carahsoft.

Bill C-8: Canada's Critical Cybersecurity Framework

Preparing for the Critical Cyber Systems Protection Act (CCSPA)

June 2026

Overview

Granted Royal Assent on June 15, 2026, Bill C-8 establishes a major new federal cybersecurity framework for federally regulated critical infrastructure. It creates a dual regime: Part 1 amends the Telecommunications Act to make telecommunications security a formal policy objective and authorizes binding government orders to service providers, while Part 2 enacts the Critical Cyber Systems Protection Act (CCSPA), establishing mandatory cybersecurity obligations for designated operators of critical cyber systems. Part 1 is in force. The CCSPA has been enacted but is not yet in force: as of September 2026, no coming into force order has been made and Schedule 2 remains empty, so no operator classes are currently designated under the Act.

Framework

The CCSPA establishes a framework to protect critical cyber systems supporting services and systems vital to national security or public safety. Once in force, it will define which operators are covered, establish cybersecurity and incident-reporting obligations, address supply-chain risk, and provide compliance and enforcement authorities through existing federal regulatory bodies rather than a single new regulator.

Framework components include:

- **Designated Operators and Critical Cyber Systems**
  Schedule 1 lists six vital services and systems: telecommunications, interprovincial and international pipelines and power lines, nuclear energy, federally regulated transportation, banking, and clearing and settlement. Schedule 2 will identify covered classes of operators and their corresponding regulators through orders of the Governor in Council; it is currently empty.
- **Cyber Security Programs**
  Once applicable, designated operators will be required to establish a documented cybersecurity program addressing risk identification and management, protection of critical cyber systems, incident detection, impact minimization, and prescribed requirements. The program must generally be established within 90 days after an operator becomes a member of a designated class, subject to an extension granted by the regulator, and reviewed on prescribed dates or annually if no dates are prescribed.
- **Incident Reporting**
  Once applicable, designated operators will be required to report prescribed cybersecurity incidents involving critical cyber systems to the Communications Security Establishment (CSE) within a period set by regulation, which may not exceed 72 hours. CSE may share incident report information with the appropriate regulator in accordance with the Act.
- **Supply-Chain and Third-Party Risk**
  Once applicable, designated operators will be required to identify and manage cybersecurity risks associated with their supply chains and use of third-party products and services, and to take reasonable steps to mitigate identified risks as required by the Act and regulations.
- **Cyber Security Directions and Telecommunications Orders**
  The regime authorizes binding, and potentially confidential, cybersecurity directions to designated operators and separate orders affecting telecommunications service providers, including restrictions on specified products or services and requirements relating to equipment removal.
- **Records, Oversight and Enforcement**
  The CCSPA establishes Canadian record keeping requirements for specified compliance records and distributes inspection, internal audit, compliance order, and administrative monetary penalty authorities across six federal regulatory authorities. A ministerial review of the legislation is required within five years of Royal Assent.

What Does This Mean for Government?

Federal implementation now shifts from legislation to operationalization. Regulatory responsibility will be distributed across six federal authorities: OSFI, the Bank of Canada, the Minister of Industry, the Minister of Transport, the Canadian Energy Regulator, and the Canadian Nuclear Safety Commission. CSE will serve as the central recipient of cybersecurity incident reports and a source of

technical guidance. Key operational details will be established through coming-into-force orders, Schedule 2 designations, regulations, and guidance.

Key implementation priorities include:

- Bringing relevant CCSPA provisions into force and establishing covered operator classes and corresponding regulators through Schedule 2
- Developing regulations and guidance defining cybersecurity-program requirements, incident-reporting periods, record requirements, and administrative monetary penalties
- Building regulator capacity for inspections, internal audits, compliance orders, enforcement, and information sharing with CSE
- Notifying NSICOP and NSIRA within 90 days after a Governor in Council cybersecurity direction is made, as required by the Act

What Does This Mean for Government?

Once the CCSPA comes into force and Schedule 2 classes are designated, covered operators will face binding cybersecurity duties backed by significant financial and personal exposure, shifting cyber risk management from best practice toward documented and auditable compliance. Technology suppliers may also feel the regime indirectly through procurement requirements, contract terms, audit rights, incident-notification clauses, and increased vendor-risk scrutiny.

Key implications include:

- A 90-day cybersecurity-program compliance period generally applies after an operator becomes a member of a class designated in Schedule 2 following publication of the applicable order in the Canada Gazette, Part II. Extensions may be available on written request to the appropriate regulator.
- A broad incident-reporting trigger will capture prescribed incidents affecting, or having the potential to affect, critical cyber systems, with reports to CSE due within the regulatory period, which cannot exceed 72 hours. These requirements may operate alongside other applicable privacy and sector-specific breach notification duties.
- Formalized supply-chain risk management, including greater scrutiny of third-party products and services, contract controls, audit rights, and incident-notification terms.
- Canadian record-keeping requirements will require specified compliance records relating to program implementation, reportable incidents, supply-chain mitigation, and cybersecurity directions to be kept in Canada.
- Substantial penalty exposure: statutory maximums can reach $15 million per violation for organizations and $500,000 for individuals, with each day of a continuing violation potentially constituting a separate violation, in addition to offence provisions and potential director and officer liability.
- Commercial uncertainty from supplier exclusion powers, including stranded asset risk, as no compensation is payable for losses from an order.

What Does This Mean for Government?

Once in force and applicable, the CCSPA will make cybersecurity capabilities increasingly important to auditable compliance, with implications for asset visibility, detection and response, logging, third-party risk, governance, and compliant record management. Covered operators will need to demonstrate that controls are documented, maintained, reviewed, and capable of supporting prescribed incident-reporting and regulatory requirements.

Key technology considerations include:

- Asset visibility and risk management, including inventory, criticality mapping, vulnerability management, and continuous risk assessment
- Security monitoring and incident response, including logging, SIEM/XDR, SOC tooling, orchestration, and incident-management capabilities that can support reporting to CSE within the prescribed timeframe, which cannot exceed 72 hours
- Supply-chain and third-party risk management, potentially increasing demand for software supply-chain visibility, SBOM capabilities, vendor attestations, and continuous vendor-risk monitoring

- Governance, compliance, and secure record management, including audit trails, evidence management, policy controls, and Canadian storage for records the Act requires to be kept in Canada
- Vendor and equipment visibility, including asset and supplier inventories capable of identifying affected products if federal authorities restrict suppliers, products, services, or require equipment removal

What Does This Mean for Government?

Policy Elements	Key Dates	Focus & Key Provisions
Bill C-8 Introduced	**June 18, 2025**	Reintroduced in the 45th Parliament after predecessor Bill C-26 died on the Order Paper at prorogation in January 2025.
Committee Amendments	**March 2026**	Maximum individual CCSPA penalty cut from $1M to **$500,000**.
Royal Assent	**June 15, 2026**	Adopted by the Senate June 4; enacted as **S.C. 2026, c. 9** (CCSPA is s. 11).
Telecommunications Act Amendments (Part 1)	**In Force**	Adds security as a telecom policy objective and authorizes supplier prohibitions and equipment removal. Penalties reach **$10M ($15M for subsequent contraventions)**.
CCSPA (Part 2) Coming into Force	**Not Yet Set**	Phases in on day or days fixed by the Governor in Council. No coming-into-force order identified as of September 2026.
Schedule 2 Designation Orders	**Not Yet Made**	Schedule 2 remains empty, so no operator classes are currently designated. Once an applicable order is published in the Canada Gazette, Part II, covered operators generally have 90 days after becoming members of a designated class to establish their cybersecurity programs.
Regulations & Consultation	**To Be Developed**	Will establish key implementation details, including cybersecurity-program requirements, incident-reporting periods (capped at 72 hours), prescribed requirements, and administrative monetary penalty amounts.
Statutory Review	**By June 2031**	Ministerial review of the Act, reported to Parliament.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.