the funds and capacity to implement them fully.

- Two of the three departments did not finish defining their internal roles and responsibilities for managing incidents.

- Although TBS began the process of collecting information from departments in September 2021, at the time of the audit, it did not know if all departments had implemented cybersecurity event management plans.[20]

Consequently, the OAG recommended that TBS should

- Ensure that the Government of Canada Cyber Security Event Management Plan applies to the evolving cloud environment and shared responsibilities, review and test it at least annually, and update it as needed.

- Follow up annually to ensure that departments finalize, implement, and regularly test their security event management plans.[21]

In its Detailed Action Plan, TBS stated that it "will ensure relevance of the GC Cyber Security Event Management Plan (GC CSEMP) and that it is reviewed and tested annually and updated if required. Ensure departments use GC CSEMP."[22] The department also provided the following milestones:

> Fall 2022—GC CSEMP updated and published
>
> March 2023—Explore options for tools to enable departments to facilitate cloud-based simulation exercises

20 Ibid., paras. 7.37 to 7.39.

21 Ibid., para. 7.40.

22 TBS, Detailed Action Plan, p. 1.

> April 2023—Include a requirement for departments to submit their CSEMP with their Plan for Service and Digital[23]

At the hearing, Catherine Luelo, Deputy Minister and Chief Information Officer of Canada, Treasury Board Secretariat, provided an update regarding the CSEMP:

> 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.[24]

Therefore, the Committee recommends:

Recommendation 2

That, by 31 January 2025, the Treasury Board of Canada Secretariat provide the House of Commons Standing Committee on Public Accounts with a progress report on how it has ensured that the Government of Canada Cyber Security Event Management Plan applies to the evolving cloud environment and shared responsibilities. Moreover, the progress report should show how the plan will be reviewed and tested at least annually and how it is to be updated; it must also include the procedures for following up annually with departments to ensure they have finalized, implemented, and are regularly testing their own security event management plans.

Departments Confused on Cybersecurity Roles

The OAG found that "organizations were unclear about who should do what in certain areas, such as who should evaluate the information technology security controls for data

23 Ibid.

24 House of Commons Standing Committee on Public Accounts, *Evidence*, 1st Session, 44th Parliament, 30 March 2023, Meeting No. 56, 1550.

residency requirements."[25] Specifically, TBS's Government of Canada Cloud Roles and Responsibilities Matrix did not include or modify cloud roles and responsibilities, which have evolved or been added since March 2018 (when the matrix was last updated).[26]

The roles and responsibilities for cloud security are articulated in multiple documents. As a result, the OAG found that departments were confused about some of their roles and responsibilities. For example, the Directive on Service and Digital states that departments are responsible for ensuring that data stored in the cloud, including sensitive and personal information, resides in Canada. However, after the OAG reviewed the contracts and supply arrangements established by SSC and PSPC, it found that not all parties involved understood this.[27]

According to the OAG, without "a clear understanding of who ensures that data stored in the cloud resides in Canada, organizations risk not knowing whether personal information ends up stored in a different country and if so, whether it is subject to different (potentially inferior) privacy protection laws and security protocols."[28]

Consequently, the OAG recommended the following:

> In consultation with Communications Security Establishment Canada, Shared Services Canada, Public Services and Procurement Canada, and departments, the Treasury Board of Canada Secretariat should document and proactively communicate to any department that is using or contemplating cloud services the roles and responsibilities needed to design, implement, validate, monitor, coordinate, and enforce the security controls needed to protect sensitive and personal information in the cloud. The secretariat should review and update these roles and responsibilities at least every 12 months.[29]

In its Detailed Action Plan, TBS stated that it will "ensure that roles and responsibilities required for security controls are clearly documented and proactively communicated to departments."[30] The department also committed to the following milestones:

> October 2022—publish the Cloud Responsibility Matrix

25 OAG, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, para. 7.41.

26 Ibid., para. 7.45.

27 Ibid., para. 7.46.

28 Ibid.

29 Ibid., para. 7.47.

30 TBS, Detailed Action Plan, p. 2.

March 2023—complete a review of the responsibility matrix

September 2023—increase proactive communications

March 2023—updates to the community on review cycles[31]

At the hearing, Catherine Luelo stated that since the audit, the government had updated its cloud roles and responsibilities document, along with the corresponding matrix, and published it internally, so that relevant teams have access to them.[32]

Therefore, the Committee recommends:

Recommendation 3

That, by 31 January 2025, the Treasury Board of Canada Secretariat provide the House of Commons Standing Committee on Public Accounts with a progress report on A) How it is documenting and proactively communicating with departments their respective roles and responsibilities for designing, implementing, validating, monitoring, coordinating, and enforcing the security controls needed to protect sensitive and personal information in the cloud; and B) What steps it has taken to ensure it is reviewing and updating these roles and responsibilities at least every 12 months.

No Costing Model or Long-Term Funding Approach

When TBS released its cloud adoption strategy in 2018, it did not develop or release a long-term funding approach or costing model to go with the strategy, nor did it have these for the OAG to review during the audit. Thus, the OAG could not "determine how these might address departments' known challenges in understanding the costs of moving information to and securing information in the cloud and funding the long-term protection of that information."[33]

When deciding whether applications or services should reside in a data centre hosted by SSC or in the cloud, cost is an important consideration for federal organizations. This is because they will now absorb some of the costs of data storage and application hosting from SSC; this also includes assuming responsibility "for funding the ongoing cloud

31 Ibid.

32 House of Commons Standing Committee on Public Accounts, *Evidence*, 1st Session, 44th Parliament, 30 March 2023, Meeting No. 56, 1550.

33 OAG, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, para. 7.51.

operations and the cybersecurity responsibilities that come with cloud adoption," including "building teams with cloud and cybersecurity skills, purchasing cybersecurity tools, and maintaining operations and security on an ongoing basis."[34]

Although departments have short-term funding to departments to migrate their applications to the cloud, officials have noted that how departments will fund their ongoing cloud operations remains unknown. Concurrently, "departmental spending on cloud services government-wide has increased significantly year over year, to almost $120 million in 2021 from $35 million in 2018."[35] As an example, without acquiring long-term funding for ongoing operations, the three departments selected for this audit were "using a variety of short-term funding measures to finance support their cloud and cybersecurity operations, including reallocating funds that had been intended for other purposes."[36]

And while some of the larger departments may be better able to absorb certain costs of cloud adoption and security, this is likely not sustainable in the long run; smaller departments may not be able to cover any of these costs. Moreover, "shifting resources from other information technology operations to fund cybersecurity can put these other information technology operations at risk."[37]

Consequently, the OAG recommended that in consultation with SSC and other departments, TBS should do the following:

- Develop and provide a costing model to help departments make informed decisions about moving to the cloud and determine whether additional resources and funding are required; and

- Help departments determine their long-term operational funding needs and support their access to funding so they can fulfill their evolving responsibilities for cloud operations, including securing sensitive information in the cloud.[38]

34 Ibid., para. 7.52.

35 Ibid., para. 7.53.

36 Ibid., para. 7.56.

37 Ibid., para. 7.57.

38 Ibid., para. 7.58.

In its Detailed Action Plan, TBS stated that it will "develop and provide a costing model and tools to help departments make informed decisions about moving to the cloud and determine resources and funding required."[39] It also provided the following milestones:

> Fall 2022—Recommendations from government-wide consultations to GC Chief Information Office on the path forward
>
> June 2023—provide a costing model and guidance; assist departments and SSC with forecasting[40]

At the hearing, in response to a question about the proposed costing model, Sony Perron provided the following:

> 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.[41]

Notwithstanding the above, the Committee nevertheless recommends:

Recommendation 4

That, by 31 January 2025, the Treasury Board of Canada Secretariat provide the House of Commons Standing Committee on Public Accounts with a progress report on A) their costing model to help departments make informed decisions about moving to the cloud and determining whether additional resources and funding are required; and B) how they are working with departments to help them determine long-term operational funding needs and support access to funding so they can fulfill their evolving responsibilities for cloud operations, including securing sensitive information.

No Environmental Criteria for Cloud Procurement

TBS and PSPC developed guidance and training to help contracting officers integrate environmental considerations into the procurement of services. Also, PSPC and SSC

39 TBS, Detailed Action Plan, p. 2.

40 Ibid., pp. 2–3.

41 House of Commons Standing Committee on Public Accounts, *Evidence*, 1st Session, 44th Parliament, 30 March 2023, Meeting No. 56, 1600.

trained their procurement officers in green procurement.[42] However, they "did not require cloud service providers to demonstrate their environmental performance or to explain how their services would reduce Canada's greenhouse gas emissions."[43]

And although they "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."[44]

The OAG examined 14 contracts and supply arrangements for cloud services and found that none included environmental clauses. Furthermore, there were no standard environmental clauses relating to cloud services in PSPC's Standard Acquisition Clauses and Conditions Manual.[45]

Although departments can include their own environmental requirements, the three departments selected for this audit explained that they did not write their own contract clauses, but instead relied on the Standard Acquisition Clauses and Conditions Manual (to ensure that clauses were applied consistently across departments).[46]

Consequently, the OAG recommended that PSPC and SSC "should include environmental criteria when procuring cloud services to support sustainability in procurement practices and contribute to achieving Canada's net-zero goal."[47]

In its Detailed Action Plan, SSC stated that environmental criteria "will be included in PSPC and SSC strategies and incorporated into cloud contract templates being developed for the procurement of cloud services across the Government of Canada."[48] It also provided the following milestones:

> Develop rated environmental criteria for inclusion in competitive cloud solicitations. (31 August 2022)

---

42 OAG, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, para. 7.68.

43 Ibid., para. 7.69.

44 Ibid.

45 Ibid., para. 7.70.

46 Ibid., para. 7.71.

47 Ibid., para. 7.72.

48 Shared Services Canada, Detailed Action Plan, p. 1.

Begin including environmental criteria in the competitive solicitation processes under the SSC Cloud Framework Agreement.
(29 September 2022)

Develop a draft of a standard template for cloud contracts that includes standard sustainability terms for cloud service providers.
(29 September 2022)

Consult industry on standard cloud terms and conditions template, including sustainability terms/ Update the standard templates post-consultation. (31 March 2023)

Develop Resulting Contract Clauses related to GHG reduction targets, post industry consultation. Incorporate these into PSPC and SSC solicitations as well as standard template for cloud contracts.
(31 March 2023)[49]

Lastly, PSPC's Management Action Plan provided the following milestones to:

Key interim milestone A (31 March 2023):

Refresh the PSPC Software-as-a-Service Supply Arrangement (SA) with modifications that address Government of Canada priorities related to net-zero greenhouse gas emissions (GHGs), as follows:

- Update the environmental information collected.
- Provide the ability for clients to include environmental criteria in bid solicitations issued against the SA.
- Incorporate 'Resulting Contract Clauses' related to GHG reduction targets.

Key interim milestone B (Completed):

49 Ibid., pp. 1–2.

> In collaboration with SSC, develop and release to procurement officers a standard template for cloud contracts which includes sustainability terms for cloud providers.[50]

At the hearing, when question as to whether this recommendation has been addressed, Sony Perron stated the following:

> 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.[51]

Costas Theophilos, Director General, Cloud Product Management and Services, Shared Services Canada, added the following about specific criteria to be considered:

> 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.[52]

Therefore, the Committee recommends:

Recommendation 5

That, by 31 January 2025, the Public Services and Procurement Canada provide the House of Commons Standing Committee on Public Accounts with a report on the environmental criteria to be used when procuring cloud services in order to support sustainability in procurement practices and contribute to achieving Canada's net-zero goal.

Recommendation 6

That, by 31 January 2025, Shared Services Canada should provide the House of Commons Standing Committee on Public Accounts with a report explaining its progress with regard to developing environmental criteria when procuring cloud services to support

---

50 Public Services and Procurement Canada, Management Action Plan, p. 1.

51 House of Commons Standing Committee on Public Accounts, *Evidence*, 1st Session, 44th Parliament, 30 March 2023, Meeting No. 56, 1700.

52 Ibid., 1710.

sustainability in procurement practices and contribute to achieving Canada's net-zero goal.

Additional Findings Related to Security

The OAG found gaps in the way security inspections for cloud service providers were carried out. However, the Office cannot report its findings publicly because doing so could reveal information on vulnerabilities and pose a risk to Canada's national security. Instead, the OAG reported them directly to PSPC, along with a recommendation relating to the communication of physical security inspection results to stakeholders and the renewal of physical security inspections.[53]

CONCLUSION

The Committee concludes that the Government of Canada had controls at its disposal to prevent, detect, and respond to cybersecurity events that threaten the security of Canadians' personal information in the cloud. However, it did not effectively implement them, nor did it establish and communicate clear roles and responsibilities for implementing them.

Additionally, TBS did not provide a long-term funding approach or costing model to help federal departments better understand the costs of moving to and operating in the cloud. Lastly, the federal government did not include environmental criteria in its procurement of cloud services, even though it was required to reduce greenhouse gas emissions.

In this report the Committee has made six recommendations to help the Government of Canada better manage its responsibilities regarding the safeguarding of personal information pertaining to the use of cloud computing services.

53 OAG, Cybersecurity of Personal Information in the Cloud, Report 7 of the 2022 Reports of the Auditor General of Canada, paras. 7.25.

APPENDIX A:
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Communications Security Establishment	2023/03/30	56
Rajiv Gupta, Associate Head, Canadian Centre for Cyber Security		
Department of Public Works and Government Services	2023/03/30	56
Catherine Poulin, Assistant Deputy Minister, Departmental Oversight Branch		
Paul Thompson, Deputy Minister		
Office of the Auditor General	2023/03/30	56
Jean Goulet, Principal		
Andrew Hayes, Deputy Auditor General		
Gabriel Lombardi, Principal		
Shared Services Canada	2023/03/30	56
Sony Perron, President		
Costas Theophilos, Director General, Cloud Product Management and Services		
Treasury Board Secretariat	2023/03/30	56
Catherine Luelo, Deputy Minister and Chief Information Officer of Canada		

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 56 and 138) is tabled.

Respectfully submitted,

John Williamson
Chair

Conservative Dissenting Report to the 42nd Report of the Standing Committee on Public Accounts:
Cybersecurity of Personal Information in the Cloud

44th Parliament

The Liberal-NDP Coalition Prioritizes Ideological Carbon Reduction Over Canadians Cybersecurity

The Office of the Auditor General of Canada has tabled a scathing report that shows how little the Government of Canada is doing to protect Canadians' cybersecurity. Instead of addressing the shortcomings, the reaction from the Liberals is to tie needed cybersecurity investment to carbon reductions.

As clearly explained in the body of this report, and the Office of the Auditor General's November 2022 Report *Cyber Security of Personal Information in the Cloud*, the Treasury Board of Canada Secretariat, Shared Services Canada, Public Services and Procurement Canada, and Communications Security Establishment Canada have failed to adequately protect the personal information of Canadians due to Liberal incompetence and lack of prioritizing this urgent issue.

The Government of Canada should focus all its cyber security resources and efforts into complying with their own rules and regulations and above all address the deficiencies so that Canadians are protected. This includes securing software applications and databases, ensuring enforcement of cloud guardrails, and preventing and responding to cyber attacks.

The Liberal Government should not be wasting cybersecurity investment and resources on their ideologically driven pursuit on reducing carbon or other greenhouse gas emissions. Cybersecurity and the protection of Canadians should not be sacrificed for political messaging of the Liberal government.

The Office of the Auditor General has reported the Liberal government's failure in implementing the 2018 Cloud Adoption Strategy. The report also highlights that departments are struggling to understand their roles and responsibilities, leading to confusion regarding cybersecurity tasks. This confusion further amplifies the potential risks to Canadians' safety due to bureaucratic and political inefficiencies and incompetence within the Liberal government. Given the existing delays, confusion, and potential security risks, adding additional unrelated tasks is not a prudent course of action.

No evidence was provided to suggest that requesting Public Services and Procurement Canada or Shared Services Canada to write a report linking the procurement of cloud services and cybersecurity to a 2050 target will contribute to emission reductions.

Conservatives disagree with implementing Recommendation 5 and Recommendation 6 of the majority report where the focus is on the Liberal government's ideological pursuit of net zero instead of protecting Canadians.

Instead, Conservatives recommend the following in place of recommendation 5 and 6:

> **That, Treasury Board of Canada Secretariat take immediate action to resolve the confusion between departments regarding roles and responsibilities for cyber security and finally lay out clear and concise mandates to departments involved in cyber security.**
>
> And

That, in working to immediately address the failures as reported by the Auditor General, Public Services and Procurement Canada and Shared Services should prioritize the protection of personal information of Canadians and not pursue unrelated goals that are outside the core purpose of cybersecurity operations.