2025 REPORT OF THE AUDITOR GENERAL OF CANADA TO THE PARLIAMENT OF CANADA

Cyber Security of Government Networks and Systems

Office of the Auditor General of Canada
Bureau du vérificateur général du Canada

INDEPENDENT AUDITOR'S REPORT

Performance audit reports

This report presents the results of a performance audit conducted by the Office of the Auditor General of Canada (OAG) under the authority of the Auditor General Act.

A performance audit is an independent, objective, and systematic assessment of how well government is managing its activities, responsibilities, and resources. Audit topics are selected on the basis of their significance. While the OAG may comment on policy implementation in a performance audit, it does not comment on the merits of a policy.

Performance audits are planned, performed, and reported in accordance with professional auditing standards and OAG policies. They are conducted by qualified auditors who

- establish audit objectives and criteria for the assessment of performance
- gather the evidence necessary to assess performance against the criteria
- report both positive and negative findings
- conclude against the established audit objectives
- make recommendations for improvement when there are significant differences between criteria and assessed performance

Performance audits contribute to a public service that is ethical and effective and a government that is accountable to Parliament and Canadians.

This publication is available on our website at www.oag-bvg.gc.ca.

Cette publication est également offerte en français.

Cat. No. FA1-27/2025-1-10E-PDF

ISBN 978-0-660-78926-2

ISSN 2561-343X

Cover photo: Olemedia/Gettyimages.ca

At a Glance

Overall message

Overall, we concluded that the federal government had tools in place to protect and defend government networks and systems from cyber threats; however, there were significant gaps in cyber security services, monitoring, and response during active attacks. As cyber attacks become more sophisticated, pervasive, and harmful, the federal government must continually bolster its defences.

The responsibility for protecting government information technology (IT) systems and operations is shared by the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada. The organizations work together and with departments and agencies to prevent data theft and limit disruptions to systems that deliver programs and services to Canadians. However, not all federal organizations were subject to the same security policies, which resulted in the inconsistent use of available cyber security services. Gaps in cyber security defences undermine the government's ability to protect critical information and manage cyber security risks.

Protecting federal networks and systems also requires the government to analyze the potential vulnerabilities of all government devices, including laptops, smartphones, and servers. Our audit found that Shared Services Canada and Communications Security Establishment Canada did not have a comprehensive, up-to-date inventory of all government IT assets. In 2017, Shared Services Canada began developing a cyber security project designed to provide a complete view of government devices, but the project had not been completed. Without up-to-date IT information across all departments and agencies, the federal government risks not being aware of—let alone being able to quickly respond to—changing cyber security challenges.

We also found that the coordination among the 3 organizations was insufficient during active attacks. For example, a lack of information sharing delayed the government's response to a significant cyber attack in January 2024, allowing the attacker prolonged access to personal information. At the time of our audit, an initiative to set up a cyber security collaboration platform and incident case management tool had not received funding.

Key facts and findings

- From April 2023 through March 2024, Communications Security Establishment Canada's network-based sensors blocked about 2.4 trillion suspicious cyber security events, which ranged from simple network scans to sophisticated cyber attacks.
- From October 2023 through September 2024, Shared Services Canada's secure Enterprise Internet Service blocked about 6.6 trillion suspicious cyber security events.
- In June 2024, Shared Services Canada put the Security Information and Event Management project on hold. This initiative aimed to identify suspicious cyber security events and trigger automated responses to cyber attacks if detected.
- Budget 2024 provided the Treasury Board of Canada Secretariat $11.1 million over 3 years to lead the implementation of a cyber security strategy. We found this strategy, launched in May 2024, to be sound and comprehensive.

See **Recommendations and Responses** at the end of this report.

Table of Contents

Introduction

Background

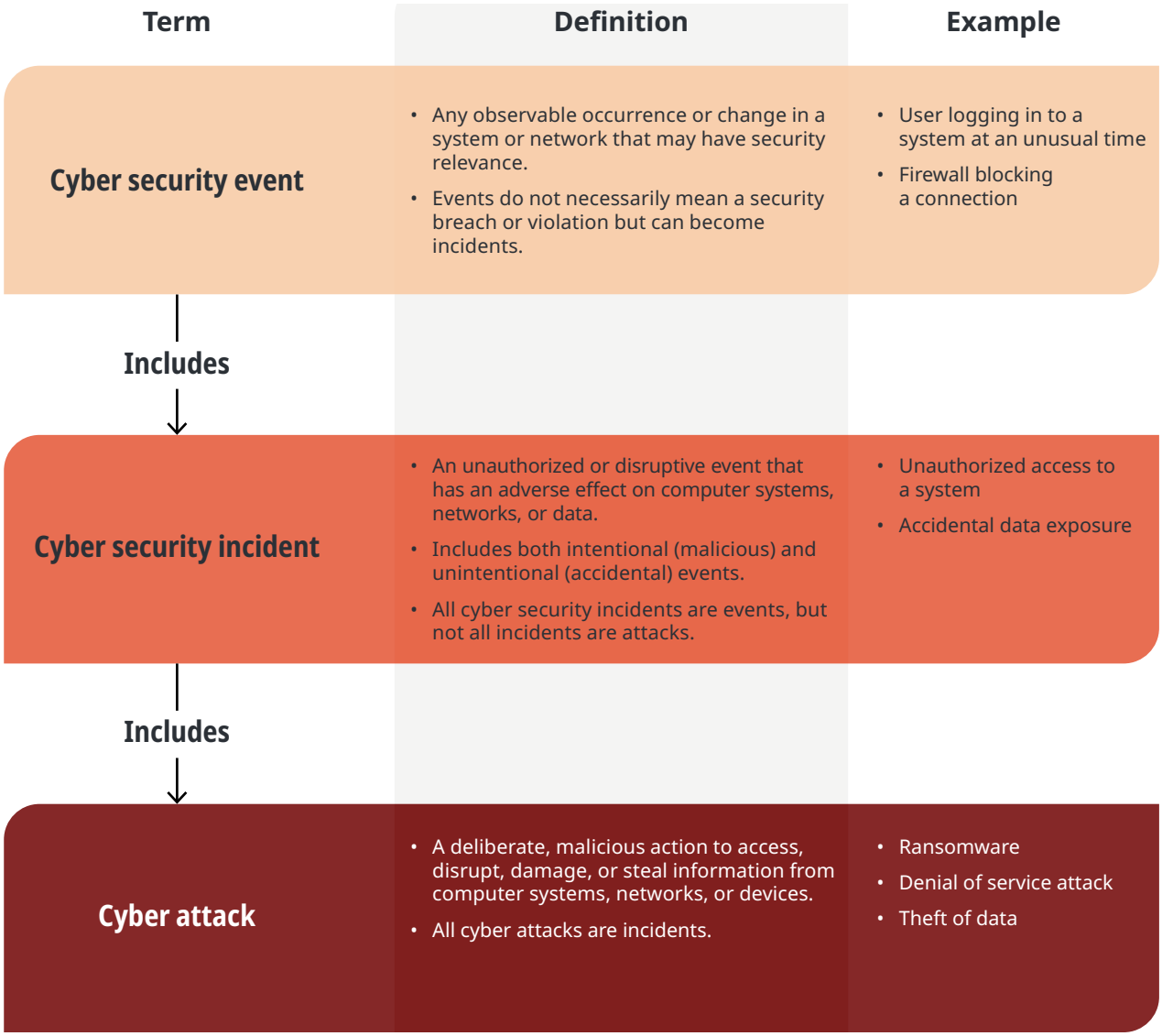
Securing government networks and systems from cyber attacks

1. Cyber attacks (Exhibit 1) have become a frequent daily occurrence worldwide. Canada's economy, critical infrastructure, and the federal government's ability to provide services to Canadians are relying more and more on information technology (IT) systems. Canada is an attractive target for cyber attacks by those wishing to undermine national security, economic prosperity, the Canadian way of life, and the trust in democratic institutions.

2. The Government of Canada defends its networks and systems against numerous daily cyber attacks. But the sophistication of these cyber attacks is evolving as quickly as the government's ability to prevent and respond to them. Government networks and systems are sometimes breached, such as at the Treasury Board of Canada Secretariat and the Department of Finance Canada in 2011 and at the National Research Council Canada in 2014. The latter breach caused reputational harm, resulted in the loss of intellectual property, cost the government an estimated $100 million to mitigate, and resulted in a years-long effort to rebuild the organization's network with appropriate cyber security.

3. More recently, in January 2024, Global Affairs Canada was subject to a month-long cyber attack that compromised its network and resulted in the theft of personal information. And in March 2024, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) was targeted by a cyber attack, requiring it to take some of its corporate systems offline. These were 2 of 1,017 cyber security events (Exhibit 1) that Communications Security Establishment Canada responded to in the 2023–24 fiscal year.

Exhibit 1—Cyber security event, cyber security incident, and cyber attack



Source: Based on information from Communications Security Establishment Canada and the Treasury Board of Canada Secretariat

Read the Exhibit 1 text description

Roles and responsibilities

4. **Treasury Board of Canada Secretariat.** The secretariat is responsible for providing policy leadership, and advice and guidance for all matters related to government security, including cyber security. It establishes and oversees a government-wide approach to security management, in cooperation with Communications Security

Establishment Canada and Shared Services Canada, and provides strategic policy oversight and coordination for government security management activities. Within the secretariat, the Office of the Chief Information Officer is responsible for leading and supporting the implementation of the federal government's enterprise cyber security strategy.

5. **Communications Security Establishment Canada.** This agency is responsible for protecting and defending government networks and systems and mitigating impacts of cyber attacks. Within the agency, the Canadian Centre for Cyber Security was created in 2018 to ensure the protection of the government's networks and systems as well as Canada's critical infrastructures of importance to the federal government. The centre is Canada's single unified source of expert advice, guidance, services, and support on cyber security for government, critical infrastructure owners and operations, the private sector, and the Canadian public.

6. **Shared Services Canada.** This department is responsible for planning, designing, building, operating, and maintaining effective, efficient, and responsive IT infrastructure and services. This includes delivering cyber security services to secure government networks and systems under its responsibility.

Focus of the audit

7. This audit focused on whether the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada had the tools in place to protect and defend government networks and systems from cyber attacks in a coordinated manner.

8. This audit is important because as cyber attacks become more sophisticated, frequent, and damaging, the federal government's defences must continually evolve to successfully protect its networks and systems, including sensitive information and Canadians' personal information stored within them.

9. More details about the audit objective, scope, approach, and criteria are in **About the Audit** at the end of this report.

Findings and Recommendations

A strategy was in place to manage cyber security

Why this finding matters

10. This finding matters because having a sound and comprehensive cyber security strategy focusing on the federal government is important for managing cyber security risks. A strategy sets out a vision and objectives for the government and identifies initiatives required to strengthen the cyber security of the government's networks and systems.

A new strategy guided the government's cyber security activities

Findings

11. Budget 2024 provided $11.1 million over 3 years, starting in 2024–25, to the Treasury Board of Canada Secretariat to lead the work on implementing a cyber security strategy. We found that in May 2024, the secretariat launched the Government of Canada Enterprise Cyber Security Strategy to strengthen cyber security across government operations. The strategy's purpose was also to maintain Canadians' confidence that their personal information in the care of the government was protected and that the government's programs and services would be provided without interruption. We found that this strategy was sound and comprehensive. It listed cyber security gaps affecting government networks and systems and provided objectives with key actions and expected measurable outcomes aimed at addressing these gaps (Exhibit 2).

Exhibit 2—Objectives and key actions of the Government of Canada Enterprise Cyber Security Strategy

Vision	Strategy objectives	Examples of key actions*
"Building a world-class, sustainable, and resilient federal government to reduce cyber security risks so that departments and agencies can enable secure and reliable digital service delivery." **Implementing the strategy:** • Treasury Board of Canada Secretariat • Communications Security Establishment Canada • Shared Services Canada • Departments and agencies	**Articulate cyber security risk and its business impacts**	• Establish a government-wide compliance and assurance program to assess departments' cyber security defences to identify and prioritize cyber security risks. • Create a government-wide vulnerability management program to manage and reduce vulnerabilities affecting government systems and networks.
	Prevent and resist cyber attacks more effectively	• Expand cyber security defences to small departments and agencies. • Establish a framework to improve the ability to detect and prevent fraudulent activity against government applications.
	Strengthen capabilities and resilience across the Government of Canada	• Establish a framework for departments to maintain accurate asset inventories of government applications and systems. Conduct year-round testing and reviews of cyber security protection and defence. • Implement a government-wide cyber security event collaboration platform to manage and respond to cyber events.
	Foster a diverse federal workforce with the right cyber security skills	• Build cyber talent through cross-functional training programs in cyber security. • Promote a talent management culture to recruit and retain skilled candidates.

* There are many other actions under the strategy. The examples listed here represent some of the actions intended to have a government-wide impact.

Source: Based on information from the Government of Canada Enterprise Cyber Security Strategy, Treasury Board of Canada Secretariat, 2024

Read the Exhibit 2 text description

Cyber security services were made available to protect federal organizations, but some were not using them

Why this finding matters

12. This finding matters because gaps in the use of cyber security services create a federal government cyber security landscape that is fragmented, making it harder for the government to mitigate cyber security risks. This in turn increases the likelihood of successful cyber attacks that can result in significant damages, such as the theft of personal or sensitive information, the denial of access to services, and financial loss.

Good cyber security services were developed to protect the government's networks and systems

Findings

13. We found that Communications Security Establishment Canada developed and offered cyber security defence sensors to detect and mitigate cyber security events, cyber security incidents, and cyber attacks (Exhibit 3). These sensors provide a layer of cyber security in addition to services offered by Shared Services Canada or by commercially available services, such as antivirus and firewall software.

14. We found that the agency's network-based sensors blocked an average of 6.6 billion suspicious cyber security events a day between April 1, 2023, and March 31, 2024, for a yearly total of approximately 2.4 trillion. These actions ranged from scans of the government's networks to sophisticated cyber attacks. The effectiveness of Communications Security Establishment Canada's cyber security defence sensors is recognized internationally. The government of the United Kingdom has adopted some of these sensors to enhance its own cyber security.

15. We found that Shared Services Canada offers the Enterprise Internet Service, which provides secure connectivity for federal government users to access the internet and for Canadians to access government websites. The Enterprise Internet Service includes enhanced cyber security that monitors internet traffic and blocks suspicious cyber security events. It also integrates Communications Security Establishment Canada's cyber security defence network-based sensors (Exhibit 3). Between 1 October 2023 and 30 September 2024, the Enterprise Internet Service blocked an average of 18 billion suspicious cyber security events a day, for a yearly total of approximately 6.6 trillion.

Exhibit 3—Communications Security Establishment Canada developed 3 types of cyber security defence sensors to detect and mitigate cyber security events and cyber attacks

Cyber security defence sensors	Deployed	Description
Network-based sensor 	2010	Detects and mitigates cyber security incidents on the government's networks. This sensor is typically integrated with Shared Services Canada's Enterprise Internet Service.
Host-based sensor 	2012	Detects cyber attacks on IT endpoint devices such as laptop computers, servers, and local networks. The sensor analyzes and processes collected information to detect suspicious cyber security events occurring on a host machine. The information gathered is used to report anomalies and weaknesses to affected federal organizations.
Cloud-based sensor 	2019	Operates in federal organizations' cloud infrastructure and works in conjunction with the defences provided by cloud vendors. This sensor automates the collection of logged activity in the cloud and analyzes the information to detect and mitigate suspicious cyber security events.

Source: Based on information from Communications Security Establishment Canada

Read the Exhibit 3 text description

Not all departments, agencies, and Crown corporations were using cyber security services offered by Communications Security Establishment Canada and Shared Services Canada

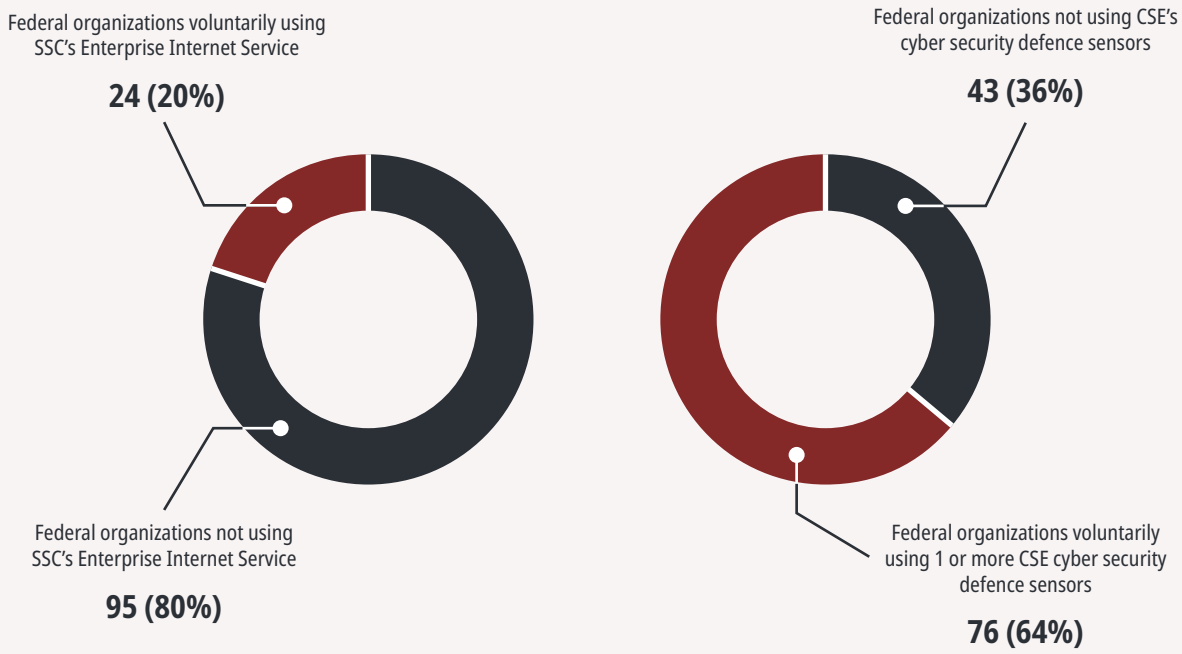
Findings

16. At the time of our audit, the Government of Canada was composed of 204 **federal organizations**.[1] Eighty-five of these federal organizations, including most large departments, were subject to Treasury Board policies that required them to use Shared Services Canada's Enterprise Internet Service and Communications Security Establishment Canada's cyber security defence sensors. We found that all of the 85 federal organizations were using cyber security defence sensors, while 22, or 26%, of these 85 federal organizations were not using the Enterprise Internet Service.

1 **Federal organization**—A department, agency, Crown corporation, or federal entity (board, council, commission, secretariat, agent of Parliament, administrative tribunal, etc.) established by the Government of Canada or Parliament to carry out federal responsibilities. Each type of organization is governed by legislation and may or may not be required to follow Treasury Board policies.

17. All of the other 119 federal organizations were not subject to these Treasury Board policies and, consequently, were not required to use these cyber security services. However, the Treasury Board of Canada Secretariat strongly encouraged these organizations to do so. We found that the majority of these 119 federal organizations were not using Shared Services Canada's Enterprise Internet Service, while most were using Communications Security Establishment Canada's cyber security defence sensors (Exhibit 4).

Exhibit 4—The 119 federal organizations not required to use the cyber security services of Shared Services Canada (SSC) and Communications Security Establishment Canada (CSE) were encouraged to use the services, but many chose not to



Source: Based on data from Shared Services Canada and Communications Security Establishment Canada

Read the Exhibit 4 text description

18. Officials from Communications Security Establishment Canada told us that the inconsistent deployment of its cyber security defence sensors across all federal organizations created cyber security gaps, impacting the agency's ability to defend government networks, systems, and devices.

19. We consulted 13 federal organizations (Crown corporations and small departments and agencies) not required to use Shared Services Canada's and Communications Security Establishment Canada's cyber security services to understand why they were not using the services. The following concerns were mentioned:

- Using these cyber security services could be perceived as a threat to the independence of Crown corporations.
- Shared Services Canada and Communications Security Establishment Canada have a limited capability to tailor their cyber security services to the needs of these federal organizations.
- The performance of support and maintenance of their cyber security services by Shared Services Canada and Communications Security Establishment Canada could be improved.

20. The networks and systems of Crown corporations and small departments and agencies hold sensitive information as well as Canadians' personal information. It is our view that by not using Shared Services Canada's and Communications Security Establishment Canada's cyber security services, organizations declined a strong and proven line of defence that could augment their current protection. That additional protection includes defence against highly sophisticated cyber attacks that may not be detected by commercially available cyber security services. Not using the services also impacts the ability of Shared Services Canada and Communications Security Establishment Canada to defend the federal government's networks and systems more broadly.

There were important gaps in tools to monitor and respond to cyber attacks

Why this finding matters

21. This finding matters because gaps in the cyber security of government networks and systems as well as delays in responding to cyber attacks increase the likelihood that these cyber attacks may succeed, resulting in the theft of personal or sensitive information and in damage to IT systems. In turn, this can affect the delivery of programs and services to Canadians. The key to strong cyber security is having the appropriate tools and supporting procedures for monitoring suspicious cyber security events and incidents to prevent potential cyber attacks and efficiently respond to actual cyber attacks.

There was a gap in monitoring suspicious cyber security events occurring on the government's networks and systems

Findings

22. Shared Services Canada began developing a Security Information and Event Management application in April 2017, and it was to be completed by March 2023. The new application would provide visibility over suspicious cyber security events occurring on the government's networks and systems, would be managed by the department, and would trigger automated responses to cyber attacks that the application detected. When designed and implemented correctly, the new application would also increase Shared Services Canada and Communications Security Establishment Canada's ability to predict and anticipate sophisticated cyber attacks and reduce the time needed between detection and response.

23. The project to develop the application had an original budget of $72.7 million, which was revised to $144.3 million in May 2021. We found that the project was delayed for several reasons, including difficulties in identifying and selecting a qualified vendor. The project was put on hold in June 2024, pending approval of additional funding.

24. The delay in the project meant that existing gaps in cyber security monitoring were not resolved, and it also created cost inefficiencies. We found the following:

- Shared Services Canada could not monitor all suspicious cyber security events occurring on the government's networks, systems, and devices under the department's responsibility.
- For cyber security events that Communications Security Establishment Canada had the responsibility for analyzing, Shared Services Canada was sharing only some of these events for analysis with Communications Security Establishment Canada. The agency reported that the cost for analyzing these suspicious cyber security events was about $16.9 million in total for the 3 fiscal years from 2021–22 to 2023–24 and an estimated $13.8 million for the 2024–25 fiscal year. Officials from Communications Security Establishment Canada told us they expected costs to continue rising and that the agency needed additional resources to continue this analysis in future years.

Recommendation

25. Shared Services Canada, in collaboration with Communications Security Establishment Canada, should develop a clear action plan with defined criteria and a timeline to develop a Security Information and Event Management application that addresses the existing gaps in cyber security monitoring.

The department's response. Agreed.

See **Recommendations and Responses** at the end of this report for detailed responses.

Central inventories of the government's IT assets were incomplete, increasing risk to cyber attacks

Findings

26. We found that Shared Services Canada and Communications Security Establishment Canada did not have complete inventories of IT assets operated by the federal organizations that they serviced. These IT assets included local area networks (LANs) and IT endpoint devices, such as laptops, printers, and servers. Specifically, we found the following:

- Since Shared Services Canada did not have a complete central inventory of the networks or systems under its responsibility, it did not have a comprehensive understanding of which networks and systems, including supporting software, needed to be patched, updated, or maintained or were no longer supported by a vendor.
- Communications Security Establishment Canada was not provided with a complete central inventory of all IT endpoint devices by the federal organizations it serviced. At the end of September 2024, the agency's host-based sensors were installed on approximately 770,000 IT endpoint devices. However, not all IT endpoint devices had the agency's sensors installed on them.

27. Not having a complete inventory of IT assets limited and impacted Shared Services Canada and Communications Security Establishment Canada's ability to support federal organizations they service and to manage cyber security risks to the government's networks and systems. The incomplete inventory also made it difficult for the department and the agency to obtain a complete understanding of the IT assets that federal organizations were using and their inherent vulnerabilities that could be exploited in a cyber attack.

28. We found that delays in Shared Services Canada's Endpoint Visibility, Awareness and Security project hindered the department's ability to obtain the complete inventory of IT assets under its responsibility. The project, which started in November 2017, was to be completed by September 2024 and had a budget of $174.8 million. However, at the end of the period covered by our audit on September 30, 2024, the project was still ongoing because of various challenges, including changes to the department's requirements. Officials from Shared Services Canada told us that the project would require at least an additional 3 years, until 2027, to be completed.

29. We found that in August 2024, the Treasury Board of Canada Secretariat issued a security policy directive with the goal of improving the cyber security health of the government's networks and systems. Among the requirements, the directive required that by mid-November 2024, the 85 federal organizations that were required to use the services of Communications Security Establishment Canada confirm with the agency that cyber security defence sensors (Exhibit 3) had been implemented on all of its IT endpoint devices. At the end of our audit period, this initiative was still underway.

Recommendation

30. Shared Services Canada should:

- ensure that it has an up-to-date central inventory of networks and systems across federal organizations it services and a process to manage devices that need to be patched, updated, maintained, or replaced. The department should install the needed patches, perform the required updates, and maintain and replace networks and systems accordingly.
- determine a solution to resolve the challenges facing the Endpoint Visibility, Awareness and Security project

The department's response. Agreed.

See **Recommendations and Responses** at the end of this report for detailed responses.

Recommendation

31. The Treasury Board of Canada Secretariat, in consultation with Communications Security Establishment Canada, should ensure that federal organizations:

- implement cyber security defence sensors on all of its IT endpoint devices so that their associated vulnerabilities can be identified
- remediate vulnerabilities in a timely manner

The secretariat's response. Agreed.

See **Recommendations and Responses** at the end of this report for detailed responses.

Coordination and information sharing procedures and protocols for cyber attacks were incomplete, and there was no tool to support seamless coordination and collaboration

Findings

32. The response to cyber attacks on federal government organizations is framed by the Government of Canada Cyber Security Event Management Plan, which was prepared by the Treasury Board of Canada Secretariat. Although the secretariat led the creation of the plan, the secretariat, Communications Security Establishment Canada, and Shared Services Canada share the responsibility for establishing procedures and protocols for coordination and information sharing among themselves and federal organizations when responding to cyber attacks. However, we found that the coordination and sharing procedures and protocols were incomplete, resulting in a delayed response to stop a cyber attack (Exhibit 5).

Exhibit 5—Information sharing and coordination shortfalls affected the timely response to a cyber attack

In a recent significant cyber attack against a federal organization, issues in coordination and sharing of sensitive information and resources delayed the government's response:

- When initially trying to respond to the cyber attack, Communications Security Establishment Canada had an urgent need to access key, sensitive information from Shared Services Canada to evaluate the significance and source of the ongoing cyber attack. However, because of incomplete procedures and protocols for sharing that information, it took 7 days to request and transmit the information, which delayed the response to the cyber attack.
- On more than 1 occasion during the cyber attack, the federal organization under attack had difficulty reaching subject matter experts at Shared Services Canada to get urgent technical support to assist in responding to the cyber attack.

The delayed response provided attackers more time to access the federal organization's information of the organization's employees. In our view, had complete coordination and information sharing procedures and protocols been in place during that cyber attack, the government's response would have been faster.

33. We also found that there was no coordination tool to support seamless collaboration and information sharing for timely decision making and action when responding to cyber attacks. During our audit, we reviewed the post-event reports for 8 past cyber attacks that occurred between calendar years 2022 and 2024 and that impacted various federal organizations. We found recurrent issues in the ability to share information among all the federal organizations involved in responding to these attacks, and no collaboration tool to facilitate information sharing.

34. In accordance with the Government of Canada Enterprise Cyber Security Strategy, Communications Security Establishment Canada was to implement a government-wide cyber security event collaboration platform and incident case management tool that would enable seamless collaboration and information sharing when responding to cyber attacks. We found that the agency had no implementation timelines and had not made a funding request for this tool. Officials from Communications Security Establishment Canada acknowledged that the government's ability to effectively collaborate and coordinate in the event of a cyber attack would be impacted until this initiative was implemented. At the end of our audit period, these officials told us that work was underway to prepare a funding request for the tool.

Recommendation

35. The Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada should re-evaluate their cyber security incident management practices to enable the better coordination and timely sharing of required critical information when responding to cyber attacks affecting federal organizations.

The 3 organizations' response. Agreed.

See **Recommendations and Responses** at the end of this report for detailed responses.

Recommendation

36. Communications Security Establishment Canada should finalize its funding request and prioritize its work to develop and implement a cyber security event collaboration platform and incident case management tool. The new platform and tool should enable the standardized communication, tracking, monitoring, and documentation of cyber security events and should be accessible by the Treasury Board of Canada Secretariat, Shared Services Canada, and other federal organizations.

The agency's response. Agreed.

See **Recommendations and Responses** at the end of this report for detailed responses.

Conclusion

37. We concluded that the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada had the tools in place to protect and defend government networks and systems from cyber attacks. However, there were gaps in coordination and information sharing during cyber attacks, and some tools needed to be developed or finalized to improve the government's ability to respond to cyber attacks.

38. There is a significant number of federal organizations that are not required to use cyber security services offered by Communications Security Establishment Canada and Shared Services Canada and do not use them. The inconsistent use of these cyber security services has impacted the government's awareness of cyber security events across the federal public service and its ability to defend its networks and systems from cyber attacks and from threat actors seeking to disrupt government operations.

About the Audit

This independent assurance report was prepared by the Office of the Auditor General of Canada on the cyber security of networks and systems. Our responsibility was to provide objective information, advice, and assurance to assist Parliament in its scrutiny of the government's management of resources and programs and to conclude on whether the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada complied in all significant respects with the applicable criteria.

All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the CPA Canada Handbook—Assurance.

The Office of the Auditor General of Canada applies the Canadian Standard on Quality Management 1—Quality Management for Firms That Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements. This standard requires our office to design, implement, and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

In conducting the audit work, we complied with the independence and other ethical requirements of the relevant rules of professional conduct applicable to the practice of public accounting in Canada, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

In accordance with our regular audit process, we obtained the following from entity management:

- confirmation of management's responsibility for the subject under audit
- acknowledgement of the suitability of the criteria used in the audit
- confirmation that all known information that has been requested, or that could affect the findings or audit conclusion, has been provided
- confirmation that the audit report is factually accurate

Audit objective

The objective of this audit was to determine whether the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada had the tools in place to protect and defend government networks and systems from cyber attacks in a coordinated manner.

Scope and approach

Our audit work included reviewing plans, strategies, policies, and guidelines; interviewing relevant department and agency officials; reviewing past cyber security events; and conducting analyses on the adoption of key cyber security services provided to federal organizations:

- We examined the existence and quality of strategies and plans to address the cyber security needs of the government, including its objectives and initiatives to improve its cyber security posture.
- We obtained a listing of federal organizations and validated this information with the Treasury Board of Canada Secretariat to arrive at a total number of federal organizations. This amounted to a total of 204 federal organizations, including 85 organizations required to use the cyber security services of audited organizations, 44 Crown corporations, 9 agents or officers of Parliament, and 66 other organizations, such as small departments and agencies, boards, councils, commissions, and administrative tribunals. We determined the number of federal organizations that had onboarded onto the cyber security defence services within our audit scope.
- We obtained a listing of the cyber security events and cyber attacks affecting federal organizations that were identified by or reported to Communications Security Establishment Canada and that occurred between calendar years 2022 and 2024 (up to the end of our audit period). After validating the list of cyber attacks with the Treasury Board of Canada Secretariat, we reviewed post-event reports of 8 past cyber attacks that included the compromise of information, affected more than 1 federal organization, or required the involvement of the audited entities to resolve. The selection of these examples was not meant to be statistically representative. For 1 of these cyber attacks, we performed additional work at the federal organization under attack to better understand the details of the attack, the role the organization played, and how it and other audited organizations collaborated to respond to the attack.
- We selected 3 ongoing cyber security projects or initiatives, from a combined listing of 18 projects and initiatives provided by Shared Services Canada and Communications Security Establishment Canada, and assessed their implementation progress. We selected these projects and initiatives on the basis of their dollar values (budgets), their expected timelines to implement, their government-wide focus, and their relevance to our audit objective and scope.

To gather perspectives on why Crown corporations and small departments and agencies not required to use the cyber security services of audited organizations had or had not adopted Shared Services Canada's services or the cyber security defence sensors of Communications Security Establishment Canada, we used a questionnaire to interview officials and consulted with 13 of these federal organizations, 5 small departments and agencies, and 8 Crown corporations. While their comments provided valuable insights, it is important to note that the selection of these federal organizations was not designed to be statistically representative. Although we understand that the views expressed may align with those of other organizations, we did not verify this assumption through further consultations or analysis. The goal of the consultations was to better understand the reasons behind decisions and challenges in adopting, or not adopting, the government's cyber security services.

We did not conduct penetration testing or other assessments to test the effectiveness of Communications Security Establishment Canada's or Shared Services Canada's cyber security services.

Criteria

We used the following criteria to conclude against our audit objective:

Criteria	Sources
The Treasury Board of Canada Secretariat, Shared Services Canada, Communications Security Establishment Canada and selected departments develop and maintain a collaborative and coordinated approach to protect and defend government networks and systems. The Treasury Board of Canada Secretariat develops a cyber security strategy that sets out a vision and strategic objectives to improve the cyber security of government operations. The Treasury Board of Canada Secretariat sets a direction and establishes priorities for securing government IT networks and systems. The Treasury Board of Canada Secretariat, Shared Services Canada, and Communications Security Establishment Canada have the necessary governance, information, and tools in place to collaborate, respond, and report on cyber security events and incidents. The Treasury Board of Canada Secretariat, Shared Services Canada, and Communications Security Establishment Canada measure the results of the government's cyber security posture, including its effectiveness to respond to threats. Shared Services Canada and Communications Security Establishment Canada protect government networks and systems. Shared Services Canada and Communications Security Establishment Canada exercise their respective responsibilities to defend and protect government networks and systems against cyber security threats and events. Shared Services Canada and Communications Security Establishment Canada identify all IT infrastructure and systems that pose a risk and threat to the cyber security of the federal government.	• Communications Security Establishment Act • Shared Services Canada Act • Policy on Government Security, Treasury Board, 2019 • Directive on Security Management, Treasury Board, 2019 • Policy on Service and Digital, Treasury Board, 2020 • Directive on Service and Digital, Treasury Board, 2020 • Guideline on Service and Digital, Treasury Board of Canada Secretariat, 2020 • Policy on Results, Treasury Board, 2016 • 2024–25 Departmental Plan, Treasury Board of Canada Secretariat • Government of Canada Enterprise Cyber Security Strategy, Treasury Board of Canada Secretariat, 2024 • Digital Operations Strategic Plan: 2021–2024, Treasury Board of Canada Secretariat • Security Control Profile for Cloud-Based GC Services, Government of Canada, 2016 • Improving GC Cyber Security Health: Security Policy Implementation Notice, Government of Canada, 2024 • 2024–25 Departmental Plan, Shared Services Canada • SSC 3.0: An Enterprise Approach, Shared Services Canada • Delivering Digital Solutions Together for Canada, Shared Services Canada • Network and Security Strategy, Shared Services Canada, 2021

Criteria	Sources
Shared Services Canada and Communications Security Establishment Canada measure the effectiveness of their cyber defence services. Shared Services Canada and Communications Security Establishment Canada are making progress on their cyber security projects and initiatives that have an impact on improving the overall cyber defence posture of all federal organizations.	• Canada's Digital Ambition 2022–23, Government of Canada • Canada's Digital Ambition 2023–24, Government of Canada • Federal budgets, 2018, 2019, 2021, 2022, 2023, and 2024 • Financial Administration Act • Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice 2017-01, Treasury Board of Canada Secretariat • Event Logging Guidance, Treasury Board of Canada Secretariat, 2020 • Patch Management Guidance, Treasury Board of Canada Secretariat, 2020 • Government of Canada Cyber Security Event Management Plan, Treasury Board of Canada Secretariat, 2023 • Government of Canada Cloud Security Risk Management Approach and Procedures, Treasury Board of Canada Secretariat • Security Playbook for Information System Solutions, Treasury Board of Canada Secretariat • National Cyber Security Strategy, Public Safety Canada, 2022 • Cyber Security Services Roadmap, Shared Services Canada • IT Security Risk Management: A Lifecycle Approach (ITSG-33), Canadian Centre for Cyber Security • Top 10 IT Security Actions, Canadian Centre for Cyber Security • COBIT 2019 Framework: Government and Management Objectives, ISACA • ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements, International Organization for Standardization and International Electrotechnical Commission

Criteria	Sources
	• ISO/IEC 27002:2022, Information Security, Cybersecurity and Privacy Protection—Information Security Controls, International Organization for Standardization and International Electrotechnical Commission • ISO/IEC 27004:2016, Information Technology—Security Techniques—Information Security Management—Monitoring, Measurement, Analysis and Evaluation, International Organization for Standardization and International Electrotechnical Commission • ISO/IEC 27005:2022, Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks, International Organization for Standardization and International Electrotechnical Commission • ISO/IEC 27010:2015, Information Technology—Security Techniques—Information Security Management for Inter-Sector and Inter-Organizational Communications, International Organization for Standardization and International Electrotechnical Commission • ISO/IEC 27031:2011, Information Technology—Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity, International Organization for Standardization and International Electrotechnical Commission • ISO/IEC 27032:2023, Cyber Security—Guidelines for Internet Security, International Organization for Standardization and International Electrotechnical Commission • Global Technology Audit Guide: Auditing IT Governance, The Institute of Internal Auditors • Global Technology Audit Guide: Assessing Cybersecurity Risk, The Institute of Internal Auditors • Global Technology Audit Guide: Auditing Cyber Incident Response and Recovery, The Institute of Internal Auditors, 2022

Criteria	Sources
	• Good Practices for Security of IoT: Secure Software Development Lifecycle, European Union Agency for Cyber Security • Draft NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology, 2017 • Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, 2018 • NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, National Institute of Standards and Technology, 2018 • NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, National Institute of Standards and Technology, 2012 • A Guide to the Project Management Body of Knowledge (PMBOK Guide), seventh edition, Project Management Institute • Transforming Our World: The 2030 Agenda for Sustainable Development, United Nations, 2015

Period covered by the audit

The audit covered the period from October 1, 2023, to September 30, 2024. This is the period to which the audit conclusion applies. However, to gain a more complete understanding of the subject matter of the audit, we also examined certain matters that preceded the start date of this period.

Date of the report

We obtained sufficient and appropriate audit evidence on which to base our conclusion on September 22, 2025, in Ottawa, Canada.

Audit team

This audit was completed by a multidisciplinary team from across the Office of the Auditor General of Canada led by Jean Goulet, Principal. The principal has overall responsibility for audit quality, including conducting the audit in accordance with professional standards, applicable legal and regulatory requirements, and the office's policies and system of quality management.

Recommendations and Responses

Responses appear as they were received by the Office of the Auditor General of Canada.

In the following table, the paragraph number preceding the recommendation indicates the location of the recommendation in the report.

Recommendation	Response
25. Shared Services Canada, in collaboration with Communications Security Establishment Canada, should develop a clear action plan with defined criteria and a timeline to develop a Security Information and Event Management application that addresses the existing gaps in cyber security monitoring.	**The department's response.** Agreed. Shared Services Canada has restarted and commits to completing the Security Information and Event Management (SIEM) project. Once completed, this will allow for more efficient situational awareness across Government of Canada environments. The department is currently focused on completing the ongoing procurement process and will be seeking the necessary contracting authorities by December 2025. Shared Services Canada will increase its ongoing collaboration with Communications Security Establishment Canada to develop agreements that facilitate appropriate funding arrangements for their role of analyzing daily cyber perimeter security events while the SIEM project is being completed.
30. Shared Services Canada should: • ensure that it has an up-to-date central inventory of networks and systems across federal organizations it services and a process to manage devices that need to be patched, updated, maintained, or replaced. The department should install the needed patches, perform the required updates, and maintain and replace networks and systems accordingly. • determine a solution to resolve the challenges facing the Endpoint Visibility, Awareness and Security project	**The department's response.** Agreed. In 2024, Shared Services Canada initiated a materiel management transformation initiative with the goal of strengthening our processes and systems for the management of assets for the department. It is expected that this initiative will continue to bring incremental improvements to Shared Services Canada's asset lifecycle controls until their completion in March 2028. The department is committed to resolving the challenges facing the Endpoint Visibility, Awareness and Security Project. A contract is expected to be awarded by the end of 2025.

Recommendation	Response
31. The Treasury Board of Canada Secretariat, in consultation with Communications Security Establishment Canada, should ensure that federal organizations: • implement cyber security defence sensors on all of its IT endpoint devices so that their associated vulnerabilities can be identified • remediate vulnerabilities in a timely manner	**The secretariat's response.** Agreed. The Treasury Board Secretariat, in consultation with the Communications Security Establishment of Canada, will work with federal organizations to ensure that cyber defense sensors are implemented on all IT endpoint devices so that their associated vulnerabilities can be identified and remediated in a timely manner. This includes leveraging the endpoint visibility and awareness (EVA) capability that will be available as part of Shared Services Canada's Endpoint Visibility, Awareness and Security (EVAS) initiative, which will enable the Government of Canada (GC) to identify assets that do not have cyber defense sensors deployed. Further, as per the Government of Canada Enterprise Cyber Security Strategy Implementation Plan, the establishment of a Federated Asset Inventory of GC Applications and Systems will enable streamlined collection and updates of GC application assets. In addition, as part of the GC Enterprise Vulnerability Management Program, the Treasury Board of Canada Secretariat, in collaboration with Shared Services Canada and the Communications Security Establishment Canada, will work with departments to identify, assess and prioritize the remediation of vulnerabilities on IT endpoint devices following a risk-based approach. At its next cyclical opportunity, the Treasury Board of Canada Secretariat will seek ongoing funding to support these initiatives.

Recommendation	Response
35. The Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada should re-evaluate their cyber security incident management practices to enable the better coordination and timely sharing of required critical information when responding to cyber attacks affecting federal organizations.	**The 3 organizations' response.** Agreed. The Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and Shared Services Canada will re-evaluate their cyber security incident management practices and protocols to enable better coordination and timely sharing of required critical information when responding to cyber security attacks affecting federal organizations. This includes testing the Government of Canada Cyber Security Event Management Plan (GC CSEMP) via a cyber simulation exercise to ensure effectiveness. Following the completion of a cyber simulation exercise the Treasury Board of Canada Secretariat will update and publish the GC CSEMP no later than end of fiscal year 2025-2026. In addition, as per the Government of Canada Enterprise Cyber Security Strategy Implementation Plan, the establishment of a GC-wide cyber security event collaboration platform and incident case management tool will enable seamless collaboration when managing GC response to cyber events. This includes support for centralized information sharing and tracking of internal GC mitigation efforts during a GC cyber security event for both central agencies and GC organizations. The Treasury Board of Canada Secretariat and Shared Services Canada will support the Canadian Centre for Cyber Security who is lead for the development and implementation of a cyber security event management platform and tool.
36. Communications Security Establishment Canada should finalize its funding request and prioritize its work to develop and implement a cyber security event collaboration platform and incident case management tool. The new platform and tool should enable the standardized communication, tracking, monitoring, and documentation of cyber security events and should be accessible by the Treasury Board of Canada Secretariat, Shared Services Canada, and other federal organizations.	**The agency's response.** Agreed. The Communications Security Establishment Canada will seek funding towards the establishment of a GC-wide cyber security event collaboration platform and incident case management tool to enable seamless collaboration when managing GC response to cyber events. This includes support for centralized information sharing and tracking of internal GC mitigation efforts during a GC cyber security event for both central agencies and GC organizations. Timeline: Unknown, subject to government decision making.

Appendix—Text Descriptions of Exhibits

Here are the text descriptions of the exhibits.

Exhibit 1—Cyber security event, cyber security incident, and cyber attack—Text description

This chart defines the terms “cyber security event,” “cyber security incident,” and “cyber attack” and includes examples for each term. It also shows that a cyber security event includes a cyber security incident and that a cyber security incident includes a cyber attack.

A cyber security event is any observable occurrence or change in a system or network that may have security relevance. Events do not necessarily mean a security breach or violation but can become incidents. Two examples of cyber security events are as follows:

- a user logging in to a system at an unusual time
- a firewall blocking a connection

A cyber security incident is an unauthorized or disruptive event that has an adverse effect on computer systems, networks, or data. It includes both intentional (malicious) and unintentional (accidental) events. All cyber security incidents are events, but not all incidents are attacks. Two examples of cyber security incidents are as follows:

- an unauthorized access to a system
- an accidental data exposure

A cyber attack is a deliberate, malicious action to access, disrupt, damage, or steal information from computer systems, networks, or devices. All cyber attacks are incidents. Three examples of cyber attacks are as follows:

- ransomware
- a denial-of-service attack
- a theft of data

Source: Based on information from Communications Security Establishment Canada and the Treasury Board of Canada Secretariat

Back to Exhibit 1

Exhibit 2—Objectives and key actions of the Government of Canada Enterprise Cyber Security Strategy—Text description

This chart shows the strategy objectives and examples of key actions of the Government of Canada Enterprise Cyber Security Strategy.

The strategy’s vision is as follows: “Building a world-class, sustainable, and resilient federal government to reduce cyber security risks so that departments and agencies can enable secure and reliable digital service delivery.” The federal organizations that are responsible for implementing the strategy are the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, Shared Services Canada, and other departments and agencies.

The chart lists 4 strategy objectives, and 2 examples of key actions are listed for each objective. There are many other actions under the strategy. The examples listed here represent some of the actions intended to have a government-wide impact.

- Strategy objective: Articulate cyber security risk and its business impacts. The 2 examples of key actions are as follows:
  - Establish a government-wide compliance and assurance program to assess departments' cyber security defences to identify and prioritize cyber security risks.
  - Create a government-wide vulnerability management program to manage and reduce vulnerabilities affecting government systems and networks.
- Strategy objective: Prevent and resist cyber attacks more effectively. The 2 examples of key actions are as follows:
  - Expand cyber security defences to small departments and agencies.
  - Establish a framework to improve the ability to detect and prevent fraudulent activity against government applications.
- Strategy objective: Strengthen capabilities and resilience across the Government of Canada. The 2 examples of key actions are as follows:
  - Establish a framework for departments to maintain accurate asset inventories of government applications and systems. Conduct year-round testing and reviews of cyber security protection and defence.
  - Implement a government-wide cyber security event collaboration platform to manage and respond to cyber events.
- Strategy objective: Foster a diverse federal workforce with the right cyber security skills. The 2 examples of key actions are as follows:
  - Build cyber talent through cross-functional training programs in cyber security.
  - Promote a talent management culture to recruit and retain skilled candidates.

Source: Based on information from the Government of Canada Enterprise Cyber Security Strategy, Treasury Board of Canada Secretariat, 2024

Back to Exhibit 2

Exhibit 3—Communications Security Establishment Canada developed 3 types of cyber security defence sensors to detect and mitigate cyber security events and cyber attacks—Text description

This chart shows the 3 types of cyber security defence sensors that Communications Security Establishment Canada developed and the years when they were each deployed.

In 2010, the department deployed the network-based sensor, which detects and mitigates cyber security incidents on the government's networks. This sensor is typically integrated with Shared Services Canada's Enterprise Internet Service.

In 2012, the department deployed the host-based sensor, which detects cyber attacks on IT endpoint devices such as laptop computers, servers, and local networks. The sensor analyzes and processes collected information to detect suspicious cyber security events occurring on a host machine. The information gathered is used to report anomalies and weaknesses to affected federal organizations.

In 2019, the department deployed the cloud-based sensor, which operates in federal organizations' cloud infrastructure and works in conjunction with the defences provided by cloud vendors. This sensor automates the collection of logged activity in the cloud and analyzes the information to detect and mitigate suspicious cyber security events.

Source: Based on information from Communications Security Establishment Canada

Back to Exhibit 3

Exhibit 4—The 119 federal organizations not required to use the cyber security services of Shared Services Canada (SSC) and Communications Security Establishment Canada (CSE) were encouraged to use the services, but many chose not to—Text description

This exhibit presents 2 charts: 1 chart showing the number of federal organizations that voluntarily use Shared Services Canada's Enterprise Internet Service and 1 chart showing the number of federal organizations that voluntarily use Communications Security Establishment Canada's cyber security defence sensors.

Of the 119 federal organizations that are not required to use Shared Services Canada's Enterprise Internet Service, 24 organizations, or 20%, voluntarily used it, and 95, or 80%, did not.

Similarly, of these 119 organizations, 76 organizations, or 64%, voluntarily used 1 or more of Communications Security Establishment Canada's cyber security defence sensors, and 43, or 36%, did not.

Source: Based on data from Shared Services Canada and Communications Security Establishment of Canada

Back to Exhibit 4

Office of the
Auditor General
of Canada

Bureau du
vérificateur général
du Canada