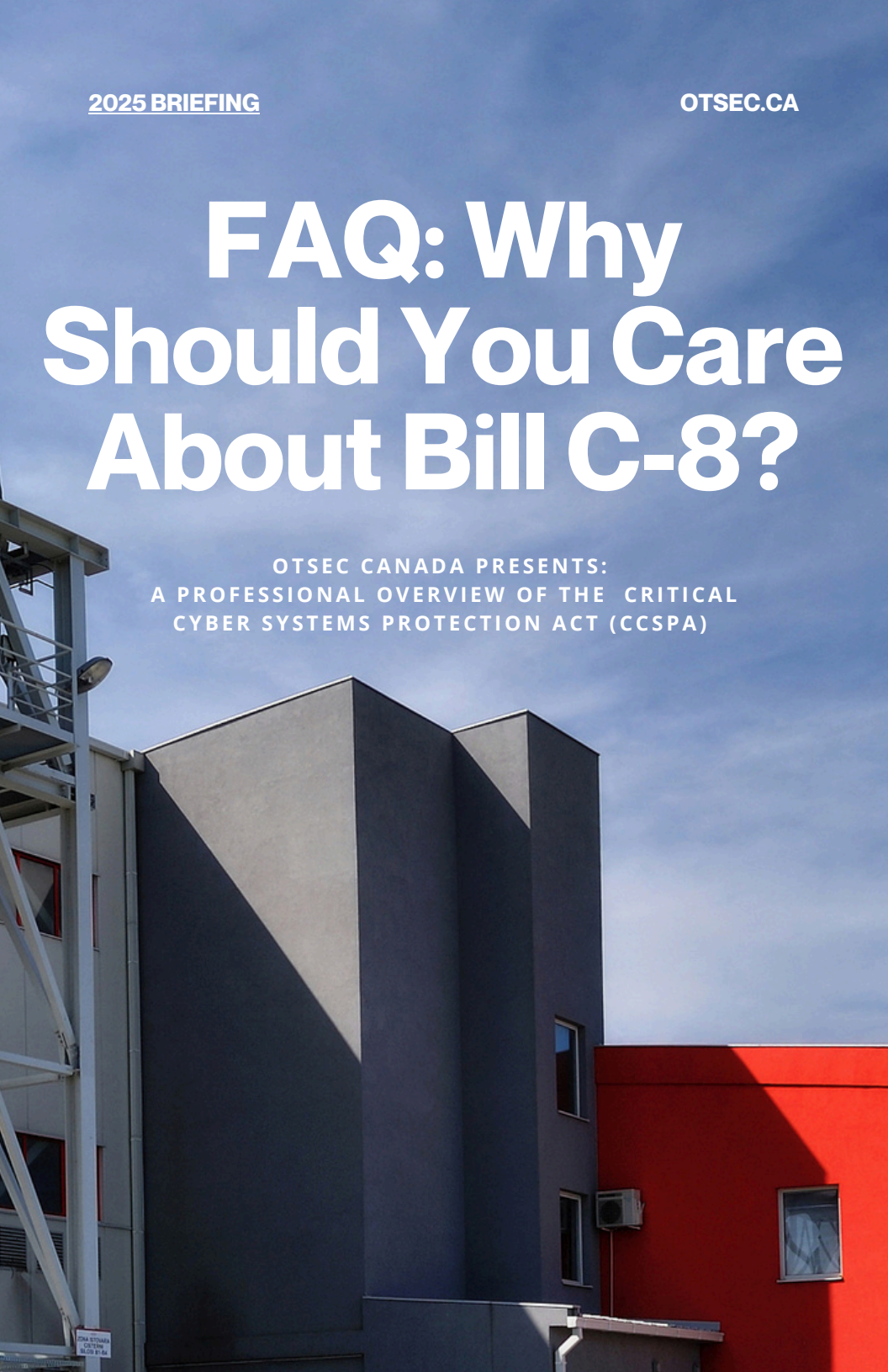
FAQ: Why Should You Care About Bill C-8?

OTSEC CANADA PRESENTS:
A PROFESSIONAL OVERVIEW OF THE CRITICAL CYBER SYSTEMS PROTECTION ACT (CCSPA)



FAQ

What Is Bill C-8 And Why Is It Important to large Canadian firms?

Bill C-8 is the reintroduction of the Critical Cyber Systems Protection Act (CCSPA). It establishes mandatory cybersecurity obligations for Canadian organizations that operate systems deemed critical to national security and public safety. If your organization operates within, or provides services to, the financial sector, telecommunications, energy infrastructure, or federally regulated transportation, this legislation will likely apply to you either directly or through contractual requirements.

Which Industry Sectors Are Affected?

The sectors specifically identified as “vital” under the Act include:

- Financial institutions, including banks and payment clearing systems
- Telecommunications providers and core service operators
- Energy infrastructure, including electrical utilities, pipelines, and nuclear facilities
- Transportation services regulated at the federal level, such as airlines, railways, and marine operators

How Is Bill C-8 Connected To Past Legislation?

Bill C-8 was introduced in Parliament on June 18, 2025. It revives the core obligations initially proposed under Bill C-26, which did not proceed in a previous session. The intent and sectoral focus of the legislation remain consistent with the earlier version.

Who Needs To Take Action?

Federally regulated operators in the designated sectors are directly responsible for compliance. However, any Canadian company that operates a “critical cyber system” supporting these entities should also consider itself in scope. This includes technology vendors, managed service providers, operational technology suppliers, and software developers.

What If My Company Is Not Directly Designated?

Even if your organization is not formally designated, you may still be required to comply with stringent cybersecurity standards if you are part of a critical operator’s supply chain. Requirements will be passed through contracts, especially where vendors have access to sensitive systems, data, or operational infrastructure.

FAQ

How Do These Requirements Affect Service Providers?

Service providers can expect contractual obligations that include:

- Providing recent and valid third-party security audit reports (such as SOC 2 or ISO 27001)
- Disclosing incident response processes and timelines
- Supplying Software Bills of Materials (SBOMs)
- Demonstrating secure software development practices
- Committing to defined Service Level Agreements (SLAs) related to cybersecurity

What Terminology Should Organizations Understand?

- MSP: Managed Service Provider
- SaaS: Software as a Service
- OT: Operational Technology, such as SCADA and industrial control systems
- SBOM: Software Bill of Materials, a list of all software components in a system

Can Other Organizations Be Designated In The Future?

Yes. The legislation allows the Governor in Council to expand the list of regulated entities or classes of operators by regulation. This means more organizations can be brought under the scope of the Act over time, depending on evolving national security priorities.

What Are The Core Compliance Obligations?

Designated operators must:

- Establish and maintain a formal cybersecurity program
- Assess and manage risks associated with third-party service providers
- Report cybersecurity incidents that affect critical systems to the Communications Security Establishment (CSE)

What Are The Reporting Timelines?

Incidents affecting the integrity, confidentiality, or availability of a critical cyber system must be reported within timelines to be set by regulation, with an upper limit of 72 hours. The timeline may be shorter depending on the nature of the incident.

FAQ

Can The Government Require Specific Actions?

Yes. The Act allows the federal government to issue targeted cybersecurity directives to one or more operators. These directions may include specific mitigation measures in response to emerging or imminent threats.

What Are The Legal Consequences of Non-Compliance?

Organizations that fail to comply with the obligations under the Act may be subject to administrative monetary penalties of up to 15 million Canadian dollars. Directors and officers may also face personal liability if found to have neglected their oversight responsibilities.

Are There Additional Requirements For Telecommunications Providers?

Yes. Bill C-8 also amends the Telecommunications Act to explicitly include cybersecurity as a policy objective. It grants the Minister new authorities to intervene when there are reasonable grounds to believe that national security is at risk.

How Will Financial Institutions And Payment Systems Be Affected?

These entities should prepare for more rigorous regulatory expectations around cybersecurity program design, incident response protocols, and oversight of third-party service providers. Reporting and accountability will also be more tightly defined.

What Should Energy Sector Operators Expect?

Operators of electrical grids, pipeline systems, and nuclear facilities will face enforceable standards set by their sector-specific regulators. These will include cybersecurity readiness, inspection authority, and mandatory compliance timelines.

What About Transportation Providers?

Federally regulated transportation services, including airlines, rail networks, and marine logistics operators, are classified as critical systems. These organizations will also be subject to the Act's core requirements.

FAQ

What Are The Implications For Vendors And Suppliers?

Companies that serve critical operators should expect:

- Mandatory third-party audit evidence (e.g., SOC 2 Type II, ISO 27001)
- Accelerated incident reporting requirements
- Disclosure of SBOMs for software systems
- Structured vulnerability management and patching SLAs

What Is The Most Effective Next Step?

Organizations should consider establishing or updating a public-facing Trust Center. This should include:

- Current and verifiable security certifications
- Clear articulation of cybersecurity practices
- Defined audit periods and scoping information
- Policies on data handling, supplier controls, and incident response

Having such a Trust Center improves transparency and readiness, and will likely become a procurement requirement for many contracts in the designated sectors.

How Can OTSEC Help?

We provide Bill C-8 Readiness Assessments, audit and risk advisory services, and supply chain cybersecurity strategies tailored for critical infrastructure.

Book Your Bill C-8 Preparedness Assessment Today

OTSEC will evaluate your current security posture, identify compliance gaps, and help your organization build a fully compliant cybersecurity program within the required timelines.

OTSEC

Contact

Otsec.ca
Otsecurity.ca