CPCSC Program Development Update

Canadian Program for Cyber Security Certification (PSPC)
Fall 2024

Joanne Lostracco
Director General, Washington Sector

Outline

1. **Context**
2. Partners
3. **Canadian Program for Cyber Security Certification (CPCSC) Objectives**
4. Program Elements
5. **Stakeholder Engagement**
6. High-level Implementation Timelines
7. **CPCSC Phase 1 Implementation**

Source: CPCSC, Fall 2024

Context

Evolving cyber threat environment

Canada's domestic defence supply chain is subject to increasingly frequent and sophisticated malicious cyber activity.

Launch of the U.S. Cybersecurity Maturity Model Certification (CMMC)

In 2021, the US Department of Defense (DoD) introduced CMMC 2.0, which will require all suppliers to the DoD who hold Federal Contract Information or Controlled Unclassified Information, including Canadian suppliers, to obtain a cyber security certification starting in summer 2025.

Highly integrated defence industrial base

49% of Canadian defence exports were destined to the U.S. representing CAD $3.1B worth of overall annual sales (2022).

Commitments to improving cyber security

Supports Canada's national Cyber Security Action Plan and the renewal of the National Cyber Security Strategy, along with Canada's Defence Policy: *Our North, Strong and Free*

Key Partners

Public Services and Procurement Canada is the **federal lead** for the CPCSC, providing horizontal coordination among eight Departments and one Crown Corporation, in addition to other roles and responsibilities within its existing mandate

Partners

- Treasury Board of Canada Secretariat
- Innovation, Science and Economic Development Canada
- Department of National Defence
- Communications Security Establishment
- Global Affairs Canada
- Public Safety
- Standards Council of Canada

Source: CPCSC, Fall 2024

CPCSC Objectives

Protect GC Data

Protect federal contractual information below the classified level on third-party, **non-federal systems**, networks and applications.

Maintain Industry Access

Ensure industry has access to domestic cyber security certification **recognized by the U.S.** and **internationally** to **bid and win international opportunities**.

Increase Cyber Resilience

Increase the cyber security baseline of Canadian industry, which in turn increases Canada's **national security** and **economic interests**, and **secures supply chains**

Maintain System Integrity

Maintain **supplier system integrity** for essential Canadian Armed Forces **capabilities** and **readiness**.

Grow the Canadian Cyber Security Industry

A domestic solution to cyber security certification will **increase Canadian industrial participation**, and be tailored to the Canadian context, accounting for our objectives of SME growth, and Indigenous procurement.

Source: CPCSC, Fall 2024

Government of Canada Information Marking

Protected

Applies to information or assets that, if compromised, could **reasonably be expected to cause injury** to a **non-national interest**—that is, an individual interest such as a person or an organization.

Protected A	Protected B	Protected C
Applies to information or assets that, if compromised, could **cause some injury** to an individual, organization or government.	Applies to information or assets that, if compromised, could **cause serious injury** to an individual, organization or government.	Applies to information or assets that, if compromised, could **cause extremely grave injury** to an individual, organization or government.

Classified

Applies to information or assets that, if compromised, could **reasonably be expected to cause injury** to the **national interest**, defence and maintenance of the social, political and economic stability of Canada.

Confidential	Secret	Top Secret
Applies to information or assets that, if compromised, could **cause injury** to the national interest.	Applies to information or assets that, if compromised, could **cause serious injury** to the national interest.	Applies to information or assets that, if compromised, could **cause exceptionally grave injury** to the national interest.

Controlled Goods

Controlled goods are primarily goods, including components and technical data that have military or national security significance, which are controlled domestically by the Government of Canada and defined in the *Defence Production Act*.

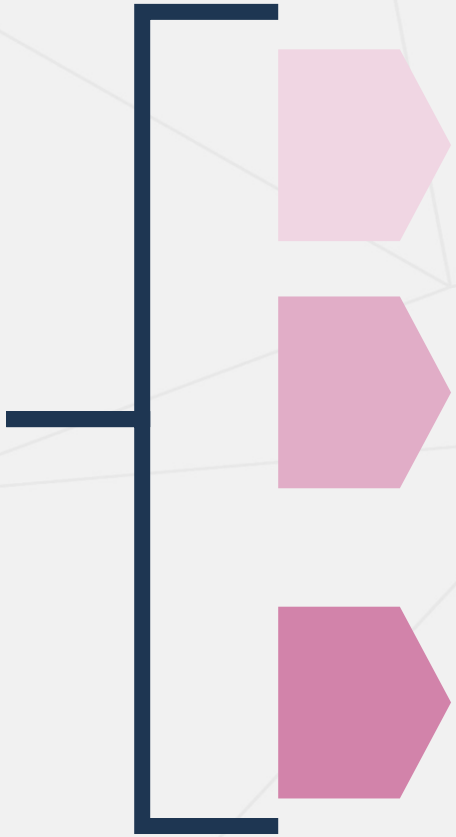
Source: CPCSC, Fall 2024

Reciprocity with US CMMC Program

Reciprocity with CMMC

Canada's program seeks to leverage the U.S. Government's **CMMC program** and **the Canada-U.S. bilateral security instrument**.

Canada is seeking U.S. recognition of the CPCSC to achieve **reciprocity.**



CPCSC and CMMC will be based on **similar standard** and **controls**.

Reduces burden by allowing a company to achieve certification in one country's program, **recognized** and **accepted** by the other.

Government of Canada will continue to leverage its **bilateral security instruments** with foreign partners to ensure **our domestic cyber security program** is **aligned** and **collaborative**.

Source: CPCSC, Fall 2024

CPCSC Certification Levels

CPCSC Certification levels will **mirror** CMMC's three levels.

The required certification level for each RFP will be determined through a Department of National Defence-led **Risk Profile.**

CPCSC Level 3	**Risk Profile**: Expert **Approach**: External Assessment **Responsible**: Department of Defence **Re-Assessment**: Triennial **Prerequisite**: Level 2 certification
CPCSC Level 2	**Risk Profile**: Advanced **Approach**: External Assessment **Responsible**: SCC-Accredited Third-Party Assessor **Re-Assessment**: Triennial **Prerequisite**: Level 1 self-assessment
CPCSC Level 1	**Risk Profile**: Foundational **Approach**: Self-Assessment **Responsible**: Supplier **Re-Assessment**: Annually **Prerequisite**: N/A

Source: CPCSC, Fall 2024

Canadian Industrial Cyber Security Standard - Development

The Canadian Centre for Cyber Security's Security Architecture (SA) team are working closely with the National Institute of Standards and Technology (NIST) on the development of **the Canadian Industrial Cyber Security Standard**

Canadianizing NIST SP 800-171 Rev3

Contextualizing each requirement with **Canadian sourcing**, **publications**, and **official language compliance**

Technically identical standard

Announcement:
Fall 2024

Canadianizing NIST SP 800-172

NIST is **reviewing** the **list of control requirements** to ensure its effectiveness

Technically identical standard once NIST finalizes SP 800-172 new controls in 2025

Announcement:
More details to follow

Source: CPCSC, Fall 2024

Canadian Industrial Cyber Security Standard - Development

The Canadian Centre for Cyber Security's Security Architecture (SA) team are working closely with the National Institute of Standards and Technology (NIST) on the development of **the Canadian Industrial Cyber Security Standard (ITSP.10.171)**

User identification, authentication, and re-authentication	**Canadianized** User identification, authentication, and re-authentication
Requirement Number 03.05.01 *a. Uniquely identify and authenticate system users and associate that unique identification with processes acting on behalf of those users.* *b. Re-authenticate users when [Assignment: organization defined circumstances or situations requiring re-authentication].*	Requirement Number 03.05.01 *a. Uniquely identify and authenticate system users and associate that unique identification with processes acting on behalf of those users.* *b. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].*
Source Controls: IA-02, IA-11	Source Controls: IA-02, IA-11
Supporting Publications: SP 800-63-3 [27]	**Supporting Publications:** Cyber Centre User Authentication Guidance for Information Technology Systems (ITSP.30.031)

Source: CPCSC, Fall 2024

CPCSC Contract Cyber Risk Assessment Criteria

Risk Assessment Criteria

DND is finalizing **risk assessment criteria** alongside partners.

Phasing in of requirements based on scoping criteria.

Risk Profile

A **Risk Profile** will determine the certification level. DND and partners are currently considering **sensitivity of information** & **criticality of goods** and **services.**

For sensitivity, currently analysing **potential mappings of CUI types** to **Protected markings** and **Controlled Goods.**

Flow Down

Requirements will flow down to suppliers via **contract clauses** and **SOW statements**.

Primes will be **responsible** for the **flow down** and **compliance** of its supply chain.

Source: CPCSC, Fall 2024

Accreditation Ecosystem

The **Standards Council of Canada** (SCC) is supporting this new Canadian program by aligning with the United States' **Cybersecurity Maturity Model Certification (CMMC)** program.

SCC Overview

Level 2 **conformance** will be **assessed** by **accredited 3PAOs**.

SCC will **accredit** these **3PAOs**.

To become a **3PAO**, an organization must be **accredited** to **ISO/IEC 17020**.

SCC Updates

The program is **under development**, aligning with CMMC.

You can **begin your journey** to **becoming** an **accredited 3PAO today**.

Interest in the **program** is **being tracked** to **share updates**.

Let us know if you are interested so we can ensure you're signed up for updates.

Source: CPCSC, Fall 2024

Canadian Centre for Cyber Security (CCCS)

The Canadian Centre for Cyber Security's (CCCS) **Defence Industrial Base (DIB) Partnerships** team connects the DIB sector with free CCCS tools, services, and advice and guidance..

- Serves the Government of Canada, Canadian critical infrastructure sectors, the private sector, and academia.
- Has access to **unique foreign intelligence** that enables us to **stay ahead** of **emerging threats**.
- Provides **advice** and **guidance** to help small and large organizations become more **cyber resilient**.
- **Connect** with DIB Partnerships team to **onboard** to CCCS **services**: dib-par-bid@cyber.gc.ca

CCCS CPCSC Resources

The CPCSC Preparatory Self-Assessment Tool

Working with Public Safety Canada to **modify** the existing **Canadian Cyber Security Tool** (CCST 2.0) to self-assess against **the Canadian Industrial Cyber Security Standard.**

DIB partners can map their assessment results to a **System Security Plan (SSP),** using the available template**.** Partners can use the template to develop an SSP to address gaps or vulnerabilities.

Publications for CPCSC Readiness

The DIB Partnerships team is working with adjacent CCCS teams such as the Cyber Security Guidance team, **develop advice** and **guidance** for **CPCSC readiness**.

Currently plans are being made for the following publications:

1. **System Security Plan Template**
2. **CPCSC Readiness Checklist**

Source: CPCSC, Fall 2024

CPCSC Request for Information – Insights

In May 2024, PSPC Washington launched a comprehensive **Request for Information** to assess the **readiness**, **perspectives**, and **needs** of key stakeholders in relation to the **Canadian Program for Cyber Security Certification** (CPCSC) and the US **Cybersecurity Maturity Model Certification** (CMMC).

57% of **prime contractors** prefer **CPCSC certification if fully reciprocal** with **CMMC**.

50% of **prime contractors** foresee **difficulty flowing down CPCSC requirements** to their subcontractors.

58% of IT consultants are interested in becoming **accredited CMMC/CPCSC assessors**.

Subcontractors reported **lower cyber maturity** compared to prime contractors and consultants, **concerns** about the **cost** and **complexity** of compliance, particularly for smaller entities.

IT Consultants and **Service Providers** expressed a need for **clearer guidance** on **CPCSC applicability** to **cloud services**, **managed security offerings**, with a strong desire to **align CPCSC** with **existing security standards** (SOC 2, ISO 27001, ITSG-33).

Source: CPCSC, Fall 2024

High-level Implementation Timelines

Ongoing stakeholder engagement

Spring/Summer 2024

- Collaboratively **develop** and **design** the CPCSC.
- Release **Request for Information** for program development.
- **Enter into** discussions with the U.S. Government.
- Develop the **Contract Cyber Risk Assessment Criteria** for phased roll out and certification level identification.

Fall 2024

- Establish the **Canadian Cyber Security Standard for federal contracting**.
- **Pilot** CPCSC implementation and process flow.
- **Accredit** third-party assessment bodies.

Winter/Spring 2025

- **Iterative launch** the CPCSC.
- Introduce mandatory cyber security certification requirements in **select defence Requests for Proposals**.
- Finalize the **Canadian Cyber Security Standard for federal contracting**.

Source: CPCSC, Fall 2024

CPCSC First Phase Implementation Strategy

CPCSC will begin with the **First Phase** of implementation in early 2025, focusing on:

January 2025

The Government of Canada will introduce CPCSC through a Soft Launch in January 2025.

CPCSC Level 1

CPCSC Soft Launch will focus on the 12 Level 1 controls referenced in ITSP.10.171 Standard.

Contract Selection

Department of National Defense will leverage the CPCSC Contract Cyber Risk Assessment Criteria to identify the initial contracts with CPCSC Level 1.

Accreditation Ecosystem

The Standards Council of Canada will focus on building out the capacity of the Third-Party Conformity Assessment ecosystem for Level 2 Certifications.

An **iterative** and collaborative launch of CPCSC to **build stakeholder trust** through **feedback loops**, **test key program elements**, onboard **users**, and **identify key risks** for full implementation.

Source: CPCSC, Fall 2024

CPCSC First Phase: Level 1 Controls

ITSP.10.171 (NIST SP 800-171 Rev. 3)

03.01.01 ***Account Management***	**03.01.02** ***Access Enforcement***	**03.01.20** ***Use of external systems***	**03.01.22** ***Publicly accessible content***	**03.05.01** ***User identification, authentication, and re-authentication***	**03.05.02** ***Device Identification and authentication***
03.08.03 ***Media Sanitization***	**03.10.01** ***Physical Access Authorizations***	**03.10.07** ***Physical Access Control***	**03.13.01** ***Boundary Protection***	**03.14.01** ***Flaw Remediation***	**03.14.02** ***Malicious Code Protection***

Source: CPCSC, Fall 2024

Contact us!

Canadian Program for Cyber Security Certification
CPCSC Secretariat

TPSGC.PACertcybersecur-APCyberSecurCert.PWGSC@tpsgc-pwgsc.gc.ca

Cyber security certification for defence suppliers in Canada – Canada.ca (tpsgc-pwgsc.gc.ca)