

Bill C-8 readiness

What to build before the CCSPA takes effect

Junior Williams | TrustCyber | 12 October 2026

Canada's cyber security legislation has passed. Leaders in potentially covered sectors can use the implementation period to settle three practical questions: which systems support their vital services, who can make an incident-reporting decision, and what evidence shows that security work is happening.

Where does the law stand?

Bill C-8 received Royal Assent on 15 June 2026 as S.C. 2026, c. 9. It enacted the Critical Cyber Systems Protection Act (CCSPA). The Justice Laws text reviewed on 12 October still marks that Act as not in force. Part 2 takes effect on a day or days fixed by Governor in Council order. [1, 2]

The Telecommunications Act amendments took effect on Royal Assent. They add security as a policy objective and introduce powers to direct telecommunications providers to take, or refrain from taking, security-related actions. That is a separate part of the legislation. [2, 3]

The decision now: appoint an accountable executive, map candidate critical cyber systems, and rehearse an incident escalation. Keep the final compliance specification open until the applicable orders, regulations and regulator requirements are confirmed.

Who should prepare?

Schedule 1 lists telecommunications services; interprovincial or international pipeline and power line systems; nuclear energy systems; transportation systems within Parliament's legislative authority; banking systems; and clearing and settlement systems. [1]

Sector membership alone does not establish designation. Section 7 provides for orders adding classes of operators and their corresponding regulators to Schedule 2. That schedule has no classes listed in the text reviewed. A critical cyber system is defined by how a compromise could affect the continuity or security of a vital service or system. [1, ss. 2, 7-8]

For a potentially covered operator, start with the service and trace its technology dependencies. For a supplier, identify customers whose critical services depend on your products, remote access, hosting or operational support. Supplying a designated operator does not, by itself, make a supplier a designated operator.

Reading this brief: legal provisions are cited by section; the preparation steps are TrustCyber recommendations. This is operational guidance, not legal advice. Confirm applicability and obligations with counsel and the relevant regulator.

What would operators have to build?

The enacted framework combines a maintained security program, incident reporting, supplier-risk mitigation and records of implementation. These CCSPA duties apply when the relevant provisions are in force and an organization falls within a designated class. Regulations and regulator decisions will supply important details. [1]

One 90-day window for the program and regulator access

After publication of the designation order in Canada Gazette Part II, section 9 requires a program within 90 days of the operator becoming a member of the class. The program must address organizational cyber risks, including supply-chain and third-party risks; protection of critical cyber systems; incident detection; impact reduction; and any prescribed requirements.

Written notice to the regulator follows immediately after the program is established. Section 10 requires the program to be provided or made available within the same 90-day period measured from class membership. These are concurrent deadlines. Section 11 allows the regulator to grant extensions on written request. Section 12 requires implementation and maintenance. [1, ss. 9-12]

A review cycle with explicit follow-through

Section 13 requires review to begin on prescribed dates or, by default, every anniversary of the program's establishment. The default completion period is 60 days, followed by notice within 30 days stating whether changes were made. Regulations may change those periods. Section 14 separately addresses notification of material ownership, control, supply-chain and third-party changes. [1, ss. 13-14]

Mitigation when a supplier risk is identified

Section 15 requires mitigation as soon as a supply-chain or third-party cyber risk is identified under the program. The enacted wording does not use a "reasonable steps" standard. Build a record connecting each risk to an owner, an action, a completion date and evidence that the action worked. [1, s. 15]

Records that demonstrate implementation

Section 30 covers program implementation, reported incidents, supplier-risk mitigation, cyber security directions and prescribed matters. Those records must be kept in Canada, at a prescribed location or, by default, the operator's place of business. The regulator determines the manner and retention period unless regulations prescribe otherwise. The section sets no universal number of retention years. [1, s. 30]

This is a requirement for specified records. It should not be presented as a blanket requirement to move every workload or all supplier data into Canada. Inventory where the relevant records are stored, who can retrieve them and how their integrity is protected.

Who makes the reporting call at 2 a.m.?

Section 17 sets a reporting period to be prescribed by regulation, capped at 72 hours, for reports to the Communications Security Establishment (CSE). The ceiling is not a confirmed 72-hour allowance. Reporting details, including the prescribed incident types, form and manner, require the applicable regulations. [1, ss. 17, 135(1)(c)]

Immediately after reporting, section 18 requires the operator to notify its regulator that the report was made and give the regulator a copy. Section 18.1 preserves the operation of PIPEDA, Canada's federal private-sector privacy law. A CCSPA workflow therefore needs to sit alongside other applicable reporting obligations. [1, ss. 18-18.1]

Rehearse the decision before the deadline is fixed

Name a reporting lead and an alternate with authority to act outside business hours. Give the incident commander, service owner, legal team and communications lead a shared escalation route. Set an internal response target that leaves time for assessment and submission once the regulatory clock is known.

Use a short exercise: a supplier reports possible compromise of remote access supporting a critical service. The technical scope is incomplete and the usual approver is unavailable. Test whether the alternate can convene the right people, establish what is known, record uncertainty and reach a documented reporting decision.

Capture detection and escalation times, the systems and services involved, known or potential impact, containment actions, the decision owner and the next update. Keep evidence of any submission and regulator follow-up. Treat these as preparation fields; they are not an official CCSPA reporting template.

Give suppliers enough time to help

Review contracts for notification triggers and timing, a continuously reachable contact, staged updates as facts develop, preservation of relevant logs, investigation support, subcontractor dependencies and access to evidence. Customer notification needs to leave the operator time to meet its own obligations.

For records needed under section 30, specify how the operator will obtain and keep the relevant evidence in Canada. Agree on scope, secure transfer and retention responsibilities with counsel. A generic promise to "comply with all laws" does not explain how a supplier will support an incident decision.

For suppliers: prepare a concise evidence pack showing the service provided, dependencies, incident contacts, recovery arrangements and available security evidence. Direct CCSPA duties depend on your own designation; customer contracts can create separate obligations. Avoid claiming CCSPA compliance before applicable requirements and scope are established.

Prepare now. Confirm the details later.

Use this page as a leadership working agenda. The actions below are recommended preparation, not additional statutory duties or a government implementation timetable.

Workstream	Prepare now	Confirm when applicable requirements are available
Scope and ownership	Name an executive sponsor. Map vital services to systems, data, IT/OT dependencies and suppliers. Record the rationale for candidate scope.	Designated class, corresponding regulator, commencement dates and final system scope.
Security program	Map existing policies and controls to risk management, protection, detection and impact reduction. Assign gaps and evidence owners.	Program content, submission manner and the actual start of the 90-day window.
Incident decisions	Name the reporting lead and alternate. Exercise after-hours escalation. Keep decision and evidence logs.	Reportable incident types, clock trigger, period, form, channel and regulator notification process.
Supplier terms	Identify critical dependencies. Review notification, cooperation, evidence access and subcontractor arrangements.	Any prescribed requirements and the customer-specific contract changes needed to support them.
Records and reviews	Inventory section 30 records and storage locations. Draft a review calendar and assign a records owner.	Required location, format, retention period, review dates and notification requirements.
Directions and change	Establish a route to receive, assess and implement a cyber security direction. Track material organizational and supplier changes.	Applicable directions, confidentiality restrictions and prescribed change-notification periods.

Build one evidence file people can actually use

Keep a controlled index linking the program to its system inventory, risk register, mitigation records, incident decisions, exercises, reviews and supplier evidence. Identify an owner and update date for each item. Restrict access appropriately and test that a second person can retrieve the records without the primary owner present.

Ask for a concrete leadership decision

Approve the accountable owner, the initial assessment scope and time for one reporting exercise. Request a short gap list with cost, dependency and service impact. Review it when a relevant order, regulation or regulator instruction changes the basis for the plan.

Accountability and sources

Who regulates, and what is at stake?

The Act names the Minister of Industry, Minister of Transport, Superintendent of Financial Institutions, Bank of Canada, Canada Energy Regulator and Canadian Nuclear Safety Commission as regulators. The applicable pairing of an operator class and regulator belongs in Schedule 2; sector familiarity alone is not confirmation of that assignment. [1, ss. 2, 7]

Section 91 caps administrative monetary penalties at \$500,000 for an individual and \$15 million in any other case, per violation. Section 92 provides a due diligence defence; section 94 makes a continuing violation a separate violation for each day. These amounts are ceilings for the regulatory scheme, not automatic fines. [1, ss. 90-94]

Separate criminal provisions also exist. For specified contraventions, section 137 permits court-determined fines and, for individuals, imprisonment of up to two years less a day on summary conviction or five years on indictment. Section 138 addresses participating directors and officers. Criminal offences and administrative violations have different rules; obtain legal advice on specific exposure. [1, ss. 136-141]

Source and status notes

Reviewed 12 October 2026. The Justice Laws consolidation states that it is current to 21 September 2026 and marks the CCSPA as not in force. The Gazette Part II indexes of 23 September and 7 October contain no CCSPA entries. This is a dated readiness brief: later instruments may change its application. [1, 4, 5]

1. **Critical Cyber Systems Protection Act.** Official text; definitions, schedules, program, reporting, records and enforcement provisions. [Justice Laws](#).
2. **S.C. 2026, c. 9.** Royal Assent and Telecommunications Act amendments; section 16 governs commencement of Part 2. [Annual statute](#).
3. **Public Safety Canada, 16 June 2026.** Government implementation statement distinguishing immediate telecommunications amendments from phased CCSPA implementation. [Royal Assent news release](#).
4. **Canada Gazette Part II, 23 September 2026.** [Volume 160, number 19 index](#).
5. **Canada Gazette Part II, 7 October 2026.** [Volume 160, number 20 index](#).

Turn the brief into a working plan

Map your critical cyber systems, decision owners and supplier terms. [Explore TrustCyber advisory](#).