CPCSC Readiness

Strengthening Canada's Defence Supply Chain

DEFSEC Halifax Roundtable
Key Findings

October 7, 2026 | Prepared by ADGA Group

ADGA

adga.ca

Purpose and scope

This sumarry refelects perspectives shared during a single industry roundtable. Convened by ADGA Group and Plurilock in consultation with Regional Development Agencies ACOA, FedDev Ontario, and FedNor, the roundtable explored practical challenges in preparing for the Canadian Program for Cyber Security Certification (CPCSC), with particular attention to the transition from readiness activities to certification. It brought together perspectives from defence manufacturing, automation, AI and software, and cyber security advisory and service delivery. Discussion covered existing suppliers, companies exploring defence opportunities, and organizations supporting supplier readiness.

Executive summary

For smaller firms pursuing defence work, roundtable participants highlighted a difficult decision: how much to invest in cyber security readiness before knowing whether they'll win a contract. Some established suppliers are already investing in infrastructure and documentation as they prepare for both CPCSC and U.S. CMMC requirements. Smaller firms may have fewer people available to do that work and less certainty about when the investment will pay off.

Participants described certification readiness as an organization-wide change effort. Technical controls alone are insufficient without documented processes, management support, staff training, and changes to everyday business practices. Preparation also requires sustained funding and access to experienced personnel; certification was viewed as an ongoing responsibility rather than a one-time milestone.

The discussion highlighted opportunities for clearer implementation guidance and practical for suppliers. AI use and cloud data handling emerged as related operational concerns requiring clearer guidance.

Principal signals

Customer requirements are a strong trigger for investment; shifting anticipated timelines can weaken momentum.

Smaller firms face a difficult investment decision when future defence revenue is uncertain.

Documentation, business process changes, and skilled personnel can be as demanding as technology upgrades.

AI and cloud services create practical questions about information handling, control enforcement, and productivity.



Key findings from the discussion

1. Readiness varies, and customer signals matter

An established supplier described starting preparation several years ago, slowing its effort as anticipated deadlines shifted, and accelerating again following renewed customer direction. Other participants described growing demand for readiness proposals. Companies with multiple entities or locations face additional coordination and scoping complexity.

2. Time, money, and uncertain returns constrain smaller firms

Service providers described smaller businesses without dedicated cyber security expertise or mature IT support. The prospective move to Level 2 was seen as particularly demanding. Firms seeking their first defence contract face a difficult balance: investing in readiness before knowing whether or when that investment will generate revenue. Participants emphasized assessing the full business commitment early.

3. Implementation requires changes across the organization

One supplier reported that progress improved when managers reconsidered how work was performed, rather than asking IT to fit existing practices into the required controls. Another organization described documentation and auditability as its main gap despite having technical capabilities in place. Participants also noted demands on support functions, including HR.

4. Skilled personnel and certification capacity are concerns

Participants reported difficulty finding experienced staff and organizations able to support assessment and certification for CPCSC and CMMC. They contrasted this with greater availability of expertise for established ISO programs. Hiring, training, and collaboration among providers were discussed as ways to build capacity; this did not establish the size of any national capacity shortfall.

5. AI and cloud services complicate information handling

Participants raised concerns about staff use of unapproved AI tools, the location and handling of data, cloud service dependencies, and enforcing policies in practice. Secure enclaves were discussed as one approach to separating sensitive work from routine operations, alongside challenges involving onboarding, productivity, and maintaining boundaries. These were operational concerns raised in discussion, rather than verified statements of CPCSC requirements.

6. Readiness needs sustained investment and collaboration

Participants expected security responsibilities to continue evolving after certification and emphasized ongoing staffing and funding. They also identified collaboration among suppliers and service providers as a practical strength, including sharing expertise and accessing additional capacity when internal resources are limited.

Opportunities for further guidance and collaboration

The discussion suggests the following opportunities for further guidance and collaboration among government, suppliers, and service providers. These are proposed areas for consideration, rather than formally agreed roundtable resolutions.

Predictable implementation information

Suppliers would benefit from accessible guidance on implementation milestones, applicability, and expectations at each stage, with confirmed requirements distinguished from anticipated changes to support investment planning.

Practical readiness resources

Practical resources could help firms assess scope, internal responsibilities, documentation needs, and demands on people and infrastructure. Examples suited to smaller firms, new defence entrants, and organizations with multiple entities or locations would be particularly useful.

Clarity on related requirements

Suppliers would benefit from clarity on how CPCSC preparation relates to CMMC, existing cyber security certifications, and other defence security processes, including where work may be reusable and where separate requirements apply.

A clear assessment and certification pathway

Clear information on the roles of readiness providers, assessors, and certification bodies could help suppliers identify appropriate qualified organizations. Further engagement could help clarify demand, workforce constraints, and potential scheduling bottlenecks. See PSPC's CPCSC Program Overview.

Practical AI and cloud guidance

Examples and authoritative references could help suppliers address sensitive information handling in AI and cloud services, including policy enforcement, service dependencies, and scoping, while distinguishing CPCSC obligations from wider governance considerations.

Access to support and continued engagement

Government and industry partners could help connect firms with existing readiness and workforce development support. A focused follow-up with SMEs could test whether guidance addresses the investment and implementation barriers described.

Questions for further clarification

- What can suppliers do now to prepare for CPCSC, and which investments depend on knowing what a specific contract will require?
- How can firms preparing for CMMC understand which activities are relevant to CPCSC and which require additional work?
- What visibility can suppliers receive on qualified assessment and certification capacity?
- Which existing support mechanisms can help smaller firms manage readiness costs and develop internal capability?

CPCSC Readiness

Roundtable findings and opportunities for continued guidance and collaboration.

Prepared by ADGA Group | DEFSEC Halifax | October 2026

Contact us

+1-613-237-3022
adga.ca

© ADGA 2026.