TRIPLE HELIX

The Impact of Canada's Cybersecurity Certification Program on Defence and Canadian Industry

by Vice-Admiral (retired) Ron Lloyd

December 2025

POLICY PERSPECTIVE

THE IMPACT OF CANADA'S CYBERSECURITY CERTIFICATION PROGRAM ON DEFENCE AND CANADIAN INDUSTRY

by Vice-Admiral (retired) Ron Lloyd

December 2025

Prepared for Triple Helix
Suite 200, 8 York Street, Ottawa, ON K1N 5S6 Canada
www.cgai.ca/triple_helix

Defence procurement in Canada is poised to encounter additional delays with the introduction of a new "small p" policy: the Canadian Program for Cyber Security Certification (CPCSC). While the technical underpinnings of CPCSC closely mirror those of the U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC), the federal government is pursuing a distinctly Canadian implementation approach that reflects the overclassification and risk aversion embedded within the broader non-legislated "small p" policy framework put in place by the public service.

For those unfamiliar with the intricacies of defence procurement, it is important to recognize that the CPCSC is not emerging in isolation. It will sit alongside three existing security frameworks, the Contract Security Program (CSP), the Controlled Goods Program (CGP), and the Canadian Centre for Cyber Security Cloud Assessment Program, which already impose significant compliance demands on industry. The CGP, much like the CPCSC, was born out of a U.S. initiative and was subsequently layered with additional requirements for Canadian industry, resulting in procurement delays and disproportionate impacts on small and medium-sized enterprises (SMEs). Likewise, there is clear evidence that Canada's approach to contract security is excessively risk-averse compared to our allies and partners, leading to procurement bottlenecks and imposing billions of dollars in extra costs on government and industry. The introduction of the CPCSC threatens to add hundreds of millions more in costs for Canadian businesses, particularly SMEs, while compounding procurement delays.

This article examines the genesis of CPCSC, contrasts Canada's approach with the U.S. model, and outlines how these differences could harm both Canadian Defence and Canada's Defence Industrial Base (DIB). It concludes with practical, actionable recommendations to ensure the program strengthens, rather than hinders, Canada's defence and economic objectives

Understanding the CMMC Model

For over a decade, the United States has strengthened its cybersecurity stance to protect Controlled Unclassified Information (CUI) within government and the defence sector. With foreign actors like China persistently targeting U.S. intellectual property, the need for robust supply chain security became clear. After years of consultation and iteration, the Pentagon began implementation of CMMC 2.0 phase one in November 2025. Two further phases will follow in 2026 and 2027, with full implementation slated for November 2028.

CMMC 2.0 sets out three tiers of IT security:

- Level 1 covers basic cyber hygiene. Companies self-attest to 15 straightforward requirements to protect Federal Contract Information (FCI). Of the U.S. defence suppliers, roughly 140,000 (63%) of the DIB are expected to require Level 1, with self-assessments underway since November 2025.

- Level 2 is more rigorous. Depending on the sensitivity of CUI, it may require either a self-assessment or an audit by a Certified Third-Party Assessor Organization (C3PAO). For most types of CUI—such as financial, privacy, or procurement data (Protected B in Canada)—a self-assessment will suffice for approximately 4000 entities (2%). For controlled technical data and other high-risk categories (not codified in Canada), third-party certification is mandated. About 77,000 firms (35%) will fall under Level 2, with self-assessments starting in phase one and C3PAO audits beginning November 2026.

- Level 3 is the strictest, aimed at mission-critical and unique technologies. Certification is handled by the Defense Contract Management Agency's Cybersecurity Assessment Centre. Only about 1% of companies (1,500) are expected to need Level 3 clearance, with implementation targeted for November 2027.

The Canadian Approach: Same Standards, Different Application, New Term

The technical standards underpinning the CMMC are presently anchored in NIST 800-171 revision 2, with a planned migration to revision 3. In the Canadian context, the CPCSC technical standards, set out in ITSP.10.171 by the Canadian Centre for Cyber Security (CCCS), are, for all intents and purposes, aligned with NIST 800-171 revision 3. Where things truly diverge, however, is not in the technical details but in governance and execution. Rather than being led by Defence, oversight for this program falls to Public Services and Procurement Canada (PSPC). The Canadian Security Establishment (CSE) and its cyber arm, CCCS, play a supporting role, while National Defence's direct involvement is largely limited to Level 3 of the framework. Canada also introduces a new term called "Specific Information" as a replacement for Controlled Unclassified Information (CUI). This new term will create even more confusion in an already complicated security classification framework that is out of step with Canada's allies and partners.

More importantly, Canada has opted for a more prescriptive and expansive application model:

- Level 1: Mandated for all procurements handling Low Sensitivity Specified Information – Protected A information and dual-use technical data. Since almost every government contract involves Protected A (e.g., basic address information), every Canadian supplier—across all industries—will eventually face Level 1 self-assessment.

- Level 2: In Canada, self-assessment is off the table. All companies dealing with Moderate Specified Information –Protected B (privacy and financial data), mission or safety-critical technical data, or controlled goods technical data must undergo third-party assessment. Given that nearly all federal procurements involve Protected B, Level 2 will impact almost all Canadian businesses. Implementation is set to begin in some contracts in January 2027.

- Level 3: Overseen by National Defence, Level 3 will apply to High Specified Information including technical data for satellite communications, C4ISR systems, weapon systems,

and encrypted communications. The examples of High Sensitive data are so expansive that most defence contracts would require Level 3, far exceeding the 1% threshold in the U.S. Full rollout is planned for 2027, a year sooner than the American equivalent.

Unintended Consequences for Canadian Industry

Ironically, one of the original hopes for CPCSC was that the U.S. would recognize it as equivalent to CMMC, letting Canadian companies sell seamlessly into the American market. That recognition is not forthcoming, and with global security tensions rising, it appears unlikely in the short term. It is assessed that absent recognized equivalency, Canadian industry would be at a competitive disadvantage having to adhere to two separate regimes.

The U.S. is already grappling with a shortage of qualified C3PAOs (CMMC Third-Party Assessor Organizations). By eliminating self-assessment for Level 2 and broadly applying Level 2 and Level 3, Canada risks making certification even costlier and more challenging. The expanded scope will create a bottleneck having to certify the cadre of C3PAOs and then certifying the artificially elevated number of suppliers by C3PAOs and Defence.

Large Original Equipment Manufacturers (OEMs) may absorb these costs and delays, but smaller Canadian businesses—already under pressure—will be disproportionately impacted, running counter to efforts to bolster these firms in our domestic defence sector in Budget 2025.

What Could Ottawa Do?

Over the past several years, the geostrategic environment has shifted with a speed and severity few could have anticipated when the Government of Canada first signalled its intent to pursue a national cyber security certification program. Today, our security, economic, and technological landscapes are marked by unprecedented uncertainty as Canada postures itself to these new realities. In this environment, strengthening the resilience of Canada's DIB is a strategic imperative.

There is no debate that Canada needs to ensure the cybersecurity of its supply chains, and as such, the U.S. CMMC provides a potential option. But it is by no means the only credible pathway forward. Our Five Eyes partners, particularly the U.K. and Australia, have adopted risk-based approaches that achieve strong security outcomes while avoiding the heavy administrative and financial burden associated with more prescriptive regimes. Their models, both of which were updated in 2024, reinforce an important lesson: effective security does not need to come at the expense of industrial competitiveness.

When the government embarked on this initiative, the intent was to pursue mutual recognition with the United States. If that outcome is no longer achievable, and even if it were, we need to ask a fundamental question: Does it make sense to rigidly adhere to a 2023 helm order that risks

placing Canadian industry at a structural disadvantage at the very moment when the government is working hard to strengthen the Canada's DIB and expand trade with our NATO and Five Eyes partners in initiatives such as Canada's participation in Security Action for Europe (SAFE)?

The answer, in my view, is clear. Canada must ensure its cyber security regime enhances, not inhibits, our strategic economic objectives. To that end, the following recommendations are offered for consideration:

1. Delay Implementation: Revisit the decision to adopt CMMC as the model for CPCSC. Conduct an options analysis comparing CMMC to other less prescriptive models, such as the U.K. and Australia, that are more in keeping with Canada's overall strategic priorities and realities.

2. Align the level of injury associated with personal information with our allies and adopt a security classification framework of Official (Sensitive), Secret and Top Secret. In the new framework, refine the categories of official and official (sensitive) information to avoid the use of another confusing term such as "specified information."

3. If the decision is to adopt a new risk-based model for CPCSC, recognize CMMC equivalency for those Canadian companies that require and have been granted CMMC accreditation.

4. If the decision is made to continue with CMMC as the template for CPCSC:

    a. Given the complexities Canada faces, and the fact that Canadian companies will still require certification under CMMC, there's little reason to move faster than our largest ally. Ottawa should phase in CPCSC at least six months to a year after the U.S., learning from their rollout.

    b. Target Level 1 More Precisely: Limit Level 1 to companies handling Federal Contract Information, aligning with the U.S. definition.

    c. Reintroduce Self-Assessment for Level 2: Allow companies to determine whether it is more cost effective to pursue self-assessment for lower-risk data and require third-party audits only for the most sensitive information—such as controlled technical data and privileged safety information.

    d. Restrict Level 3: Make Level 3 certification a requirement only upon project manager recommendation within the guardrails articulated in CMMC 2.0 and subject to independent departmental review. Use the 1% benchmark to prevent scope creep and report annually.

    e. Assess and disclose costs: The price tag for compliance will be significant, especially for SMEs. Government should collect and publish data on these costs, with industry input, to gauge the real impact and provide insight for continuous improvement.

Among cybersecurity practitioners in the defence sector, there is a growing concern that the current trajectory of CPCSC may be "destined for failure" if pursued without careful calibration. In that context, as Canada seeks to expand defence investment and strengthen our domestic supply chain, introducing another costly, prescriptive regime, no matter how well intentioned, without fully evaluating its operational and economic consequences could be counterproductive.

It is assessed that the government would benefit from exercising strategic patience and reconsidering the adoption of CMMC as the template for CPCSC. Considering recent Defence Policy announcements, there is a unique opportunity to take a holistic approach, to modernize CPCSC and the CSP, CGP and CCCS Cloud Assessment Program to ensure they are aligned with the government's priorities and that there is coherence across all the regulatory and security frameworks.

This deliberate alignment is essential to ensure that Canadian industry, particularly our small and medium enterprises, are positioned to seize what is truly a once in a generation opportunity to grow, compete, and contribute to defence at home and to allies and partners abroad in a rapidly evolving geostrategic and technological environment.

About the Author

A native of Taber, Alberta, ***Vice-Admiral (Ret'd) Ron Lloyd*** *was the 35th Commander of the Royal Canadian Navy from 2016-2019. During that time, he was also "double hatted" as the acting Vice Chief of the Defence Staff for almost half a year and as the first Chief Data Officer for the Department of National Defence and Canadian Armed Forces for a full year.*

During his 38-year career in the RCN, he was privileged to have commanded HMCS CHARLOTTETOWN, HMCS ALGONQUIN, the PACIFIC Fleet and the ATLANTIC fleet. He has extensive operational experience having deployed on numerous occasions globally.

Lloyd has over a decade of experience at National Defence Headquarters having also served as the Deputy Commander of the RCN, the Chief of Force Development for the Canadian Armed Forces, the Director General of Force Development for the RCN and Executive Assistant to the Commander of the RCN.

Lloyd holds a Bachelor of Arts in Military and Strategic Studies from Royal Roads Military College (1985) and a Master of Arts in War Studies from the Royal Military College (2004). He is a graduate of both the Command and Staff Course and the National Security Studies Course at the Canadian Forces College in Toronto. He has also attended the HARVARD Kennedy School, Executive Education, Senior Executives in National and International Security.

Today, as Principal of Leadmark Ventures, he shares his experience in leadership, strategic planning and digital transformation with organizations committed to providing innovative solutions that enhance public sector performance in defence and non- defence related activities.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.