

Cyber Readiness in the Frontier AI Era

A practical guide to Canada's October 2026 direction

By Junior Williams | 6 October 2026

For security leaders, IT teams and organizations responsible for keeping critical services available.

AI-enabled attacks put more pressure on the time between discovering a weakness and fixing it. Canada's new cyber security direction responds with six areas of action: know what matters, fix weaknesses faster, strengthen identities, contain compromise, improve detection and prove recovery.

Start with the service

Choose a critical service. Map the systems, identities, suppliers and recovery dependencies behind it. Use this guide to identify gaps, assign owners and collect evidence that the controls work.

Inside this guide

Topic	Page
Scope, dates and implementation approach	2
Identify, accelerate, harden, fortify, monitor and prepare	3-8
A suggested 30 / 60 / 90-day implementation plan	9
A scorecard built around evidence	10
A working assessment and exercise	11
Sources and key terms	12

Based on the Government of Canada's Security Policy Implementation Notice (SPIN), effective 1 October 2026. This is an independent interpretation and implementation guide. Federal direction is identified separately from recommendations in this guide.

SCOPE AND PRIORITIES

What the direction means

The SPIN reinforces existing federal security and digital-policy requirements. Its purpose is to apply baseline controls consistently, close material gaps and operate with an assume-breach approach so that compromise can be contained and services restored quickly.

Who it applies to

The notice applies to organizations listed in section 6 of the Policy on Government Security. Its scope includes federal information systems, software, hardware and IP-addressable assets, across on-premises, roaming and GC-managed cloud environments. Printers, connected laboratory equipment, network appliances and other less visible devices are included.

For organizations outside that federal scope, the six pillars offer a useful readiness framework. Applicability to a supplier should be established through its specific contract and relevant obligations. The notice directs departments to reflect relevant requirements in procurement, contracts and ongoing contract management.

Two dates to keep straight

1 October 2026: the notice takes effect. 30 November 2026: departments must submit their prioritized critical-services list in TBS's Enterprise Portfolio Management (EPM) tool under IDT-1. The November date is a list-submission deadline; the SPIN does not set it as a deadline for completing every control.

Start small, then extend coverage

Section 7 sets out a phased, risk-informed approach. Where capacity prevents simultaneous implementation across all critical services, the notice recommends an initial Category 1 scope of no more than three highest-priority services. Category 2 extends the same approach to the remaining critical services.

Departments retain responsibility for their information and assets when SSC or another provider supplies part of the service. Map those dependencies and agree who implements, verifies and maintains each control. The notice complements existing obligations.

[Source: SPIN, sections 1-4, 7.1-7.3 and IDT-1.](#)

1. Identify what matters

Start with critical services and the dependencies that let them run. Rank services by the operational, legal, financial and reputational impact of compromise. A useful inventory supports decisions about exposure, ownership and recovery.

SPIN ID	Federal direction, summarized
IDT-1	Rank critical services and supporting systems by impact. Submit the prioritized list in EPM by 30 November 2026.
IDT-2	Keep critical-service applications current in the Application Portfolio Management (APM) tool, including owners and versions. Link to SSC asset stores where possible.
IDT-3	Maintain architecture diagrams showing service dependencies, edge devices, network segments, identity systems and administration paths. Use them to examine likely attack paths.
IDT-4	Inventory Internet connections, public IPs where available, subnets and sub-domains. Provide the list and updates to the Cyber Centre's National Cyber Threat Notification System (NCTNS).
IDT-5	Maintain software bills of materials (SBOMs) for department-developed software supporting critical services. Use them to track and update dependencies.
IDT-6	Onboard to SSC's Endpoint Visibility and Awareness (EVA) solution, prioritizing endpoints that support critical services.

Evidence to collect

This guide recommends a dated service list, named business and technical owners, application and endpoint inventories, architecture diagrams, an external-exposure register and current SBOMs. Reconcile the inventories with observed assets so an unrecorded device can become an assigned remediation task.

First working question

If one important service went offline today, could its owner identify the systems, identities, suppliers and backup dependencies needed to restore it? Record every unknown and assign an owner.

Source: SPIN, section 6.1: Appendix A, Table A-1.

2. Accelerate remediation

The notice describes a shrinking window between vulnerability disclosure and exploitation. It also highlights the risk that lower-severity flaws can be combined into a high-impact attack. Prioritization therefore needs exposure, likely exploitation and service impact alongside severity.

SPIN ID	Federal direction, summarized
ACC-1	Regularly triage and act on relevant vendor alerts, Cyber Centre and NCTNS notifications, and central GC exposure findings.
ACC-2	Operate a risk-based vulnerability and patch process aligned with GC guidance. Accelerate work on critical, Internet-facing and other high-risk systems; use compensating controls when timely patching is infeasible; address unsupported technology; track progress and document delays.
ACC-3	Use defensive AI models and security tools safely, securely and responsibly to find vulnerabilities and analyze code.

Give each finding a decision path

This guide recommends recording the affected service, exposure, exploitation evidence, likely impact, owner, target date and validation method. Agree emergency change and rollback paths before an urgent vulnerability arrives. When a fix must wait, document the temporary control, remaining risk, decision authority and review date.

Use the GC Vulnerability Listing and other GC tools where available. Several references in the notice are accessible only through government networks; a public guide cannot supply their internal content or replace departmental access.

Read the timing measures carefully

Appendix A proposes triage, risk assessment and a documented response within 10 business days for high- and critical-severity notifications. This is a notional KPI for triage, not a universal patch deadline or permission to leave an exposed system vulnerable for that period. ACC-2 calls for faster targets on the highest-risk systems.

Evidence to collect

Keep alert-to-ticket records, remediation decisions, patch or mitigation evidence, rescans and an exception register. For AI-assisted review, record tool approval, the data boundary, reviewed findings and confirmed fixes.

Source: SPIN, section 6.2; Appendix A, Table A-2.

3. Harden every identity

Identity controls cover people, administrators, service accounts, machine identities and AI agents. Treat each identity as an access path with an owner, a purpose and permissions that can be reviewed and revoked.

SPIN ID	Federal direction, summarized
HRD-1	Enforce MFA for all user accounts. Use phishing-resistant MFA for administrative, privileged and other high-risk accounts.
HRD-2	Block weak, common and known-compromised passwords through current protection policies and tools.
HRD-3	Enforce least privilege and review access regularly, starting with accounts administering critical services.
HRD-4	Default to centralized authentication and single sign-on. Use an enterprise password manager where these are unavailable.
HRD-5	Reserve dedicated administrator accounts for administration. Use centrally managed privileged access management (PAM) for auditable, just-in-time elevation; an enterprise password manager is an interim measure where PAM is unavailable.
HRD-6	Govern non-person entities, including AI agents, with ownership, purpose, life cycle controls and privilege reviews. Minimize persistent access and static credentials.
HRD-7	Use centrally managed identity threat detection and response (ITDR) to find and reduce identity attack paths, prioritizing critical services and privileged accounts.
HRD-8	Update awareness and simulation programs for AI-enabled phishing, voice scams, deepfakes and helpdesk impersonation, with targeted exercises for high-risk roles.

Evidence to collect

This guide recommends identity inventories, enforced MFA reports, privileged-access reviews, PAM session records and a register for service and agent identities. The register should record an owner, purpose, credentials, rotation schedule and revocation route. Check that the permissions in use match the approved purpose.

Practical check: select one AI-agent or service identity. Confirm who can disable it, what systems it can reach and how its actions appear in monitoring.

Source: [SPIN, section 6.3; Appendix A, Table A-3.](#)

4. Limit the impact of compromise

Assume breach means designing controls on the expectation that an attacker may gain a foothold. Reduce the paths from that foothold to critical systems, administrative access and recovery infrastructure.

SPIN ID	Federal direction, summarized
FTY-1	Harden edge devices, remote access, administrative interfaces, public services and APIs to essential functions. Remove unnecessary software, services and components.
FTY-2	Inventory vendor remote access, use approved methods, limit access by time or task, monitor sessions and remove dormant or unneeded access quickly.
FTY-3	Place critical-service systems in segmented network zones aligned with the referenced Cyber Centre standards or equivalent controls.
FTY-4	In environments hosting critical services, deny outbound Internet traffic by default and allow explicitly approved connections.
FTY-5	Perform administration from GC-approved hardened endpoints over protected, monitored administrative channels isolated from lower-trust environments.

Work through an attack path

This guide recommends tracing a plausible path from a compromised employee account or vendor connection to the critical service. Identify where the path crosses a network zone, gains privileges or reaches a management interface. Test the controls that should stop those transitions.

For outbound restrictions, identify legitimate destinations and service dependencies before enforcement. Test the approved connections and check how temporary exceptions are authorized and removed. Apply restrictions through the established change process so containment controls preserve essential service functions.

Evidence to collect

Keep approved hardening baselines, configuration checks, zone diagrams, firewall rules, tested outbound allow-lists, vendor-access records and administrative session evidence. A diagram states the design; a controlled test shows whether the boundary is enforced.

Source: SPIN, section 6.4; Appendix A, Table A-4.

5. Make suspicious activity visible

Teams need visibility to recognize malicious activity, establish its reach and support containment. Start with the systems and administrative functions behind critical services.

SPIN ID	Federal direction, summarized
MTR-1	Implement logging in line with GC Event Logging Guidance, beginning with critical services. Cover endpoints, identity, cloud and edge devices end to end.
MTR-2	Protect logs from tampering using approved cryptographic safeguards. Forward them to a central facility for storage, monitoring and analysis.
MTR-3	Deploy centrally managed endpoint detection and response (EDR/XDR) on endpoints supporting critical services and administration, integrated with departmental logging and monitoring.

Check the whole detection path

This guide recommends tracing a permitted test event from its source to central monitoring, then to an alert, a responder and a decision. Check timestamps and asset context, including what happens when a log source or endpoint agent stops reporting.

Test	Evidence to retain
A relevant identity or endpoint event occurs	The original event, asset and identity context, and timestamp
The event reaches central monitoring	Ingestion evidence and the matching central record
An alert requires investigation	Alert details, assigned owner, escalation and response record
A sensor stops sending telemetry	The health alert and the action taken to restore coverage

Measure useful coverage

Report active, reporting sensors and required log sources for the systems in scope. Pair coverage figures with a recent detection test so leaders can see whether the information reaches someone able to act.

The notice also discusses deception trip wires. Use them where the team can monitor and respond to their signals effectively.

Source: SPIN, section 6.5: Appendix A, Table A-5.

6. Prove containment and recovery

Preparation connects technical response to service continuity. During an incident, the team needs clear authority, workable containment steps and a tested route back to a trusted service.

SPIN ID	Federal direction, summarized
PRP-1	Keep the cyber security event management plan (CSEMP) current, with clear authority and escalation aligned to the business continuity plan (BCP).
PRP-2	Run regular tabletop exercises to test the CSEMP and its alignment with business continuity.
PRP-3	Maintain approved incident playbooks with decision steps, service levels, escalation, pre-approved containment and forensic telemetry procedures.
PRP-4	Regularly test restores for critical-service systems and verify restored data against a known good reference.
PRP-5	Logically separate critical-service backups from production. Use immutable or write-once storage where feasible and protect the backup environment with access controls and monitoring.

Test a service, including its dependencies

This guide recommends restoring a representative service in a controlled environment and checking the application, data, identities and dependencies needed for operation. Record elapsed time and compare the result with the organization's continuity requirements. Capture the reference used to check data integrity.

Exercise who may isolate a host, disable an identity, block traffic or restrict vendor access. Confirm how those decisions are made when the usual communication channel or administrator account is unavailable. Record the changes required in the playbook and continuity plan.

Evidence to collect

Retain the approved plans and playbooks, exercise attendance, decisions, containment-test results, restore logs, integrity checks and a corrective-action list with owners and dates. Use the findings to update the plans before the next exercise.

Source: SPIN, section 6.6: Appendix A, Table A-6.

SUGGESTED IMPLEMENTATION APPROACH

A practical 30 / 60 / 90-day plan

This schedule is a suggested implementation cadence. The SPIN calls for phased, risk-informed work and sets a separate 30 November 2026 submission deadline for the prioritized critical-services list. Follow applicable GC remediation time frames and respond sooner where exposure warrants it.

Days 1-30: establish scope and act on exposure

Name an accountable lead and service owners. Rank critical services; use the notice's initial scope of up to three services where capacity is constrained. Map applications, identities, endpoints, suppliers, Internet exposure and recovery dependencies. Assign each gap to an owner. Triage urgent vulnerabilities, exposed management interfaces and unsupported components. Patch, mitigate, isolate or retire according to risk. Check privileged MFA, incident decision authority, logging coverage and backup separation. Start coordinating provider responsibilities.

Days 31-60: implement and verify controls

Close prioritized patch, identity and configuration gaps. Record exceptions and review dates. Restrict vendor and administrative access; validate network boundaries and approved outbound connections. Test log collection, endpoint reporting and escalation from a relevant alert to a responder. Update incident playbooks and continuity dependencies. Perform a representative restore and integrity check.

Days 61-90: exercise and expand

Run a service-focused tabletop with security, IT, business and provider participants. Validate containment decisions, evidence collection and recovery. Assign corrective actions and retest material failures. Present the evidence scorecard, unresolved risks and resource decisions to the accountable executive. Extend the working inventory, controls, tests and reporting approach to the remaining critical services.

Keep the decision record current

For each material gap, record the service at risk, responsible owner, target date, temporary protection, approval and evidence required for closure. Update the record when conditions change.

[Source: Implementation principles: SPIN, section 7. Timing and work sequencing on this page are recommendations in this guide.](#)

A SCORECARD FOR THE SERVICES IN SCOPE

Report readiness with evidence

Appendix A offers a notional set of KPIs. Use them to shape reporting, with a named scope, denominator, observation date and evidence source. The scorecard below selects themes from the appendix; it is not a prescribed reporting template or a complete list of its measures.

Area	Measure to report	Supporting evidence
Identify	Critical-service applications inventoried; diagrams current; endpoints visible and healthy	Portfolio records, dated diagrams and endpoint reports
Accelerate	High-risk findings fixed or mitigated within applicable targets; overdue exceptions documented	Tickets, validation scans and exception approvals
Harden	User MFA enforced; privileged phishing-resistant MFA; non-person identities governed	Identity policy reports, reviews and ownership register
Fortify	Hardening, segmentation, outbound restrictions and protected administration validated	Configuration audits, rule reviews and boundary tests
Monitor	Required logs centralized; EDR/XDR active and reporting	Log-source inventory, central records and agent health
Prepare	Services exercised; approved playbooks current; restores pass integrity and continuity checks	Exercise records, playbooks and restore-test evidence

Make gaps visible in the denominator

This guide recommends reporting the count as well as the percentage, and identifying unknown or unmanaged assets separately. Define exclusions explicitly. Keep installation counts separate from active, healthy coverage when the measure requires operational telemetry.

A closure record should answer four questions

What changed? Which service and assets does it cover? How was it tested? What risk or exception remains? Link the evidence and record who accepted the result.

Source: SPIN, section 8 and Appendix A. Reporting practices are recommendations in this guide.

ASSESSMENT AND EXERCISE WORKSHEET

Use this in the next working session

Choose one critical service and answer the questions below using current evidence. Record unknowns as open work. The worksheet and scenario are recommendations in this guide for putting the six pillars into practice.

Record	Questions to answer
Service and impact	What does the service deliver? Who owns it? What would fail if it were unavailable or its information were altered?
Dependencies	Which applications, networks, identities, suppliers and backup systems does it need? Where is the current diagram?
Exposure and fixes	Which public or administrative interfaces are reachable? Which urgent vulnerabilities, unsupported systems or exceptions remain?
Identity and access	Which people, vendor accounts and non-person identities can administer it? Are privileges, MFA and revocation tested?
Detection and response	Which events reach central monitoring? Who receives an alert and has authority to contain the incident?
Recovery	When was the service last restored? Was data integrity checked? Which continuity requirement did the result satisfy?

Questions for a provider

Ask which controls the provider operates, what evidence it supplies, how remote access is recorded, and how it supports containment and recovery. Check the answers against the contract and record unclear responsibilities.

A tabletop scenario to test

A vendor identity is compromised while a public component has an urgent vulnerability. Suspicious administrative activity appears in monitoring. The team must determine the extent of compromise while maintaining essential delivery.

Work through who revokes access, isolates systems, preserves evidence and decides whether to restore. Test how the team proceeds without its usual administrator account or communication tool. Record stalled decisions and untested dependencies.

Finish with an action record: gap | service | owner | target date | temporary protection | closure evidence | remaining risk. Retest the material gaps before marking them closed.

Source: Underlying requirements: SPIN, sections 6.1-6.6 and 7.3. Worksheet and scenario are original recommendations in this guide.

REFERENCE

Sources and key terms

Primary source

[Government of Canada: Direction on Government of Canada Cyber Security Readiness in the Frontier Artificial Intelligence Era](#), Security Policy Implementation Notice. Effective and page-modified date: 1 October 2026. Reviewed for this guide on 6 October 2026.

Pages 3-8 cover all 30 action IDs. Consult the SPIN for the full direction, policy references and notional KPI tables. The implementation plan, evidence suggestions and worksheet are recommendations in this guide.

Public resources linked by the notice

- [Policy on Government Security](#) and [Policy on Service and Digital](#).
- [GC vulnerability guidance](#) and [patch guidance](#).
- [GC MFA guidance](#) and [event logging guidance](#).
- [Cyber Centre: Frontier artificial intelligence](#).

These links are further reading cited by the SPIN. This guide summarizes the SPIN, including its references to government-network-only resources.

Terms used in this guide

Term	Meaning
Critical service	A service prioritized for the impact of disruption or compromise, with its supporting systems identified.
Assume breach	Design and operate on the expectation that compromise may occur; prepare to contain it and recover.
SBOM	Software bill of materials: an inventory of a software product's components and dependencies.
Non-person entity	A service account, service principal, machine identity or AI-agent identity.
PAM / ITDR	Privileged access management / identity threat detection and response.
EDR / XDR	Endpoint detection and response / extended detection and response.
CSEMP / BCP	Cyber security event management plan / business continuity plan.

By Junior Williams | [trustcyber.ca](#). Independent commentary; government endorsement is not implied. Check applicability against current official documents and contracts.