CYERA

Canada's CCSPA: What it is, why it matters, and how to get ready

Canada is moving toward a federal, cross-sector cybersecurity regime for critical infrastructure. Under the proposed Bill C-8 or Critical Cyber Systems Protection Act (CCSPA), the federal government can **designate vital services and systems** and the **operators** responsible for them ("designated operators"). Those operators must:

- **Establish a cybersecurity program** and file it with their sector regulator (typically within 90 days of designation);
- **Mitigate supply-chain and third-party risks;**
- **Report cybersecurity incidents** to the Canadian Centre for Cyber Security within prescribed timelines;
- **Comply with binding cybersecurity directions** issued by the government; and
- **Maintain records** to demonstrate compliance.

Although the CCSPA is not yet law, its structure and obligations closely mirror an earlier bill (Bill C-26) that had advanced through both chambers in 2024 but ultimately did not receive Royal Assent before the parliamentary reset in January 2025. The new bill (Bill C-8) will become the CCSPA once it passes Parliament, as it's expected to do this session.

What it means for affected industries

Energy.

Owners and operators of federally-regulated energy systems (e.g., pipelines, certain generation/transmission assets under the Canadian Energy Regulator) would be required to formalize cyber programs, continuously assess supplier/OT risks, and rapidly notify material incidents. Expect regulator audits and potential administrative monetary penalties for failures to implement and maintain programs.

Telecommunications.

In addition to CCSPA duties, telecom providers face **expanded ministerial powers** under the amended Telecommunications Act—up to and including orders to remove or not use specified equipment/services for national-security reasons, and to take actions necessary to secure networks. This codifies the federal ability to act quickly on systemic risks in the telecom stack.

Financial services.

Banks and other federally-regulated financial institutions would be designated operators with obligations to implement programs, report incidents, and preserve auditable records. Oversight and enforcement authorities are explicitly laid out for the Office of the Superintendent of Financial Institutions (OSFI), including compliance orders and monetary penalties.

Across sectors, the CCSPA's emphasis on **third-party and supply-chain risk, incident notification,** and **demonstrable governance** is clear—and non-compliance can trigger significant administrative penalties.

CYERA

Canada's CCSPA: What it is, why it matters, and how to get ready

Part of a global trend toward tougher critical-infrastructure rules

Canada's move aligns with what we're seeing worldwide:

- **EU NIS2.** NIS2 (Directive 2022/2555) expanded its scope to "essential" and "important" entities and imposed risk-management and incident-reporting obligations across many sectors.
- **Australia's SLACIP amendments.** The 2022 SLACIP Act strengthened the Security of Critical Infrastructure Act by requiring risk-management programs and creating enhanced obligations for "systems of national significance."
- **China's Cybersecurity Law (CSL) & CIIO regime.** Operators of **critical information** infrastructure (CII) face elevated duties, including security reviews and localized controls for key data and network operations.

The common threads: **board-level accountability, third-party risk control, rapid incident reporting, and regulator visibility.** Canada's CCSPA fits this pattern.

How Cyera helps designated operators get compliant faster

Whether you're in energy, telecoms, transportation or finance, CCSPA readiness hinges on knowing **where critical data lives, how it moves, who can access it, and whether controls are working** —continuously and provably. That's Cyera's wheelhouse.

- **Data discovery & classification across clouds and data stores.** Cyera's **DSPM** maps regulated and sensitive data across your environments, enriching it with business context to feed your **cybersecurity program** and asset inventories. This supports CCSPA duties to establish and maintain a program grounded in real risk.
- **Supply-chain & third-party risk visibility.** Leverage Omni DLP to trace data flows to and from vendors and managed services; identify shadow integrations and over-privileged service accounts; generate evidence for **third-party risk mitigation** requirements.
- **Least-privilege access & policy enforcement.** Utilize **Identity Access** to demonstrate continuous program maintenance and due diligence by detecting excessive permissions and misconfigurations, and automating guardrails to reduce an incident's blast radius.
- **Incident readiness & reporting.** Maintain lineage and data-impact context to accelerate triage and produce regulator-friendly incident reports that answer "what data, where, and who" within hours—not weeks.
- **Audit-ready evidence & records.** One-click reports show current data locations, access, retention, and policy effectiveness, providing automated, auditable evidence of compliance..

Bottom line

The CCSPA would formalize a risk-based cybersecurity baseline for Canada's most vital services, with special attention to supply chains and timely incident response. Organizations in energy, telecoms, and finance that **build a data-centric program now**—backed by continuous discovery, access control, third-party oversight, and audit-ready reporting—will be best positioned to comply when the law takes effect.