

Understanding CPcsc Level 1 and What It Means for Defense Contractors in Canada

If you work with the Canadian government on defense or security contracts, you have likely heard about the Program for Cyber Security Certification. It is a framework that aims to protect sensitive information and systems across the supply chain. The program introduces a set of clearance levels, and for many organizations the first step is understanding what cpcsc level 1 actually requires. It is not just another compliance checkbox. It is a baseline that shapes how you handle IT security, controlled goods, and overall contract security from the start.

I have spent years helping companies navigate industrial security requirements in Canada. One thing I have learned is that the earlier you align your internal processes with the cybersecurity certification program, the smoother your contract work becomes. Level 1 is designed for organizations that handle controlled goods or sensitive information but do not necessarily need the higher clearance levels. It sets a foundation for your company security program and forces you to think about security controls in a structured way.

What Is the Program for Cyber Security Certification?

Public Services and Procurement Canada oversees the Program for Cyber Security Certification. It is a response to growing threats against national security and the need for a consistent cybersecurity framework across defense contractors. The program covers everything from physical security of facilities to IT security of networks and data. It applies to any organization that bids on or fulfills contracts involving controlled goods, classified information, or assets that affect national security.

The certification has multiple levels, each building on the previous one. [cpcsc level 1](#) is the entry point. It focuses on basic security practices that every organization should have in place. The goal is to ensure that even the smallest subcontractor in the supply chain has a baseline of protection. Without it, a weak link could compromise the entire contract. That is why the Canadian government has made it a requirement for many defense contracts.

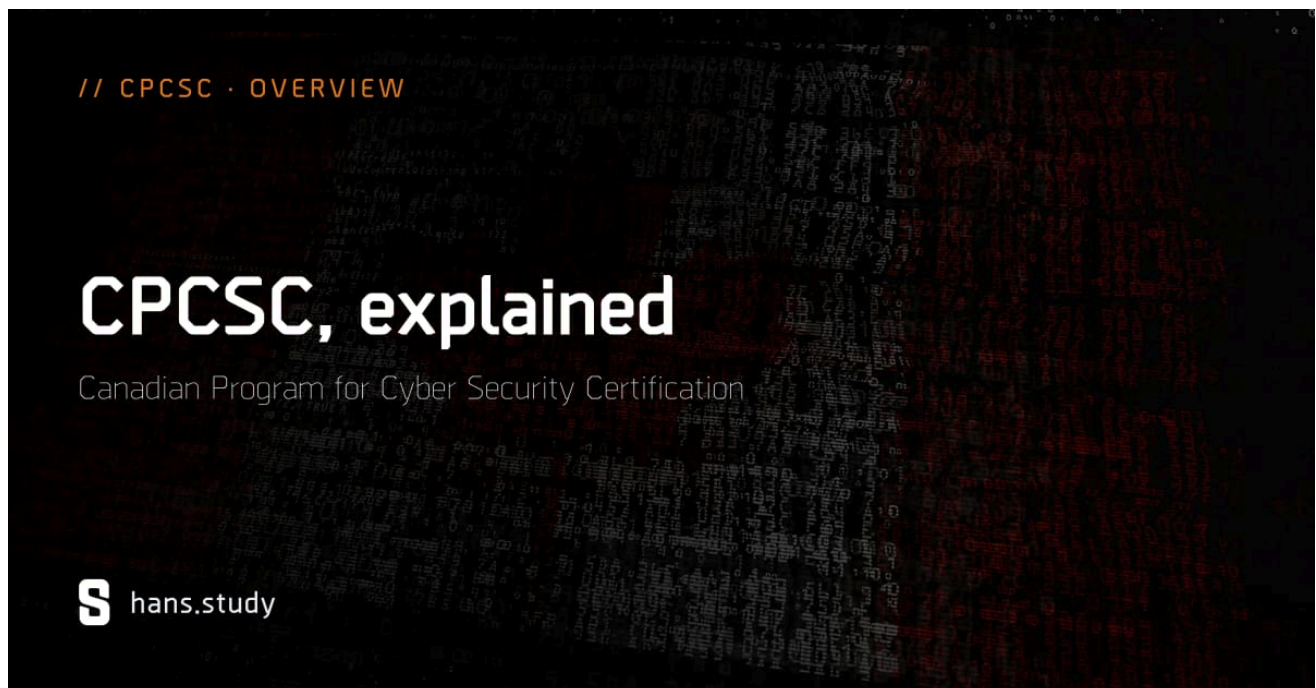
Who Needs cpcsc Level 1 Certification?

If your company handles controlled goods or provides services that support defense or security programs, you likely need this certification. It applies to prime contractors and subcontractors alike. The requirement often appears in the contract security clauses of solicitations from Public Services and Procurement Canada. Even if you only touch a small piece of a larger project, the government wants to know that your company security program meets the minimum standard.

From my experience, many small and medium-sized businesses underestimate the scope of the requirement. They think because they do not handle top-secret information, they can skip certification. But controlled goods cover a wide range of items, from technical data to physical components. If your work touches any of those, you need to start the security assessment process. Level 1 is manageable, but it does require deliberate effort.

Key Requirements of cpcsc Level 1

The requirements for level 1 are not overly complex, but they demand attention to detail. Here is what you need to have in place:



- A documented company security program that outlines policies and procedures for protecting controlled goods and sensitive information.
- Basic security controls for your facilities, including access control and visitor management.
- IT security measures such as firewalls, antivirus software, and patch management for systems that handle contract data.
- Training for employees on security awareness and their responsibilities under the contract.
- A process for reporting security incidents to the appropriate authorities.

These requirements are the foundation. They show that you have thought about security and have taken practical steps. The certification process involves a third-party assessment or a

self-declaration, depending on the contract. In either case, you need to demonstrate that your controls are in place and working.

How the Certification Process Works

The process starts with a security assessment of your organization. You submit your company security program and evidence of your security controls to the designated authority. For many contracts, that authority is Public Services and Procurement Canada or the department overseeing the program. They review your submission and may conduct a site visit to verify your claims.

One common mistake I see is companies treating the assessment as a one-time event. But cybersecurity certification is not a static badge. It requires ongoing maintenance. Your security controls must stay current, your employees need refresher training, and your IT security measures must adapt to new threats. The Canadian government expects certified organizations to maintain their level of security throughout the life of the contract.

The assessment itself is not meant to be punitive. It is a chance to identify gaps and improve your posture. Many organizations find that the process helps them tighten up practices they had overlooked, such as how they store controlled goods or manage subcontractor access. That is a benefit that extends beyond the contract.

Common Challenges and How to Address Them

One challenge I see frequently is confusion about what counts as a controlled good. The definition is broad and can include technical drawings, software, and even certain types of equipment. If you are unsure, it is better to err on the side of caution and seek guidance from your contracting officer or a security specialist. Another challenge is aligning your existing IT security with the framework. Many companies have basic protections, but they are not documented or tied to a formal company security program. The certification requires that you formalize what you already do.

Budget is another concern. Small businesses worry about the cost of implementing security controls and going through a third-party assessment. But the investment is often smaller than expected. Basic controls like access logs and encryption are not expensive. And the cost of non-compliance can be much higher, including losing the contract or facing legal penalties.

I also see companies struggle with the timeline. The certification process can take several weeks or months, depending on your readiness. Do not wait until the contract is awarded to start. Begin your internal security assessment early. That way, when the requirement appears in the solicitation, you are ready to respond.

Integrating Level 1 into Your Company Security Program

Your company security program is the backbone of your certification. It should be a living document that describes your policies for protecting controlled goods, managing access, and responding to incidents. It should also cover supply chain security, because your subcontractors may introduce risk. The program must be approved by your senior management and communicated to all employees.

One practical tip: use the certification as a driver to improve your overall security posture. The controls you put in place for level 1 will also help you meet other regulatory requirements, such as those from the Defence and Security Public Engagement program or industry-specific standards. It is not extra work; it is foundational work that pays off in multiple areas.

For IT security specifically, make sure your network is segmented so that contract data is separate from general business operations. Implement role-based access controls so that only people who need the information can access it. Regularly patch your systems and run vulnerability scans. These are basic practices, but they are often overlooked in smaller organizations.

DWG - 003 / 02 - FIRST EDITION - 2026

CPCSC - ITSP.10.171 - SCOPING - EVIDENCE

// THE STUDY GUIDE TO

CPCSC READINESS

A Field Reference for Canadian Defense Suppliers

// AUTHOR

Hans Study, CISSP

NETWORK AND SECURITY CONSULTANT

// REVISION 1.3 - OCTOBER 2026

Includes the September 29, 2026
program changes

Looking Beyond Level 1

Once you have achieved cpcsc level 1, you may find that your customers or future contracts require higher clearance levels. The foundation you have built will make that transition easier. The higher levels add more stringent controls, such as enhanced personnel security screening and more rigorous third-party assessment. But the discipline of maintaining a company security program and documenting your security controls remains the same.

I have worked with organizations that started at level 1 and later moved to level 2 or 3 as their contracts grew. They consistently say that the upfront investment in their security program saved them time and money later. They did not have to rebuild their processes from scratch. They just built on the base they already had.

Final Thoughts

Navigating the Program for Cyber Security Certification can feel daunting at first, especially if your organization has not dealt with government security requirements before. But cpcsc level 1 is a practical starting point. It asks you to put in place the basic security controls that any responsible organization should have. It protects your business, your employees, and the national security interests of Canada.

The key is to start early, take the assessment seriously, and view the certification not as a burden but as a tool for improvement. With the right approach, you can meet the requirements, win contracts, and build a stronger security culture within your company. That is good for your bottom line and good for the country.