Unprotected

Audit of Cyber Security (Security Policy Implementation Notice)

Summary Report (For Online Publication)

Audit and Evaluation Branch

July 2025

This Publication is available online at https://ised-isde.canada.ca/site/audits-evaluations/en/internal-audit/internal-audit-reports-fiscal-year/audit-cyber-security-security-policy-implementation-notice-summary-report

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/publication-request or contact:

ISED Citizen Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: ISED@Canada.ca

Permission to Reproduce

Cat. No. Iu4-447/2026E-PDF

ISBN 978-0-660-79607-9

Aussi offert en français sous le titre *Audit de la cybersécurité (Avis de mise en œuvre de la politique sur la sécurité).*

Iu4-447/2026E-PDF
ISBN 978-0-660-79607-9

Background

Cyber Security at the Government of Canada (GC)

In August 2024, Treasury Board Secretariat (TBS) released the Security Policy Implementation Notice (SPIN) - *Improving Cyber Security Health* to reinforce requirements identified in the TBS Policy on Government Security and *the* Policy on Service and Digital. The purpose of the SPIN is to:

- reduce the overall attack surface and minimize the risk of unauthorized access to GC information systems as soon as possible;
- aggressively remediate known exploited vulnerabilities to protect federal information systems and reduce cyber incidents; and
- make measurable progress toward enhancing visibility into departmental assets and associated vulnerabilities.

To achieve these objectives, the SPIN required departments to implement specific measures to secure Information Technology (IT) assets, including deploying host-based sensors, developing a plan to identify, assess, and remediate vulnerabilities based on TBS' list of Top 25 vulnerabilities, and enforcing multifactor authentication with phishing-resistant security controls. TBS set an implementation timeline of three to nine months, depending on the specific initiative. Innovation, Science and Economic Development (ISED) was required to meet all SPIN cybersecurity requirements by May 2025.

Implementation of the SPIN at ISED

At ISED, the Digital Transformation Service Sector (DTSS) and the Chief Information Officer (CIO) are responsible and accountable for the development, implementation, improvement and monitoring of departmental IT security requirements, practices and controls. The responsibility for ensuring that the SPIN requirements are met is delegated to the Director of Cyber Security, who also serves as the Department Official for Cyber Security. The Director is accountable for reporting progress to the CIO and the Chief Information Officer Management Committee.

Prior Engagements

Between 2020 and 2025, the Audit and Evaluation Branch (AEB) conducted 5 engagements on various areas and controls of ISED's cyber security environment, including endpoint devices and the cloud. Many components requested by TBS in the SPIN, such as multifactor authentication, vulnerability management, and patch management, have been audited in these engagements. However, the requirements of the SPIN are different, necessitating a fresh perspective on these components.

Audit Objective and Scope

The objective of the engagement was to assess ISED's compliance with the SPIN.

The engagement's scope included an assessment of the compliance with all the requirements of the SPIN applicable to ISED, including:

- the review of the departmental records of information systems that support critical services and activities in the TBS Office of the Chief Information Officer's (OCIO) Application Portfolio Management (APM) tool or comparable tool;
- the deployment of the CCCS' host-based sensors (HBS) on all client endpoints in

accordance with the Government of Canada's Cloud Guardrails;
- the establishment of a plan following a risk-based approach to identify, assess and remediate applicable vulnerabilities from TBS's Top 25 Vulnerabilities List and to implement mitigation measures;
- the elaboration of an emergency patch management plan with clear roles and responsibilities;
- the onboarding of publicly accessible systems into the Canadian Center for Cyber Security (CCCS)' National Cyber Threat Notification System; and
- the implementation of secure remote access configurations that enforce phishing proof multifactor authentication and provide a secure, encrypted connection to the Government of Canada enterprise network.

The scope of this audit included all endpoint devices and internal and public facing systems managed by ISED. The audit covered the period of August 2024 to May 2025. Information technology assets managed by Shared Services Canada (SSC) were not included in the scope of this engagement.

Approach

The methodology for this engagement included various procedures to address the engagement objective, such as:

- documentation review;
- interviews;
- walkthroughs of systems and processes; and
- sampling and testing endpoint devices and secure remote access configurations.

Criteria

Based on the entity risk assessment, review criteria and sub-criteria linked to the overall review objective were developed for this engagement (see Appendix A). They generally follow the structure of the SPIN's requirements.

Conformance

This engagement was conducted in accordance with the Institute of Internal Auditors Standards and the Treasury Board *Policy on Internal Audit*, as supported by the results of the Audit and Evaluation Branch's quality assurance and improvement program.

Findings and conclusions

The findings and conclusions of this audit were shared internally with DTSS, the CIO, the Deputy Minister and the Departmental Audit Committee. For security reasons, the Audit and Evaluation Directorate does not publish audit findings related to cyber security analyses.

Appendix A: Review Criteria

Review Criteria	Sub-Criteria
Criterion Theme - Identify Assets	
Criterion 1: There is continuous and comprehensive asset visibility, along with the monitoring of these assets, to effectively manage cyber security risks to the ISED enterprise network.	The information entered into the Application Portfolio Management (APM) for mission critical applications is accurate and complete.
	Endpoint devices have had the CCCS host-based sensors deployed onto them.
	The CCCS' cloud-based sensors have been fully deployed, according to the Government of Canada's Cloud Guardrails.
Criterion Theme – Understanding Exposure	
Criterion 2: There is an understanding of the security exposure of assets to enable a risk-based approach for prioritization of mitigation measures.	The plan to identify, assess and remediate applicable vulnerabilities from the Top 25 Vulnerabilities List is comprehensive and risk-based.
	The Emergency Patch Management Plan to support the execution of emergency patches to address critical vulnerabilities is comprehensive and aligned with GC and SSC guidance.
	Publicly accessible systems have been onboarded into CCCS' National Cyber Threat Notification System to ensure that departments are notified of misconfigured services, vulnerabilities, and compromised infrastructure on their Internet Protocol address (IP) space.
Criterion Theme - Reduce Exposure	
Criterion 3: ISED's overall attack surface is reduced and safeguards to minimize the risk of unauthorized access to departmental information systems have been implemented.	Mitigation strategies have been implemented to address the applicable vulnerabilities from the Top 25 Vulnerabilities List based on previously developed action plans (in response to SPIN Criteria 6.2.2) with a priority focus on information systems that are publicly accessible.
	Multifactor authentication is enforced with security measures to achieve phishing resistance for the overall authentication process, such as ensuring that the user is authenticating from a GC-managed device, verifying the device is configured properly, and detecting anomalous geolocation.
	A secure, encrypted connection to the GC enterprise network (section 3.1 of the Remote Access Configuration Requirements) using GC-approved pathways to the Internet rather than via a direct connection to the Internet, to leverage the CCCS' cyber defences.