

// 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

Preface

This book exists because of the fabricators. From 2016 to 2020 my readiness work ran across PCI-DSS, ISO 27001, NIST SP 800-53, and ITSG-33, the federal government's IT security risk management framework, getting organizations compliant and keeping them there. Then CMMC came over the border. I believe the first CMMC and 800-171 engagement came around March 2020... right around the time everything else started. The defense contractors I worked with were already living under NIST SP 800-171 through their primes, and most of them were small, family-run shops making wiring harnesses for weapon systems, fasteners bound for a fighter program, machined parts for attack helicopters. We did the gap analysis, the security testing, and the build-out that followed... and I spent a lot of that time translating.

Translating, because a requirement would say endpoints must be protected against malicious code, and the owner would hear "buy something for 45 computers." Only 2 of those 45 ever touched the drawings. Do those 2 need to talk to the other 43? No. Do they need the internet? Sometimes. So they get their own VLAN, that segment becomes the compliant one, the business network still gets hardened, and the phones go somewhere else entirely; everyone had been running all of it on one wifi. That is the method in this book. Read each requirement for what it's asking, then size the controls to the shop in front of you. A harness maker with one defense job among 400 customers doesn't need the plant in kiosk mode. An engineering team writing firmware for a networked braking subsystem on an armoured vehicle, on laptops they take home, needs more than it has.

CPCSC is new enough that nobody has a decade of it; I'd had conversations with ISED about CyberSecure Canada while that program was still in development, and CPCSC is where that road ended up. The controls underneath it are the ones I've been implementing all along, and those engagements inspired the scenarios in this book, with details changed and composites used. If one looks like your network, that's the point.

Nobody paid for placement here, no assessor reviewed it for friendliness, and where the program is awkward or underbaked, I say so. It will keep moving after this prints; the companion pages at hans.study carry the current CPCSC state with a verification date, and the policy templates and checklists from the back of this book live there too, as editable downloads.

Hans Study

contact@hans.study · [@studybyt3s](https://t.me/studybyt3s)

CPCSC AT A GLANCE

Three levels. The contract names which one you need, and the requirement follows the data down the supply chain.

// LEVEL 1

13

requirements

// WHO ASSESSES

Self-assessment and a signed attestation in CanadaBuys

// CYCLE

Every year

LIVE · in select contracts since summer 2026

// LEVEL 2

98

requirements

// WHO ASSESSES

Third-party assessment by an SCC-accredited certification body

// CYCLE

Every 3 years, annual affirmation

SPRING 2027 · planned for select contracts

// LEVEL 3

130+

controls

// WHO ASSESSES

Assessed by National Defence; 98 plus enhancements from NIST SP 800-172

// CYCLE

Every 3 years, annual affirmation

IN DEVELOPMENT · restated Sept 29, 2026

Level 1 is the first step for everyone; the Standards Council of Canada lists the Level 1 self-assessment as a prerequisite for Level 2.

What CPCSC Is and Why Ottawa Built It

Canada's defense supply chain now has a cyber security gate on it, and the gate was 10 years in the making.

// LEARNING OBJECTIVES

What the Canadian Program for Cyber Security Certification is and who runs it. What Specified Information means. Where the program came from, why it exists, and why it looks the way it does.

The Short Version

The Canadian Program for Cyber Security Certification, CPCSC, is a mandatory certification program for suppliers that bid on or perform Government of Canada defense contracts involving Specified Information. Public Services and Procurement Canada manages it. The technical foundation is ITSP.10.171, a Canadian adaptation of NIST SP 800-171 published by the Canadian Centre for Cyber Security. Certification comes in 3 levels, and the level a supplier needs is written into each solicitation and contract.

That's the program in one paragraph. The part that changes behaviour is the enforcement model. There's no CPCSC inspector, no fine schedule, and no compliance deadline in the abstract. Enforcement runs through procurement: once a solicitation names a level, a supplier that can't demonstrate it isn't eligible for award. The program doesn't chase anyone; it waits at the door of every contract you want.

Eight federal bodies have a hand in it, and knowing which does what saves time when you need an answer. PSPC leads and runs the certification processes. National Defence performs the Level 3 assessments and shapes the requirements. The Standards Council of Canada accredits the certification bodies that perform Level 2 assessments. The Cyber Centre, inside the Communications Security Establishment, wrote ITSP.10.171. Treasury Board Secretariat owns the policy framework, ISED covers industry readiness, Global Affairs Canada handles the allied-market access objective, and Public Safety Canada ties it to the National Cyber Security Strategy. The government describes its own approach as risk-based and adaptive, with standards and processes reviewed as the rollout teaches it things, which is a polite way of saying the details will keep moving. The 4 commitments behind that approach: apply the requirements the same way across defense contracts and state them clearly in procurement, make sure the accredited certification bodies have the capacity and expertise, keep governance tight with the Standards Council of Canada, and stay aligned with international standards and allied practice.

THE 13 LEVEL 1 REQUIREMENTS

// ACCESS CONTROL

- 03.01.01 Account management
- 03.01.02 Access enforcement
- 03.01.20 Use of external systems
- 03.01.22 Publicly accessible content

// IDENTIFICATION AND AUTHENTICATION

- 03.05.01 User identification and authentication
- 03.05.02 Device identification and authentication
- 03.05.03 Multi-factor authentication**

// MEDIA PROTECTION

- 03.08.03 Media sanitization

// PHYSICAL PROTECTION

- 03.10.01 Physical access authorizations
- 03.10.07 Physical access control

// SYSTEM AND COMMUNICATIONS PROTECTION

- 03.13.01 Boundary protection

// SYSTEM AND INFORMATION INTEGRITY

- 03.14.01 Flaw remediation
- 03.14.02 Malicious code protection

03.05.03 catches CMMC shops. MFA on privileged and non-privileged accounts is required at CPCSC Level 1. CMMC Level 1 has no MFA requirement.

Filing It in CanadaBuys

PSPC's guidance on meeting Level 1 sets out the mechanics, and they're simpler than the attestation's weight suggests. The certification has to be in place at contract award, and proof of it goes in with the bid, so finish it before bid season rather than during it.

1. Make sure the organization has an active CanadaBuys account and supplier profile; without one you can't take part in a procurement that requires Level 1. 2. Read the Level 1 criteria and PSPC's CPCSC Level 1 Scoping Guide, then draw your boundary as chapter 6 describes. 3. Complete the self-assessment with PSPC's online tool. You can assess by another means, but you're responsible for keeping the results either way. 4. When you finish, the tool shows a results page with an expiry date. Print it or save it as a PDF, and file it with your evidence folder. 5. In CanadaBuys, confirm the self-assessment result and its expiry date in the organizational supplier profile questionnaire. 6. When you bid on a defense contract that requires Level 1, include proof of the self-attestation and its expiry date with the submission. 7. Put the expiry date in the calendar with a month's lead time, and treat a material change to the environment as a reason to reassess early.

Screen names and menus in CanadaBuys change. Follow the portal's current wording, and check the companion pages if a step has moved.

When You Don't Meet a Control

// WARN

The annual cycle is a floor, not a trigger. If your environment changes materially mid-year, a new site, a new cloud tenant, a merger, the systems holding Specified Information moved, your last attestation describes a network that no longer exists. Re-run the assessment when the environment changes, and treat the anniversary as a backstop.

Fix it first. Level 1 controls are cheap to close; the expensive ones live at Level 2. Attesting falsely to avoid 2 weeks of remediation is trading a small schedule problem for a legal one, and the schedule problem was probably solvable inside the bid window anyway. If a gap can't close before a bid deadline, that is a conversation with your contracting authority about timing rather than a box to shade optimistically.

The work: baselines for the enclave's workstation and server classes, hardened against a recognized benchmark, local admin stripped from daily-driver accounts, an inventory of what runs, and every change recorded with a date and a name. Tedious, and it powers half the other families, because drift is where controls stop working without anyone noticing.

How we can interpret it: Baselines, change approval, and evidence. For the technical side, rConfig is my push for network gear, and network configs can be diffed automatically so drift shows up on its own. The managerial side is the documented change process. Someone wants to run Windows Update on the server or change a firewall rule, so they submit a request, the named approver approves, a change window gets set, and the completion gets recorded. I have been audited on federal systems several times a year, and the conversation is always the same. Do you do change management? Yes. Show me. Here's the email asking the IT director for a window, here's the completion email, and here's the documented process they match.

```
// EXAMPLE · CHANGE REQUEST RECORD
Request ID:      CR-2026-014
Requested by:    (name, role)
Change:         Apply September cumulative update to FS01
Systems:        FS01 (enclave file server)
Reason:         Monthly patch cycle; CVE remediation
Risk / rollback: Snapshot before install; revert on failure
Window:         Sat 2026-10-04, 06:00-08:00
Approver:        (name, role)      Approved: (date)
Completed by:    (name)            Completed: (date/time)
Evidence:        WSUS report attached; login/logout log attached
```

Identification and Authentication

Requirements: 03.05.01 User identification, authentication, and re-authentication (Level 1) · 03.05.02 Device identification and authentication (Level 1) · 03.05.03 Multi-factor authentication (Level 1) · 03.05.04 Replay-resistant authentication · 03.05.05 Identifier management · 03.05.07 Password management · 03.05.11 Authentication feedback · 03.05.12 Authenticator management.

Intent: know who is on the system before it does anything.

Reality: MFA on the VPN maybe, absent on email, absent on the domain, absent on the cloud tenant's admin plane.

The work: MFA on every path to Specified Information and on every privileged account, unique IDs, a written password policy that matches the one applied, and replay-resistant mechanisms. MFA on privileged and non-privileged accounts is already a Level 1 requirement (03.05.03); Level 2 adds the rest of the family, replay resistance and authenticator management included.

How we can interpret it: Get a decent layer 3 gateway, segment the network, route between VLANs on purpose, and never permit any-to-any. MSPs love installing a branded firewall and telling the client the blinky box protects them. The blinky box protects nobody until it's configured, and it can carry every feature on the datasheet while doing nothing. That is why configuration auditing matters. For the assessment, bring a logical topology diagram, the list of controls between a user and the enclave, and the firewall rule set, because they will ask for the rule set. Add DNS filtering; in Canada, CIRA DNS Firewall is the business service (Canadian Shield is the free home product). Lock down web access on the enclave to what the work needs.

// SCENARIO

The friendly version of this failure: a shop lets employees put their phones on the wifi, and the wifi is the same flat network as everything else. No segmentation, so every personal device shares a broadcast domain with the CAD workstations and the CNC controllers. Nobody broke a rule, because there was no rule; the network just grew that way. The fix is ordinary. Guest and personal devices get their own SSID and VLAN, firewalled from the production segments, and the enclave sits behind its own edge. What made it urgent was reading the standard against the network diagram and realizing the diagram was one circle.

System and Information Integrity

Requirements: 03.14.01 Flaw remediation (Level 1) · 03.14.02 Malicious code protection (Level 1) · 03.14.03 Security alerts, advisories, and directives · 03.14.06 System monitoring · 03.14.08 Information management and retention · 03.14.09 Dedicated administration workstation.

Intent: patch on a cadence with proof, run current malware protection everywhere in scope, act on the alerts your own tools raise, and do administrative work only from a dedicated, isolated workstation.

Reality: "we patch when we can," Windows patched and nothing else, alerts landing in a mailbox nobody owns.

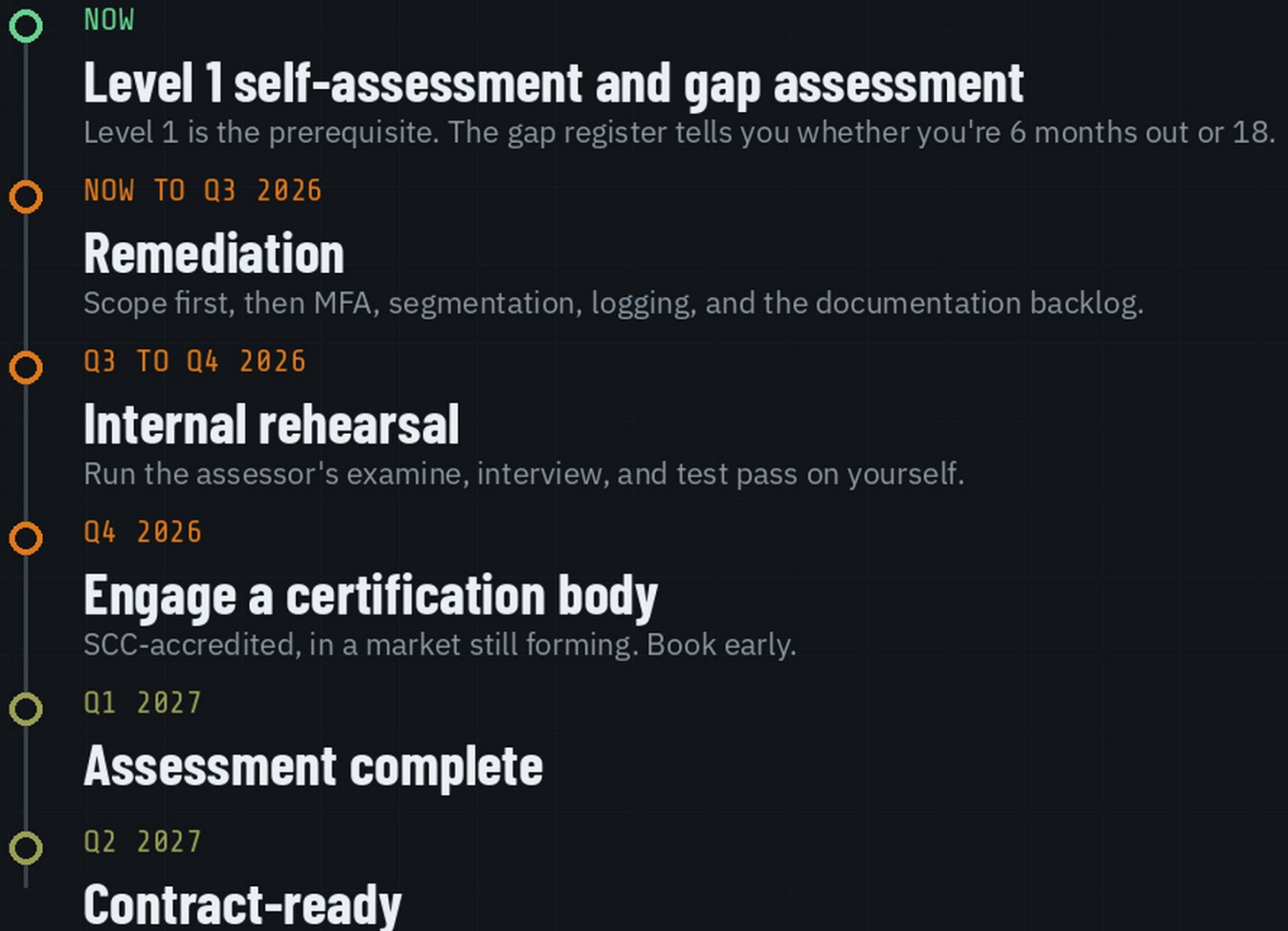
The work: "critical patches inside 14 days, the rest monthly, exceptions recorded," with the patch report joining the evidence folder and every alert routed to a ticket that gets closed.

How we can interpret it: Endpoint protection, XDR or MDR where the budget allows, and patch management that covers Office and third-party software, not just Windows. The evidence is the report. Route alerts into the ticket system so each one gets acknowledged, remediated, and closed, and you can show the auditor that the alert arrived on a date, a named person looked at it, and the update got applied.

Canada's addition, 03.14.09: dedicated administration workstation. This is the one requirement in ITSP.10.171 that isn't in NIST SP 800-171, and it comes from the Canadian control catalogue (source control SI-400, the ITSG-33 lineage) rather than from NIST. It asks for 3 things. Administrative and superuser actions get done from a physical workstation dedicated to that work and isolated from all other functions and networks, especially the internet. Remote connection from that workstation to the network it administers runs over a carrier private network, such as VPLS or

THE ROAD TO SPRING 2027

Level 2 reaches select contracts from spring 2027. Count back from the bid you want and the start date is closer than it looks.



A contained shop with current infrastructure needs roughly 6 months of part-time effort. A flat network with shared admin accounts needs 18 months and some capital.

// THE STUDY GUIDE TO CPCSC READINESS

READ THE FULL BOOK, FREE

This sampler pulls a few pages from the book. The full digital edition covers all 12 chapters, all 98 ITSP.10.171 requirements with a plain reading of each family, the Canada and US terminology table, and the templates, free under CC BY-ND 4.0.

// THE BOOK

hans.study/CPCSC_BOOK

// CPCSC HUB · UPDATED AS THE PROGRAM MOVES

hans.study/CPCSC

// TEMPLATES AND CHECKLISTS

hans.study/CPCSC/templates



SCAN FOR THE FULL BOOK

CPCSC is still being built. Level 2 and Level 3 details, certification bodies, and fee structures are still to come. The hub carries the current state with a last-verified date.

// <https://hans.study>

Hans Study · DOI 10.5281/zenodo.23145961
ISBN 978-1-0680175-2-0 (PDF) · CC BY-ND 4.0