

// 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

// THE STUDY GUIDE • CODES • STANDARDS • PRACTICE

The Study Guide to CPCSC Readiness

A Field Reference for Canadian Defense Suppliers

Hans Study, CISSP

hans.study • Ontario, Canada

The Study Guide to CPCSC Readiness

A Field Reference for Canadian Defense Suppliers

Copyright © 2026 Hans Study.

This book is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International licence (CC BY-ND 4.0). You may copy and redistribute it in any medium or format, for any purpose, as long as you credit Hans Study, link to the licence, and indicate if changes were made; you may not distribute modified versions. Licence text: <https://creativecommons.org/licenses/by-nd/4.0/>

Suggested attribution: The Study Guide to CPCSC Readiness, by Hans Study, hans.study/CPCSC_BOOK, licensed CC BY-ND 4.0. The policy templates on the companion site carry their own terms.

ISBN 978-1-0680175-2-0 (digital PDF edition)

Also available as an EPUB, ISBN 978-1-0680175-3-7, and in paperback, ISBN 978-1-0680175-1-3

First edition, September 2026.

Revision 1.3, October 1, 2026 (includes the September 29, 2026 program updates) · built 2026-10-01

DOI 10.5281/zenodo.23145961 · <https://doi.org/10.5281/zenodo.23145961>

This book describes a government program that continues to evolve. It's a field reference, not legal advice, and not a substitute for the contract clauses in front of you. Where this book and an official Government of Canada publication disagree, the official publication wins. Current program state: hans.study/cpsc

Scenarios and Study Notes are illustrative composites inspired by real engagements; identifying details have been changed.

No vendor sponsored, reviewed, or paid for placement in this book.

*For Desiree (DW),
for the support through the long nights
and everything that came with them.*

I love you.

*And for Scott, friend, business partner, and the audit mind that set me on the right path.
We built a company together, and he taught me how to look at an audit:
what to ask, and what to make them show you.
They say Marines eat crayons. This one ate Excel sheets.
I don't look at a spreadsheet the same way anymore... they look tasty now.*

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)

Contents

// PART I • THE PROGRAM

01	What CPCSC Is and Why Ottawa Built It	8
	The Short Version	8
	Specified Information	9
	How Canada Got Here	9
	Why the Program Exists	10
02	The 3 Levels, Plainly	11
	Level 1: Self-Assessment Against 13 Controls	11
	Level 2: Third-Party Assessment Against 98 Controls	11
	Level 3: Assessed by National Defence	12
	Which Level You Need	12
03	Does This Apply to You	13
	The Test Is the Data	13
	Flow-Down	13
	Boundary Cases from the Field	13
	The "We Only Have a Few Files" Trap	14
04	CPCSC, CMMC, and ITSP.10.171	15
	The Family Tree	15
	Where the Requirements Come From	15
	Where the Programs Diverge	16
	Mutual Recognition: Not Yet	17
	What Transfers If You've Done One	17

// PART II • GROUNDWORK

05	Level 1: The 13 Controls and the Attestation You're Signing	19
	What the 13 Controls Are About	19
	Scope Before You Answer Anything	20
	Evidence for a Self-Assessment	20
	Filing It in CanadaBuys	21
	When You Don't Meet a Control	21
06	Scoping: Where Specified Information Lives	22
	Why Scope Is the First Engineering Decision	22
	Mapping the Flow	22
	Asset Categories	23
	Shrinking the Footprint	23
07	Running Your Own Gap Assessment	25
	Before You Spend a Dollar	25
	The Method	25
	Ranking What You Found	26

Reading the Result	26
--------------------------	----

// PART III • THE WORK

08 The Technical Work, Control Family by Control Family	27
How to Read This Chapter	27
Access Control	27
Awareness and Training	28
Audit and Accountability	29
Configuration Management	29
Identification and Authentication	30
Incident Response	31
Maintenance	32
Media Protection	32
Personnel Security	33
Physical Protection	34
Risk Assessment	34
Security Assessment and Monitoring	35
System and Communications Protection	35
System and Information Integrity	36
Planning	37
System and Services Acquisition	37
Supply Chain Risk Management	38
09 Documentation That Survives an Assessor	39
The Stack, Smallest to Largest	39
The System Security Plan	39
The Remediation Register	40
Evidence Without Drowning	40

// PART IV • CERTIFICATION

10 Level 2 Prep: What Third-Party Assessment Looks Like	42
The Assessment Machinery	42
What Assessors Do	43
The Common Findings	43
The Calendar Math	43
11 Small Shop Realities: MSPs, Cloud, Cost, and Sequencing	44
You Without a Security Team	44
The MSP Relationship Grows Up	45
Cloud, Sovereignty, and the Fine Print	45
What This Costs	45
12 Staying Certified: Life After the First Attestation	47
The Recurring Clocks	47
What Re-Opens Scope	47

Incidents and Obligations	47
Watching the Program Move	48

// APPENDICES

A	Level 1 Readiness Checklist	49
B	Terminology Translation, Canada and the US	50
C	Primary Sources and Where the Current State Lives	52
D	Templates and Examples	53
E	ITSP.10.171 Requirement Index	55

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.

// WARN

CPCSC is a program under active development. Levels 2 and 3 were still being built when this edition went to print, and PSPC revises its pages without announcement; the September 29, 2026 program overview changed the Level 3 count with no press release attached. Before you act on a date, a count, or a procedure in this book, check the companion pages at hans.study/cpcsc, which carry the current state and a last-verified date.

Specified Information

Everything in CPCSC hangs off one term. Specified Information is sensitive but unclassified government information, identified in a contract as requiring safeguarding when it lives on supplier systems. It's Canada's counterpart to the American term Controlled Unclassified Information, and in real contracts it looks like technical drawings, statements of work, schedules, pricing, specifications, and Controlled Goods data.

Two properties of Specified Information do most of the work in this book. It's defined by the contract, so the same drawing can be Specified Information on one project and ordinary business correspondence on another; read the clauses. And it follows the data, so the requirement flows down to subcontractors who store, process, or transmit it. Being 2 tiers below the prime doesn't exempt you; holding the data obligates you.

// SPEC · THE CORE TEST

If your systems store, process, or transmit Specified Information under a Department of National Defence contract, CPCSC applies to your organization at the level named in that contract, regardless of your size, your tier in the supply chain, or your line of business.

How Canada Got Here

The pressure started south of the border. In 2016 and 2017 the US wrote basic safeguarding clauses into federal contracts, FAR 52.204-21 for federal contract information and DFARS 252.204-7012 requiring NIST SP 800-171 for CUI. Canadian companies selling into the American defense market started meeting those obligations through their US contracts while Canada had no domestic equivalent. For years, a Canadian supplier's cyber security obligations depended on which side of the border the cheque came from.

The US then spent 2020 and 2021 demonstrating how not to launch a certification program. CMMC 1.0 arrived with 5 levels and third-party assessment for nearly everyone; industry pushback forced a redesign into the 3-level CMMC 2.0 within 2 years. Canada took notes. When Treasury Board approved CPCSC in fall 2023, with \$25 million identified in Budget 2023 for design and implementation through 2025 to 2026, the program that emerged had 3 levels, self-assessment at the bottom, and an existing standard underneath it rather than a new invention.

The build-out ran through 2025. The program's first phase opened in March 2025: standards work, development of the Level 1 self-assessment tool, and the Standards Council of Canada opening applications from organizations seeking accreditation as certification bodies. ITSP:10.171 took effect April 2, 2025, with a second release following on October 28, 2025. Level 1 became available to suppliers on April 1, 2026, with attestations recorded in CanadaBuys, was formally announced 2 weeks later, and began appearing in select defense contracts that summer. Level 2 third-party assessments are planned for select contracts starting spring 2027.

Why the Program Exists

The government's stated outcomes are worth reading because they explain the design. Protect federal contractual information held below the classified level on contractor systems. Maintain Canadian industry's access to international procurement with similar certification requirements. Raise the baseline of cyber security across the defense industry. Keep the supplier base reliable enough to support Canadian Armed Forces capability and readiness. And grow Canadian industry's participation in the certification program itself, which is the quiet admission that assessor capacity is a national problem as much as a supplier one. PSPC ties all of it to the Defence Industrial Strategy and the National Cyber Security Strategy, and describes the program's working parts as 4 things: cyber security controls, cyber security risk assessments, contractual clauses, and accredited third-party assessors.

The second outcome is the one that explains the design. Five Eyes partners are converging on certified supply chains, the US fastest of all. A Canadian company that can't demonstrate certification against the 800-171 control family risks getting squeezed out of allied procurement no matter what Ottawa requires domestically. Building CPCSC on the same technical controls keeps Canadian suppliers interoperable with that direction, while Canada keeps its own certification authority, its own assessor accreditation, its own portal, and its own data governance, so the control set matches the allies and the machinery stays Canadian.

// STUDY NOTE

The calls I get about CPCSC split into 2 groups. Defense primes saw this coming years out and have teams on it. Everyone else found out from a solicitation. The integrator putting cameras into a DND facility, the machine shop 3 tiers down on a vehicle program, the software sub with one government customer... they don't think of themselves as the defense industrial base, and the program doesn't care how they think of themselves. It reads the data flow. If I could get one sentence in front of every supplier in the country, it's this: check your contracts for Specified Information clauses before your competitors do, because the ones who check first get to plan, and the ones who check last get to scramble.

There's a blunter reason underneath the policy language. Defense supply chains get attacked because contractors hold sensitive government data on networks that are softer than government networks. The engineering data for a platform that took 20 years to develop can leave through a machine shop's unpatched file server in an afternoon. Raising the floor across thousands of suppliers, most of them small and medium businesses, costs less than absorbing that kind of loss even once.

The 3 Levels, Plainly

Three tiers, three assessment models, and a cost curve that bends hard between the first and second.

// LEARNING OBJECTIVES

What each CPCSC level requires, who assesses it, on what cycle, and what the real effort looks like at each tier.

Level 1: Self-Assessment Against 13 Controls

Level 1 is an annual self-assessment against 13 security requirements, completed with PSPC's online tool, with the result and its expiry date confirmed in your CanadaBuys supplier profile. It's been available since April 1, 2026, and it's the level appearing in select contracts now.

The 13 controls cover foundational safeguarding: account management and access enforcement, user and device authentication with multifactor, media sanitization, physical access, boundary protection, patching, and malicious code protection. If your network is competently run you meet most of them already, with MFA the usual exception. Chapter 5 lists the 13 by identifier.

The trap at Level 1 isn't technical difficulty. The trap is treating a self-assessment as a formality. That attestation is a signed representation in a federal procurement context, and misrepresenting your compliance carries legal exposure. The American side put a number on that exposure in September 2026, when an aerospace supplier settled False Claims Act allegations over NIST SP 800-171 failures for about \$2 million while the CMMC certification phase was suspended. The pause stopped assessments and left the liability where it was. "Self-assessed" describes who does the checking, and nothing about how seriously the answers get treated later. Answer it like someone might read it back to you in a dispute, because someone might.

// SPEC • LEVEL 1 AT A GLANCE

Controls: 13 security requirements
Assessor: the supplier (self-assessment)
Artifact: signed attestation via CanadaBuys
Cycle: annual
In contracts: select defense contracts, summer 2026 onward

Level 2: Third-Party Assessment Against 98 Controls

Level 2 is where the program grows teeth. 98 controls drawn from ITSP.10.171, assessed by a third-party certification body accredited by the Standards Council of Canada, on a 3-year certification cycle with an annual affirmation in between. It's planned to appear in select contracts starting spring 2027.

The jump from 13 controls to 98 understates the jump in effort. Level 1 asks whether you do sensible things. Level 2 asks you to prove it to a stranger: documented policies, enforced procedures, a system security plan that matches your actual environment, evidence for every control, and a scope tight enough that the assessment doesn't wander across your entire business. Chapters 6 through 10 are essentially a manual for that jump.

One pattern from the American experience with the same control set is worth stating this early: governance fails organizations more often than technology does. Firewalls and encryption get budget because they're purchasable. Documented procedures, separation of duties, evidence discipline, and change control are where third-party assessments go sideways, and they're what an assessor reads first.

Level 3: Assessed by National Defence

Level 3 is assessed by National Defence itself, on the same 3-year cycle with annual affirmations, against what PSPC now describes as 130-plus controls: the 98 of ITSP.10.171 plus enhanced requirements adapted from NIST SP 800-172. Earlier program pages said 200; the September 29, 2026 program overview restated it, and PSPC describes Levels 2 and 3 as under development. It's aimed at the most sensitive work. The Level 3 criteria and assessment method had not been published at press time.

For most readers of this book, Level 3 is a horizon item. If your work sits at that tier, you already have a security team and a relationship with the department, and you're using this book to bring your subcontractors along rather than to orient yourself.

Which Level You Need

// **WARN**

Don't infer your level from your company size or your work's sensitivity as you perceive it. Suppliers guess low. The contract clause is the only authority on what level applies, and the time to read it is before bid strategy, not during proposal week.

None of them, until a contract says otherwise. The required level is set per solicitation, which means your CPCSC target is a business development question before it's a security question. One sequencing fact is fixed regardless: the Standards Council of Canada states that a completed Level 1 self-assessment is a prerequisite for Level 2 certification, so Level 1 is everyone's first step, including the shops heading straight for Level 2. The level you prepare for should come out of your pipeline: the contracts you hold, the ones you intend to bid over the next 2 years, and what their clauses name.

Does This Apply to You

The suppliers most surprised by CPCSC are the ones who never thought of themselves as defense suppliers.

// LEARNING OBJECTIVES

How to determine whether CPCSC reaches your organization, how flow-down works, and where the boundary cases land.

The Test Is the Data

CPCSC doesn't apply to "defense companies." It applies to organizations whose systems store, process, or transmit Specified Information under a defense contract. That distinction moves the boundary a long way out from where most people draw it instinctively.

Work through the test in order. Do you hold, or will you bid, a contract connected to the Department of National Defence, directly or through a prime? Does that contract identify Specified Information, in its clauses or its security requirements checklist? Does any of that information touch your systems: your file server, your email, your laptops, your cloud tenant, your backups? Three yeses and you're in the program at whatever level the contract names. The size of your company never enters the test.

Flow-Down

Primes don't absorb the obligation on your behalf. When a prime holds a contract with CPCSC requirements and passes Specified Information to a subcontractor, the safeguarding requirement travels with the data, and the sub attests or certifies on its own account. Expect primes to get systematic about this quickly; a prime whose award depends on supply chain compliance will start asking subs for their CPCSC status the way they already ask for insurance certificates. Some already are.

The practical consequence is that your CPCSC posture is becoming part of your sales position even when the government never sees your name. A sub that can show a completed Level 1 attestation today, and a credible Level 2 plan for 2027, is easier to keep on the bid team than one that answers the security questionnaire with silence.

Boundary Cases from the Field

The integrator. You install cameras and access control at a defense facility. Whether CPCSC reaches you depends on what touches your systems. If your commissioning laptops hold facility drawings, device schedules, or network documentation identified as Specified Information, you're in. If you never hold the data, the physical site access rules that already govern you are a separate regime. Most integrators who look will find project folders full of exactly this material.

The machine shop. You cut parts from drawings supplied by a prime, 3 tiers up from DND. Those drawings are the canonical Specified Information case. The shop's ERP, the engineer's workstation, the email the drawing arrived in, and the backup of all 3 are in scope.

The software subcontractor. Your code runs in someone else's environment, but the requirements documents, interface specs, and test data on your systems can all be Specified Information. Read what the prime sent you.

The MSP. You're not a defense supplier at all; your client is. If you administer the systems where their Specified Information lives, your access, your tooling, and your personnel are inside their scope, and their assessor will look at you. Chapter 11 deals with this relationship in detail, from both sides.

The commodity vendor. You sell the prime standard laptops off a price list. Selling unmodified commercial goods without receiving Specified Information generally sits outside the program's reach. The moment customization starts and technical data flows to you, re-run the test.

The "We Only Have a Few Files" Trap

The most common self-exemption I hear is volume-based: we only hold a handful of drawings, surely this isn't aimed at us. The program has no volume threshold. One drawing on one laptop puts that laptop, and everything it meaningfully connects to, inside the question. Volume matters enormously for scoping cost, which is Chapter 6's subject, and not at all for applicability.

// STUDY NOTE

A shop owner told me last spring that CPCSC couldn't apply to him because his DND-connected work was 4 percent of revenue. We found Specified Information in 6 places in an afternoon: the quoting folder, 2 engineers' laptops, the shared drive, his own email, and the cloud backup of everything above. The program applied to 4 percent of his revenue and roughly 80 percent of his network. That ratio is normal, it's the whole argument for scoping properly, and it's why "how much defense work do you do" is the wrong question. Where the data went is the question.

The second most common is the Controlled Goods conflation. Controlled Goods Program registration governs who may examine or possess controlled technical data; CPCSC governs how the systems holding contract data are secured. They overlap on the same drawings and satisfy nothing about each other. If you're CGP-registered, you have a head start on knowing where your sensitive data is, and no head start on certification.

CPCSC, CMMC, and ITSP.10.171

Two programs built on one control set, with no mutual recognition between them, so the overlap saves implementation work and none of the paperwork.

// LEARNING OBJECTIVES

How the Canadian and American programs relate, what ITSP.10.171 changes from NIST SP 800-171, and what transfers between the 2 regimes when you face both.

The Family Tree

NIST SP 800-171 is the common ancestor. The US wrote it to protect Controlled Unclassified Information on non-federal systems, wired it into defense contracts through DFARS 252.204-7012 in 2017, and later built CMMC on top of it as the verification layer. Canada's Cyber Centre took the same publication and produced ITSP.10.171, "Protecting Specified Information in Non-Government of Canada Systems and Organizations," effective April 2, 2025. PSCC describes the Canadian standard as closely adapted from both SP 800-171 and SP 800-172, the enhanced-requirements companion, which is where Level 3's additional controls come from. CPCSC is the verification layer on the Canadian adaptation.

The government has been direct about what the adaptation changes: nothing substantive in the technical requirements. The differences are contextual. Specified Information replaces Controlled Unclassified Information. Treasury Board Secretariat policy replaces American regulatory references. Canadian privacy law sits underneath instead of American frameworks. If you can implement one document, you can implement the other; the controls are the point of the exercise, and the controls match.

Where the Requirements Come From

ITSP.10.171 is the fourth link in a chain, and each link explains something about the document you'll be working from. NIST SP 800-53 is the catalogue: every security and privacy control the US federal government draws on, now in its fifth revision, which Canada maintains in its own version as ITSP.10.033, the catalogue that superseded ITSG-33 Annex 3A, the control catalogue federal departments selected from for over a decade. NIST SP 800-171 is a tailored slice of that catalogue, the moderate baseline cut down to what protects the confidentiality of controlled unclassified information on systems the government doesn't own, first published in 2015. Revision 2, from 2020, carries 110 requirements and is what CMMC assesses today. Revision 3, from May 2024, restructured the set to 97: duplicates consolidated, 3 families added (planning, system and services acquisition, and supply chain risk management), and organization-defined parameters introduced so the standard could stop hard-coding numbers that vary by organization.

ITSP.10.171 is the Cyber Centre's adaptation of Revision 3. First release April 2, 2025; second release October 28, 2025, which is the current one. It carries 98 requirements across the 17 families, the 97 from Revision 3 plus one Canada added (03.14.09, dedicated administration workstation, covered in chapter 8), keeps the identifiers NIST withdrew as not allocated so the numbering lines up across the border, swaps Specified Information for CUI, and points at Canadian policy and privacy law instead of American references. The document itself says the technical content isn't substantively changed, and reading the 2 side by side bears that out.

Two companions matter in practice. NIST SP 800-171A supplies the assessment procedures: for each requirement, the determination statements an assessor works through and the 3 methods available, examine, interview, and test. PSPC's Level 1 criteria is a Canadian version of 171A Revision 3, which is why chapter 5 keeps pointing you at it. SP 800-172 holds the enhanced requirements for higher-sensitivity work; CPCSC Level 3's additional controls are adapted from it.

Organization-defined parameters deserve their own paragraph because they decide how much of this standard you get to set yourself. An ODP is the blank inside a requirement: how long before an inactive account is disabled, how many failed logins before lockout, how long logs are retained, what counts as a privileged function at your shop. ITSP.10.171 allows government departments and non-government organizations to specify the values. Unless a contract names a value, you choose it, you write it in the system security plan, and you defend it in the assessment. The square brackets in the templates at the back of this book and on the companion site are exactly those blanks. PSPC had not published fixed values for any level by press time; if that changes, the companion pages will say so.

Where the Programs Diverge

Everything administrative diverges, and administration is where the money and calendar time go.

Legal machinery. CMMC lives in US federal rulemaking: 32 CFR Part 170 established the program in December 2024, and the 48 CFR acquisition rule made certification a condition of award through DFARS 252.204-7021 in November 2025. CPCSC lives in Canadian procurement policy under PSPC, expressed through RFP and contract clauses. Different instruments, different amendment processes, different people to argue with.

Assessor structures. CMMC third-party assessments run through C3PAOs accredited under the Cyber AB. CPCSC Level 2 assessments run through certification bodies accredited by the Standards Council of Canada. Separate accreditations, separate markets, separate scheduling queues, and the Canadian queue is still forming ahead of spring 2027.

Level arithmetic. CMMC Level 1 is 15 requirements; CPCSC Level 1 is 13. CMMC Level 2 assesses the 110 controls of NIST SP 800-171; CPCSC Level 2 assesses 98 controls under ITSP.10.171. CMMC Level 3 adds 24 enhanced requirements from NIST SP 800-172 to its Level 2 base; CPCSC Level 3 is 130-plus controls assessed by National Defence, with the enhanced requirements adapted from the same SP 800-172. The sets are close cousins, and scoping against the wrong document still wastes real hours. The difference is revision. The CMMC program rule assesses NIST SP 800-171 Revision 2 and its 110 requirements; ITSP.10.171 is a Canadian version of Revision 3, whose consolidated structure yields 98 requirements across 17 families. The Department has rulemaking under way to move CMMC onto Revision 3, which would close most of that gap when it lands.

Middle-tier structure. CMMC Level 2 splits by solicitation into self-assessment for some contracts and C3PAO certification for others. CPCSC Level 2 as published is third-party assessment, every 3 years, with annual affirmations. No self-assessed variant.

Filing systems. American attestations file in SPRS under a named affirming official. Canadian attestations file through CanadaBuys. Your compliance calendar has to track both if you sell into both markets, because neither system knows the other exists.

Rollout positions. CMMC has been enforceable in contracts since November 2025. Its Phase 2 expansion, the move to third-party certification as a condition of award, was suspended in July 2026 pending a departmental review, and a September class deviation made that suspension binding on contracting officers, with the review's report delivered to the CIO and unpublished as this edition went to print. CPCSC Level 1 entered contracts in summer 2026 with Level 2 still ahead. One program is mid-course-correction and the other is early in its rollout; both are contractually real today.

Mutual Recognition: Not Yet

As of this edition, no mutual recognition exists between the programs. A CMMC certificate satisfies nothing in a CPCSC clause; a CPCSC certification satisfies nothing in DFARS 252.204-7021. Cross-border suppliers run both processes and pay both assessment costs. The technical overlap shrinks the implementation work and leaves the administrative load untouched.

Recognition talks are the obvious future, and both governments have gestured at Five Eyes interoperability as a goal. Plan on the current state. A readiness program built on "they'll surely recognize each other by the time we're assessed" is a bet with your contract eligibility as the stake.

What Transfers If You've Done One

Carries well: the implemented controls, the enclave architecture, the system security plan's substance, the evidence habits, and the organizational muscle of someone owning the program. An environment built to 800-171 is most of the way to ITSP:10.171, and the reverse.

// STUDY NOTE

Cross-border shops keep making the same sequencing mistake. The controls transfer, so they assume the compliance does, and the second program becomes an afterthought until a bid needs it. Then they discover the second assessment queue, the second portal registration, and the second set of documentation conventions, each adding calendar weeks at the worst possible moment. Run both compliance calendars from day one even if only one program's clause has reached your contracts. The engineering overlaps; the bureaucracies have never been introduced, and you'll be the one doing the introductions.

Carries poorly: attestations, portals, assessment contracts, affirmation calendars, and certificates, which are all program-specific. Scope can also shift under Canadian data governance expectations, so an enclave accepted in a CMMC assessment isn't automatically the enclave a Canadian contract accepts. Read each solicitation's data handling requirements rather than assuming the architecture ports.

Translate your documentation. An assessor reading your SSP shouldn't have to guess that "CUI" means Specified Information in the Canadian binder. It's an afternoon of find-and-replace plus a glossary page, and it signals care in exactly the way assessors notice.

Level 1: The 13 Controls and the Attestation You're Signing

Thirteen controls most shops already meet, under a signature with legal weight.

// LEARNING OBJECTIVES

What the Level 1 requirements cover, how to complete the self-assessment defensibly, and what the attestation commits you to.

What the 13 Controls Are About

Level 1 assesses 13 of ITSP.10.171's 98 requirements, drawn from 6 families. PSPC publishes the assessment criteria for each one as a Canadian version of NIST SP 800-171A Revision 3, with determination statements an assessor works through and the methods available: examine the documents and settings, interview the people, test the mechanism. The 13, by identifier:

// SPEC · CPCSC LEVEL 1 REQUIREMENTS (PSPC LEVEL 1 CRITERIA)

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, authentication, and re-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

PSPC groups the 13 under plain-language practices for owners who don't speak control families: managing who can access systems, controlling how systems and data are used, verifying users and devices, protecting data and equipment, and defending systems from cyber threats. Useful framing for the toolbox talk; the identifiers are what you attest against.

One of those is worth reading twice. 03.05.03 requires strong multifactor authentication for privileged and non-privileged accounts, at Level 1. The American Level 1 has no MFA requirement at all, so a shop that cleared CMMC Level 1 on the strength of passwords is not at CPCSC Level 1 yet. The rest is the floor you'd expect: accounts managed and enforced, external systems and public content controlled, devices identified, media sanitized before it leaves, physical access authorized and controlled, a boundary that monitors and controls traffic, flaws patched inside a defined window, and malicious code protection that scans and blocks.

Read that list against a competently run small business network and most of it is already true. Accounts exist, the firewall exists, the antivirus updates itself, the front door locks. Level 1 gets hard in 3 places people don't expect: knowing the exact boundary of the systems you're attesting about, being able to show each control is real on those systems, and understanding what the signature means.

Scope Before You Answer Anything

The self-assessment asks about "your systems," and answering it without deciding which systems is how organizations attest to things that aren't true. Before the first question, map where Specified Information lives. Chapter 6 covers scoping in depth; the Level 1 version is a directed afternoon, not a project. List the contracts with Specified Information clauses. Trace where that data arrives, gets stored, gets worked on, and gets backed up. Draw the line around those systems. That's what you're attesting about.

The line matters in both directions. Drawn too wide, you're attesting controls on systems that never touch the data and creating exposure for no reason. Drawn too narrow, you've excluded the engineer's laptop that holds the drawings, and your attestation is wrong on day one.

Evidence for a Self-Assessment

Nobody reviews your evidence at Level 1 by default, and PSPC reserves the right to look. Collect it anyway. For each of the 13 requirements, keep one artifact that shows the control operating: the firewall config export, the screenshot of the AV console showing current signatures, the user list with dates, the media destruction receipt. An hour of screenshots turns your attestation from a memory into a record.

The reason is the signature. The attestation is a representation made in a federal procurement context, renewed annually, and misrepresentation carries legal exposure. If a dispute, an incident, or an audit ever puts your attestation under a light, "here's the evidence folder from the week we attested" is a different conversation than "we believed it to be true." Build the folder. Date it. Refresh it each year when the attestation renews.

```
// SPEC · LEVEL 1 WORKING METHOD
1. List contracts carrying Specified Information clauses
2. Map where that data lives; draw the system boundary
3. Answer the 13 requirements against those systems only
4. Capture one dated evidence artifact per requirement
5. Fix any gap before attesting, not after
6. Record the result and expiry date in CanadaBuys; calendar the renewal
7. Store the evidence folder with the attestation record
```

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.

Scoping: Where Specified Information Lives

Scope decides cost before a single control gets implemented.

// LEARNING OBJECTIVES

How to map Specified Information flows, define an assessment boundary, and shrink the footprint before it gets expensive.

Why Scope Is the First Engineering Decision

Every control you implement, document, and prove applies to every system inside your boundary. A supplier that confines contract data to a defined enclave assesses that enclave. A supplier that lets drawings and SOWs spread across every laptop and mailbox assesses the whole company. Same controls, same standard, and the second supplier pays several multiples of the first, at Level 1's afternoon scale and brutally at Level 2's.

Scoping runs backwards from how most people approach compliance. The instinct is to start with the control list. Start instead with the data, because until you know where Specified Information lives, the control list has no denominator.

Mapping the Flow

Trace the data's life. Where does it arrive: a prime's portal, email, a customer file transfer? Where does it rest: file server shares, project folders, the ERP, SharePoint, someone's desktop? Where does it get worked on: engineering workstations, CAM stations, the estimator's laptop? Where does it travel internally: email again, chat tools, the print server? Where does it leave: to your own subs, back to the prime? And where does it echo: backups, sync clients, archived mailboxes, the cloud recycle bin nobody thinks about?

Do this with the people who touch the data, not from the org chart. The official process says drawings live on the project share. The actual engineer has a working copy in Downloads, a marked-up copy in email, and a photo of one on their phone from the shop floor. The map you want is the real one; the assessor will find the real one either way.

// SCENARIO

A machine shop the way I keep finding them: CAD workstations, the software driving the CNC machines, the office PCs, and the owner's laptop, all on one small business network behind a Bell modem-router combo. One flat subnet, consumer wifi, no segmentation. The customer's drawings were reachable from every device in the building, which put every device in the building in scope. Readiness there didn't start as a paperwork exercise; it started as a network build. A real firewall at the edge, the shop floor split from the office, an enclave for the drawings, wifi moved to its own segment. The documentation came after the architecture, and it finally described something worth describing.

Asset Categories

Sort what the map found into rough bins. Systems that store, process, or transmit Specified Information are in scope, full stop. Systems that provide security functions to those systems, the domain controller, the firewall, the backup server, the AV console, ride along inside the boundary because compromising them compromises the data. Systems that connect but are kept from the data by real technical separation can sit outside, and the word doing the work in that sentence is "real." A VLAN with an any-any rule between segments is a diagram, not a separation. PSPC hasn't published scoping guidance of its own yet; the categories here follow the practice the 800-171 family has used for years, which is how a Canadian assessor will have learned to think.

Shrinking the Footprint

Almost every first map is bigger than it needs to be, which means almost every supplier can buy down their assessment with architecture instead of controls. The moves, in rough order of value:

// STUDY NOTE

The 4-percent shop from Chapter 3 ended up with an enclave: one file server, 3 workstations, a managed transfer tool for receiving drawings, and a firewall rule set I could read in one sitting. Their in-scope system count dropped from roughly 40 devices to 9. The build cost them a few weeks of an integrator's time and some licensing; the alternative was bringing 40 devices, including the owner's home laptop, to a Level 2 standard by 2027. Scoping, done this way, is the cheapest security architecture decision they'll ever make.

Consolidate storage. One project share, or one enclave file server, instead of copies scattered across personal drives. This single move usually removes more systems from scope than any other.

Contain email. Email is the great scope-spreader; every mailbox that ever received a drawing is a system holding Specified Information. Route contract data through the enclave, a managed transfer folder, or a dedicated project mailbox, and make "don't email drawings" a rule with an easy alternative attached, because rules without easy alternatives lose to deadlines every time.

Separate the enclave. A defined segment for defense work, with its own workstations or virtual desktops for the people who need them, real firewalling at its edge, and its own backup job. For a shop where defense is a minority of revenue, this turns "certify the company" into "certify the room."

Purge the echoes. Old proposals, dead projects, and departed employees' mailboxes hold Specified Information that serves nobody. Data you've defensibly deleted is data you don't protect, document, or answer for. Defensibly means after checking the contract's records retention clause, because some contract data has to be kept for years after the job, and that data gets archived into the enclave rather than deleted.

Running Your Own Gap Assessment

A spreadsheet, the standard, and a week of honest answers beat any tool you can buy at this stage.

// LEARNING OBJECTIVES

How to run a defensible internal gap assessment against ITSP.10.171, rank what it finds, and turn the result into a remediation plan with dates on it.

Before You Spend a Dollar

The readiness industry would like to sell you a platform before you know what you need, and the platforms aren't bad, they're premature. A gap assessment needs 4 things: your scope map from Chapter 6, a copy of ITSP.10.171, a spreadsheet, and access to the people who run your systems. The purpose is a truthful picture of distance: how far your real environment sits from the standard, control by control, so the remediation plan is built on facts instead of hope.

Assign it an owner. Gap assessments run by committee produce diplomatic answers; you want one person accountable for the sheet, pulling in the network admin, the MSP, and the office manager who knows where things get saved.

The Method

Build the sheet with one row per requirement, straight from ITSP.10.171's numbering so it traces cleanly later. Columns: the requirement, your current state in plain sentences, the evidence that state rests on, a status, the gap if any, and eventually an owner and a date.

Then answer each row against the scoped environment with the only test that matters: show me. Not "do we control access" but "show me the access list for the project share, today, with dates." Not "do we log" but "pull the log from last Tuesday." A control you can't demonstrate on request is a gap regardless of what the policy binder says, because "show me" is precisely the game a Level 2 assessor plays, and rehearsing it now is free.

Status in 4 bins: implemented and demonstrable; implemented but undocumented or unproven; partial; absent. The second bin is the interesting one. Most competent shops discover a third of their controls live there, real practice with no paper, and Chapter 9 exists because closing that bin is cheaper than it looks and mandatory anyway.

```
// SPEC · GAP REGISTER COLUMNS
Req ID      · ITSP.10.171 requirement number
Requirement · text, paraphrased for the sheet
Current state · plain-language description of reality
Evidence     · artifact proving the state (or "none")
Status       · demonstrable / undocumented / partial / absent
Gap          · what's missing, specifically
Fix          · remediation action
Owner · Date · one name, one deadline
```

Ranking What You Found

Not all gaps cost the same, and not all of them block you equally. Rank on 2 axes: risk to the data, and drag on certification. MFA missing on remote access is high on both axes; a policy document that exists in practice but not on paper is low risk and pure certification drag. Sequence accordingly: burn down the risky items first because they're why the program exists, then grind the documentation debt, then the long-tail process items.

Resist the urge to solve gaps in the spreadsheet as you find them. Assessment and remediation are different modes; mixing them turns a 1-week assessment into a 3-month wander, and the picture you're building loses its date.

Reading the Result

// STUDY NOTE

The most useful gap assessment I saw this year was also the ugliest: 40 percent of rows red, the owner swearing under his breath by row 30. Six months later they were the calmest client I had, because nothing an assessor could ask was going to surprise them; they'd already met every skeleton personally. The shops that frighten me are the ones whose self-assessment comes back nearly clean on the first pass. That's almost never excellence. It's almost always a scoring standard of "probably fine," and probably fine is exactly the answer "show me" is designed to destroy.

The finished register tells you your real Level 2 distance, and the honest ranges are wide. A shop with a contained scope, current infrastructure, and existing IT discipline is looking at roughly 6 months of part-time effort to demonstrable. A shop with flat networks, shared admin accounts, no logging, and data everywhere is looking at 18 months and some capital, and the number doesn't improve by being measured optimistically. Spring 2027 minus your distance is your start date; for the second shop, that math already says "now."

The Technical Work, Control Family by Control Family

Where the 98 controls bite, and the handful of failures that account for most of the findings.

// LEARNING OBJECTIVES

What each control family demands in a real environment, and which gaps show up in nearly every first assessment.

How to Read This Chapter

ITSP.10.171 organizes its requirements into 17 control families inherited from the 800-171 lineage. Each family below gets the same 4 parts. The intent is what the requirement is for. Reality is what a first assessment finds at a small shop. The work is what closes the gap. The interpretation is my reading of what the requirement is asking at a 12-to-45-computer shop, what the auditor wants to see, and where small shops over-build or under-build it. The stories in the interpretations come from real engagements, anonymized, with identifying details changed. Each family opens with its requirement identifiers, 98 in all, using ITSP.10.171's own numbering; the gaps in the numbering are the 33 identifiers NIST withdrew in Revision 3, which the Canadian document keeps as not allocated so the numbers line up across borders. The 13 requirements CPCSC Level 1 assesses are marked. Where a requirement contains a bracketed value, that's an organization-defined parameter, and chapter 4 explains who sets it. It's a field orientation rather than a substitute for the standard; implement from ITSP.10.171's text with this chapter beside it.

Access Control

Requirements: 03.01.01 Account management (Level 1) · 03.01.02 Access enforcement (Level 1) · 03.01.03 Information flow enforcement · 03.01.04 Separation of duties · 03.01.05 Least privilege · 03.01.06 Least privilege (privileged accounts) · 03.01.07 Least privilege (privileged functions) · 03.01.08 Unsuccessful logon attempts · 03.01.09 System use notification · 03.01.10 Device lock · 03.01.11 Session termination · 03.01.12 Remote access · 03.01.16 Wireless access · 03.01.18 Access control for mobile devices · 03.01.20 Use of external systems (Level 1) · 03.01.22 Publicly accessible content (Level 1).

Intent: the right people reach the right data and nothing more.

Reality: everyone in the "Engineering" group can reach everything Engineering ever made, 3 departed employees still have live accounts, and the shared "shop floor" login has been running since 2019.

The work: least privilege applied to the enclave. Role-based groups scoped to need, a joiner-mover-leaver process that fires the day someone changes roles, no shared accounts touching Specified Information, and remote access that terminates on the enclave's edge under MFA. Quarterly access reviews with a dated record turn this family from a hope into evidence.

How we can interpret it: This is the confidentiality corner of the CIA triad, and the plain reading is role-based access with least privilege. Ask what information is reachable, from where, and by whom. I've watched a multinational integrator that works in defense put everything on SharePoint with a single rule, that any technician can open anything because it might be needed. That doesn't hold up against least privilege. Two project managers on 2 different projects don't need each other's folders. The CFO doesn't need the CAD drawings. The hardware team placing components on PCBs doesn't need the source tree, and the developers don't need the board layouts. Take the tasks, build roles from them, and assign access to groups, never to individuals, even when the group holds one person. Project A developer access, project A hardware access, project A master access, with master held by the few people cleared for it. Being the owner of the company is not a role, and if the owner's account is breached, ownership is exactly the problem.

Three letters carry most of this chapter, so define them once. AAA is authentication, authorization, and accounting. Authentication proves who is at the keyboard, and the identification and authentication family owns it. Authorization decides what that person may touch, which is this family. Accounting records what they did, and the audit family owns that. A control gap in any one of the 3 shows up as a finding in the other 2, which is why an assessor who finds a shared login keeps pulling on the thread.

```
// EXAMPLE · GROUP HIERARCHY, PROJECT-BASED RBAC
ENCLAVE-USERS          membership = screening complete, training signed
  PROJ-A-ENGINEERING    CAD, drawings, BOMs (read/write)
  PROJ-A-FIRMWARE       source tree, build artifacts (read/write)
  PROJ-A-QUALITY         test records (read/write); drawings (read only)
  PROJ-A-MASTER         everything in Project A; 2 named people
ENCLAVE-ADMINS          separate admin accounts only; no mail, no browsing
BUSINESS-USERS          office network; no enclave rights
```

Rights are granted to groups, never to people.
A group with one member is still a group.
The owner sits in BUSINESS-USERS unless the role needs more.
Membership is reviewed quarterly; the review record is evidence.

Awareness and Training

Requirements: 03.02.01 Literacy training and awareness · 03.02.02 Role-based training.

Intent: people who touch the data know what it is, how to handle it, and what an attack on them looks like this year.

Reality: one onboarding video from 3 years ago, no record of who watched it, and a sales team posting shop-floor photos.

The work: annual training with a sign-off sheet as the floor, role-specific content for admins and privileged users, and 5 minutes at a toolbox talk each quarter, which does more than the video anyone can click through.

How we can interpret it: Do your people take basic security awareness training, yes or no, and does it cover operational security for this kind of environment? What to post and where, clean desk, how to build a password, what never goes in email, and why nobody puts project files in a personal Dropbox. The point is removing the "I didn't know" defense. I've seen a defense supplier post a photo for an unrelated reason with a recognizable piece of hardware in frame, which told the world that this warehouse with minimal security was holding that item right now. Nobody meant harm. The training exists so that photo never gets taken.

Audit and Accountability

Requirements: 03.03.01 Event logging · 03.03.02 Audit record content · 03.03.03 Audit record generation · 03.03.04 Response to audit logging process failures · 03.03.05 Audit record review, analysis, and reporting · 03.03.06 Audit record reduction and report generation · 03.03.07 Time stamps · 03.03.08 Protection of audit information.

Intent: when something happens, you can reconstruct it.

Reality: logs exist wherever vendors defaulted them on, retained until the disk fills, reviewed never.

The work: decide which events matter (authentication, privilege use, access to the enclave, changes to security configuration), aggregate them somewhere central even if it's a modest syslog box, retain them for a defined period, protect them from tampering, and review them on a schedule a human keeps. An assessor asking for last Tuesday needs to get last Tuesday.

How we can interpret it: This is the accounting in AAA. Who touched which file, when, from where, and whether DLP tripped when something was printed or copied to USB. The standard says a human reviews the logs on a schedule, and small shops read that as a job they can't staff. Automate the delivery instead. A weekly email carries the access log, the flagged events, and anything the DLP caught, sent to 2 people so it doesn't die when one is away. Reviewing it means replying "reviewed, 10:27 a.m., Friday, September 25" or letting the email open a help desk ticket that gets closed when read. No platform purchase. A documented process, evidence the process ran, and proof it repeats, which is the whole of compliance readiness in one sentence.

Configuration Management

Requirements: 03.04.01 Baseline configuration · 03.04.02 Configuration settings · 03.04.03 Configuration change control · 03.04.04 Impact analyses · 03.04.05 Access restrictions for change · 03.04.06 Least functionality · 03.04.08 Authorized software (allow by exception) · 03.04.10 System component inventory · 03.04.11 Information location · 03.04.12 System and component configuration for high-risk areas.

Intent: systems run in a known state and change on purpose.

Reality: golden images from 3 IT generations ago, local admin everywhere, and change control that lives in someone's memory.

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: Turn multifactor on. It isn't hard, especially on the systems that require it, and hardware keys are the option I push. A YubiKey on Windows login, or a YubiKey paired with Duo, is a combination I've deployed more than once. Then the password policy, which is where checkbox compliance lives. Write a simple policy, apply it, and expect the auditor to ask for a screenshot of the applied policy beside the written one. If they match, congratulations. If they don't, you have a problem. A weak policy that matches its documentation and meets the minimums is technically compliant, and I've told clients on ISO 27001 and PCI-DSS work that they meet the spirit of the requirement while doing something they shouldn't. Meeting the spirit is the floor.

```
// EXAMPLE · PASSWORD POLICY, ONE PARAGRAPH
Passwords on enclave systems are at least 14 characters,
screened against known-breached lists, and never reused across
systems. Accounts lock after 10 failed attempts. Multifactor
authentication is required for all remote access and all
privileged accounts. Shared accounts are prohibited on systems
holding Specified Information. Reviewed annually; owner: IT lead.
```

Incident Response

Requirements: 03.06.01 Incident handling · 03.06.02 Incident monitoring, reporting, and response assistance · 03.06.03 Incident response testing · 03.06.04 Incident response training · 03.06.05 Incident response plan.

Intent: when it goes wrong, you act instead of improvising.

Reality: a plan nobody has walked through, or no plan, and contract reporting timelines nobody has read.

The work: names, phone numbers, a definition of an incident involving Specified Information, containment steps for your actual environment, and the contract's reporting obligations with their timelines. Reporting obligations and their clocks live in your contract clauses and differ between contracts, so read yours rather than a summary. Then exercise it once a year on a tabletop, because a plan nobody has walked through is a document, and the difference shows within 10 minutes of a real event.

How we can interpret it: A plan, a reporting list, and proof you rehearsed. The tabletop is the evidence. IT and whoever else the plan names sit down, an incident is declared, and the room talks through it. Do you know who to call at your prime, and does your contract require reporting straight to National Defence or a service branch? Write it down with the protocol. Then walk a real scenario. Ransomware hits the enclave. Don't turn everything off; pull it off the network and leave the power on, because powering down loses the memory-resident evidence you'll want and a reboot can trigger the second stage of some ransomware. Once it's contained you move to eradication, and eradication depends on whether your logging can show what left the network. Rebuild the machine, restore from backup, and this is where I say it plainly. If you can show me 6 months of consistent restore testing under your own backup policy, followed to the letter, I'll buy you a coffee. I'm that confident most places don't.

// EXAMPLE · INCIDENT RESPONSE PLAN, ONE-PAGE SKELETON

1. Scope systems and data covered (the enclave, named)
 2. Definitions what counts as an incident involving Specified Information
 3. Roles incident lead, deputy, IT/MSP contact, management contact
 4. Contacts prime contractor security contact; contract-required government reporting contact; cyber insurer; legal
 5. Detection where alerts arrive (EDR, log server, user reports)
 6. Containment isolate, don't power off; preserve logs and images
 7. Eradication confirm scope via logs; rebuild affected systems
 8. Recovery restore from tested backups; verify before reconnecting
 9. Reporting what gets reported to whom, by when, per the contract
 10. Review what changed in controls afterward; register entry
- Exercise: annual tabletop, attendance and scenario recorded.

Maintenance

Requirements: 03.07.04 Maintenance tools · 03.07.05 Non-local maintenance · 03.07.06 Maintenance personnel.

Intent: control who services the systems, with what tools, from where.

Reality: the MSP's whole bench has a remote tool on every machine, and the photocopier technician has had a network drop for years.

The work: scope who may service what, route remote access through a jump host, record support sessions, and sanitize equipment before it leaves for repair. Your photocopier tech and your MSP both count.

How we can interpret it: Who maintains the systems, how, and from where. If an IT provider has remote access, do their people hold the screening the contract requires, and does every technician need access to everything? Almost never. I've had MSPs tell me "this is how we do it" while their whole bench had a remote tool on every machine. That arrangement is very hard to defend against the access control and maintenance requirements, and it isn't role-based anything. Put remote access through a jump host with MFA on the session, which 03.07.05 requires for non-local maintenance, keep admin work on separate admin workstations (03.14.09 sets a stricter bar for those, covered under system and information integrity), and never work under an admin account day to day. If a remote support tool stays, turn on session recording from the moment of login. I've seen those tools compromised and used to wipe fleets. The auditor's questions are ordinary: when was the server last touched, by whom, show the login and logout, show the patch window and what was applied. Screenshots and a basic central log server answer all of it. Nobody is asking for a SIEM.

Media Protection

Requirements: 03.08.01 Media storage · 03.08.02 Media access · 03.08.03 Media sanitization (Level 1) · 03.08.04 Media marking · 03.08.05 Media transport · 03.08.07 Media use · 03.08.09 System backup (cryptographic protection).

Intent: protected data on removable and portable media is controlled from creation to destruction.

Reality: USB sticks with engineering data in every drawer, and dead drives in a box under the bench.

The work: encrypt what moves, sanitize what leaves to a recognized method (ITSP.40.006 is the Canadian guidance; NIST SP 800-88 is the American one), destroy what dies, and keep the receipts. The USB stick culture around engineering data either ends or gets managed with encrypted, inventoried drives.

How we can interpret it: Mostly policy, with a few products. Encrypted drives such as IronKey for anything that moves, BitLocker with the TPM on anything that can be lost, and a preference for moving files through the server rather than on a stick. The audit conversation is about the end of the drive's life. It was transferred to a drive, fine, where is that drive now? "We threw it out" is not an answer. Drilled, photograph it, and know that drilling on its own isn't a recognized sanitization method under the Cyber Centre's ITSP.40.006 or NIST SP 800-88; platters still hold data around the hole. Spinning disks get degaussed or shredded, solid state gets a cryptographic erase and then the shredder, and either way it gets logged. Sent to a vendor, get the certificate of destruction. And then show it happened for every drive, not just the one you remembered. One more item that catches people: on failed drives under warranty, ask the vendor for media retention so the dead drive never leaves the building, because the replacement process otherwise ships your data back to the manufacturer.

Personnel Security

Requirements: 03.09.01 Personnel screening · 03.09.02 Personnel termination and transfer.

Intent: screen people before they get access to protected data, and pull access cleanly when they leave or move roles.

Reality: hiring paperwork in a filing cabinet HR can't find, and the last engineer to leave still has a live account.

The work: screening before enclave access, at the level the contract's security requirements call for, and an offboarding process with a checklist that HR and IT both sign. Where the contract carries Contract Security Program requirements, that screening runs through the program: the organization registers, appoints a Company Security Officer (and an alternate where the contract or the organization's size calls for one), and obtains a designated organization screening before it can be awarded work with protected information. The CSO and alternate are screened to reliability status themselves and are the only people who can request screening for anyone else.

How we can interpret it: HR gets pulled in here. At hiring, what was the process? Screening at the level the contract requires. Where the Contract Security Program applies, that's reliability status for access to Protected A or B information: a 5-year background check in which the CSO verifies identity, education, credentials, and references, plus the program's criminal record and credit checks, requested on form TBS/SCT 330-23E. Security clearances sit above reliability status for classified work. Read the contract's security requirements checklist to know which level applies, because Specified Information doesn't automatically mean Protected. Nobody touches project files until the checks come back. The auditor samples, picking 3 names from the access list and asking for their paperwork. Then the exit, which is the bigger failure. The last person to leave the project, show me their account. Why is it still active? Disable it, freeze the mailbox, forward the mail, don't log in as them, and preserve everything in case it turns litigious. HR notifies IT inside a set number of hours, the badge is collected, card access is pulled, the laptop comes back and gets wiped. Letting someone keep a device is where personal and work mixing hurts most, because the remote wipe takes the family photos with it.

Physical Protection

Requirements: 03.10.01 Physical access authorizations (Level 1) · 03.10.02 Monitoring physical access · 03.10.06 Alternate work site · 03.10.07 Physical access control (Level 1) · 03.10.08 Access control for transmission.

Intent: the hardware holding protected data sits behind physical access control with a short key list.

Reality: the server closet is also the janitor's closet.

The work: a lock with a short key list, a visitor log and escort rule, cameras on entries and main routes, and held-open alarms on the enclave door.

How we can interpret it: Keys work, but I recommend access control because it produces a record. Card or biometric over a PIN, since a PIN can be known and a finger is harder to borrow. The simplest things make an auditor happy: employee ID on a navy lanyard, screened contractors on yellow, visitors on red, and a card design that shows division at a glance. Held-open alarms on the enclave door, which is a checkbox on most controllers. Cameras on the main routes, and know the difference between a camera that shows someone is there and one that identifies a face, which is why thermal doesn't identify and bispectral can. Anti-passback and tailgating controls scale with the risk, from a sign to a turnstile to a two-door vestibule. For credentials, I'd set the floor at 13.56 MHz Seos or iCLASS SE with custom keys (HID's Elite program or equivalent), not the standard keyset, in a corporate format such as HID Corporate 1000 or 2000. HID's February 2024 advisories (CVE-2024-23806) showed keys could be pulled from iCLASS SE configuration cards and encoders, so readers should be on current firmware with configuration-card changes locked out, legacy and 125 kHz technologies disabled at the reader to stop downgrade attacks, and OSDP Secure Channel between reader and controller. Card plus PIN on the doors that matter. Match all of it to what you make. A washer supplier on a defense program is a defense contractor, and doesn't need a scramble pad.

```
// CHECKLIST · PHYSICAL SECURITY, QUICK AUDIT
[ ] Enclave hardware behind a lockable door with a short key or card list
[ ] Held-open and forced-door alarms enabled on enclave doors
[ ] Visitor log, escort rule, and coloured lanyards in use
[ ] Cameras cover entries and main routes; recording verified this month
[ ] At least one identification-quality camera at the enclave entry
[ ] Seos or iCLASS SE with custom keys; legacy and 125 kHz disabled at the reader
[ ] Card plus PIN on high-security doors (server room, secure storage)
[ ] Anti-passback or tailgating control matched to the site's risk
[ ] Contractor and cleaner access documented and time-limited
[ ] Exit process pulls card access the same day
```

Risk Assessment

Requirements: 03.11.01 Risk assessment · 03.11.02 Vulnerability monitoring and scanning · 03.11.04 Risk response.

Intent: assess risk to the protected data periodically, scan for vulnerabilities on a cycle, and fix what the scans find inside a defined window.

Reality: a penetration test bought before a single vulnerability scan was run, and a report nobody actioned.

The work: scan the enclave on a cycle with proper tools, rank the findings, fix inside a defined window, and record the next scan date. Progress is what the assessor wants to see.

How we can interpret it: Have someone assess risk, run vulnerability scans with proper tools, and show progress: last scan, results, what's remediated, next scan date. Progress is what the auditor wants to see. Two things I hate here. Jumping straight to a penetration test before a single vulnerability scan has been done, which helps nobody. And MSPs running a sales-oriented assessment tool and calling it a security assessment. It may tick the box, and it is still a sales tool. Your IT provider also shouldn't be assessing its own work, because some won't tell on themselves. Keep the assessment at arm's length, audit the switch and firewall configurations with something like rConfig or Nipper, and treat any provider that hides behind "proprietary" or refuses config access as a red flag.

Security Assessment and Monitoring

Requirements: 03.12.01 Security assessment · 03.12.02 Plan of action and milestones · 03.12.03 Continuous monitoring · 03.12.05 Information exchange.

Intent: check that the controls work, plan and track the fixes, and keep watching.

Reality: the gap register archived the day it was finished.

The work: keep the Chapter 7 register alive, review it on a schedule, update it when the environment changes, and track the remediation tail to completion. This is where the system security plan and the register live.

How we can interpret it: Always double-check the provider's work. If an MSP says "we do vulnerability management for you" or "our tool says you're secure," verify it with your own scan and your own read of the configs. Monitoring comes back to logging and endpoint protection, and the remediation register stays alive rather than archived.

System and Communications Protection

Requirements: 03.13.01 Boundary protection (Level 1) · 03.13.04 Information in shared system resources · 03.13.06 Network communications, deny by default, allow by exception · 03.13.08 Transmission and storage confidentiality · 03.13.09 Network disconnect · 03.13.10 Cryptographic key establishment and management · 03.13.11 Cryptographic protection · 03.13.12 Collaborative computing devices and applications · 03.13.13 Mobile code · 03.13.15 Session authenticity.

Intent: the network architecture itself defends the data.

Reality: one flat subnet behind a consumer router, and a guest wifi that is a different SSID and nothing else.

The work: a real boundary with deny-by-default rules at the edge, encryption for Specified Information in transit and wherever it's stored, which 03.13.08 requires on servers, laptops, backups, and portable media alike, separation between the enclave and everything else that isn't just a different SSID, and DNS and remote access paths you can draw. If your firewall rule set can't be explained to an assessor in one sitting, it can't be defended in one either.

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

MPLS, with VPN encryption on top. And the workstation is a hardened, single-purpose machine or thin client that isn't shared between security realms. The discussion in the standard goes further than most shops expect: the workstation isn't domain-joined, doesn't download patches from the internet, carries no office tools, and isn't used to update documentation in networked applications.

For a 20-person shop that means one admin machine, kept off the internet, patched from media you bring to it, and used for nothing but administering the enclave; admin accounts work from that machine and from nowhere else. The remote clause is the hard part. An MSP administering your enclave from its own office over an internet VPN doesn't meet the requirement as written, and a carrier private network to every client is not how most MSPs are built. This is a Level 2 requirement, it's new, and the assessment method hasn't been published... so read the text yourself, keep administrative work inside the enclave wherever you can, and get your assessor's reading in writing before you buy circuits.

Planning

Requirements: 03.15.01 Policy and procedures · 03.15.02 System security plan · 03.15.03 Rules of behaviour.

Intent: the system security plan exists, describes the real environment and boundary, and gets updated when the environment changes; rules of behaviour for users are written down.

Reality: no SSP, or a template one describing a company that doesn't exist.

The work: write the SSP skeleton first (Chapter 9), have users sign rules of behaviour on hire and annually, and wire the review trigger into change control.

How we can interpret it: This family is the paper that holds the rest together. The system security plan describes the network as it exists, with the diagram, and changes when the network changes. Every family gets a written policy and the procedure that carries it out, and users sign rules of behaviour before they touch the enclave. Baselines, the thing I reach for first, live under configuration management; the plan points at them rather than repeating them.

System and Services Acquisition

Requirements: 03.16.01 Security engineering principles · 03.16.02 Unsupported system components · 03.16.03 External system services.

Intent: security is considered when systems and services are bought or built, including what external providers are responsible for.

Reality: gear bought from whoever was cheapest that week, with no record of where it came from.

The work: a documented buying path for anything entering the enclave, provider responsibilities captured in the matrix, and a software bill of materials for anything you develop.

How we can interpret it: Where does everything come from? New or used, genuine or grey market, first-party or third-party optics, and whether criticality or a support contract such as SmartNet forces genuine parts. The same question for cloud services. Is the MSP vetted, do you buy through them, is there a bidding process, and is it all written down? For anything you develop, keep a software bill of materials so you know who maintains every package, especially the open source ones. And check NDAA-style vendor restrictions flowed down by American primes before buying cameras or components from a restricted brand.

Supply Chain Risk Management

Requirements: 03.17.01 Supply chain risk management plan · 03.17.02 Acquisition strategies, tools, and methods · 03.17.03 Supply chain requirements and processes.

Intent: know who is in your supply chain for the in-scope systems, assess the risk they bring, and flow requirements down where protected data flows down.

Reality: subcontractors receiving drawings with no clause attached and no questions asked.

The work: an inventory of who touches in-scope systems and data, flow-down language in subcontracts, and evidence that the process repeats.

// WARN

Every family above generates evidence or it generates findings; there's no third state. As you implement, capture the artifact in the same motion: the config export, the review record, the training sheet, the patch report. Retrofitting a year of evidence in the month before an assessment is the specific misery Chapter 9 exists to prevent.

How we can interpret it: Document the process for getting a PC, a switch, a camera, or a cloud seat into the enclave, show the process repeats, and show the evidence. Documented, documented as done, and repeatable.

Documentation That Survives an Assessor

A perfect environment with paper that doesn't match it still fails.

// LEARNING OBJECTIVES

What the documentation stack contains, how to write a system security plan that describes your real environment, and how to keep evidence without drowning in it.

The Stack, Smallest to Largest

Four layers, each answering a different question. Policies say what the organization requires: short, stable, signed by someone with authority. Procedures say how it's done here: specific to your systems, owned by the people who do the work. The system security plan says what exists: your scope, your architecture, and how each requirement is met in your environment. Evidence says it's true: the dated artifacts proving the controls operate. Assessments fail in the seams between layers, when the policy promises what no procedure delivers, or the SSP describes an environment the evidence contradicts.

Write in this order: SSP skeleton first, because it forces the scope and architecture decisions; procedures next, from the people who do the work; policies last, as short ratifications of what the procedures already say. The common order, policies first from a template pack, produces a binder describing a fictional company, and assessors have read that binder a hundred times.

The System Security Plan

The SSP is the document the assessment orbits, and the standard for it is unglamorous: accurate. It names the scope and draws the boundary, includes the network diagram that matches the actual network, describes the environment in plain language, and then walks the requirements stating how each is met, by which mechanism, on which systems, or noting where a plan of action stands instead.

Two properties separate a working SSP from a liability. Specificity: "access to the project share is restricted to the DefenceEng group, reviewed quarterly, record retained in the evidence folder" survives contact with an assessor; "access is restricted per policy" invites the next question with nothing behind it. Every organization-defined parameter you chose gets written down in the same place, with the value and the reason, because "reviewed quarterly" is a decision the assessor will want to see you made on purpose. Currency: the SSP gets a version number, a change log, and a review trigger wired to environment changes, because an SSP describing last year's network is worse than no SSP; it's documented inaccuracy.

// WARN

Don't buy a 200-page SSP from a template mill and find-and-replace your company name into it. Assessors recognize the products on sight, the text promises controls you've never operated, and every promise becomes a finding. A 40-page SSP that's true beats a 200-page SSP that's aspirational, every single time.

// CHECKLIST · POLICY INVENTORY

- [] Password and authentication (length, MFA, lockout, rotation rules)
- [] Account management (joiner, mover, leaver; privileged accounts)
- [] Access review (cadence, owner, record retained)
- [] Acceptable use (personal devices, personal browsing on enclave systems)
- [] Incident response (definition, contacts, containment, contract reporting)
- [] Media handling (encryption, transport, sanitization, destruction receipts)
- [] Physical security (enclave hardware, key control, visitor handling)
- [] Configuration and change management (baselines, approval, record)
- [] Vulnerability and patch management (scan cadence, fix windows, exceptions)
- [] Logging and monitoring (events captured, retention, review cadence)
- [] Security awareness and training (annual, sign-off, role-specific)
- [] Personnel security (screening to contract requirements, offboarding)
- [] Vendor and MSP responsibility (matrix, deliverables, remote access)
- [] Backup and recovery (scope, frequency, restore testing)

The Remediation Register

Gaps in progress live in a plan of action: the gap, the fix, the owner, the date, and the interim risk story. Its credibility comes from motion; a register whose dates keep sliding right tells an assessor about your organization more clearly than any interview. Keep it honest, keep it short, and close items with the evidence attached. PSPC had not published Level 2's rules for gaps found at assessment when this edition closed: whether a supplier can be certified with open items under a plan of action and milestones (a POA&M), which requirements would be eligible, or how long it would have to close them. CMMC allows limited POA&Ms closed within 180 days. Don't assume Canada will match that; plan to walk into the assessment with nothing open.

Evidence Without Drowning

The usual failure mode is an unnavigable pile of evidence rather than too little of it. Structure the folder by requirement number, one subfolder per control, artifacts dated, a one-line index at the top. Capture evidence as a by-product of operating: the quarterly access review generates its record when it runs, the patch cycle exports its report when it completes. If evidence collection is a separate activity someone must remember, it stops the first busy month; if it's the exhaust of the process, it accumulates on its own.

// STUDY NOTE

I reviewed 2 binders in the same month last year. The first was 300 pages, professionally formatted, and described a company that has never existed on this earth. The second was a shared drive holding a 35-page SSP with a hand-drawn-then-redrawn network diagram, procedures written by the actual admin with the actual server names, and an evidence tree organized by requirement. The second shop thought they were behind because their documents weren't pretty. They were the most assessable organization I saw all year. Pretty counts for nothing with an assessor. What they grade is whether it's true.

Refresh discipline beats volume. One current artifact per control, plus the periodic records your procedures generate, is a defensible position. Three-year-old screenshots prove only that the control worked once, during a different government.

Level 2 Prep: What Third-Party Assessment Looks Like

What hurts in a Level 2 assessment is the surprise you hadn't found yourself.

// LEARNING OBJECTIVES

How the Level 2 assessment process runs, what assessors sample and ask, and how to schedule backward from spring 2027.

The Assessment Machinery

Level 2 assessments are conducted by certification bodies accredited through the Standards Council of Canada, using assessors certified under the program, on a 3-year certification cycle with annual affirmations between. The assessor market is still forming as this edition goes to print, which cuts 2 ways for you: limited choice and unproven queues on one hand, and on the other, the suppliers who engage early will meet assessors who have time to do the work carefully. Late 2026 and 2027's first movers set the norms everyone else inherits. The list of accredited certification bodies, the assessment methodology, and the fee structures were still being established at press time; the process described here follows the announced program structure and the way accredited certification bodies already work under other schemes.

Expect the engagement to run in phases: a scoping and contracting phase where the boundary you defined in Chapter 6 gets agreed; a documentation review where the SSP and its stack get read before anyone visits; the assessment proper, on site or hybrid, built from evidence sampling and interviews; and a findings and disposition phase. The boundary conversation is worth real preparation, because a scope you can't defend gets widened for you, and every widening is money.

// WARN

Everything in this chapter about assessment mechanics describes the announced structure, since the methodology hadn't been published. Check hans.study/cpsc for the current certification body list, methodology, and fee information before you book anything.

What Assessors Do

They sample and they triangulate. For a given requirement, the pattern is consistent: read what the SSP claims, ask the person responsible to explain what happens, then ask for the artifact that shows it happening. Three sources, one truth test. When the 3 agree, the requirement is quickly satisfied and everyone moves on. When they diverge, the pulling starts, and adjacent requirements get pulled too, because divergence is a signal about the organization rather than the control.

Interviews reach past the IT staff. The engineer who handles drawings daily, the office manager who onboards new hires, the shop lead whose crew touches the enclave workstations: expect them to be asked what the data is, how they handle it, and what they'd do if something looked wrong. Their answers reveal whether your program is operational or laminated. Prep them with truth, not scripts; coached answers collapse under the second follow-up question, and assessors ask second follow-up questions professionally.

The Common Findings

First-cycle findings cluster tightly, and the cluster is Chapter 8's greatest hits: MFA gaps on secondary access paths, log review that exists on paper only, access lists with ghosts on them, SSP claims the evidence can't back, remediation registers with sliding dates, and scope leaks, Specified Information found living outside the boundary everyone agreed on. Every one of these is findable in advance by your own "show me" pass. A finding you discover in your own rehearsal is a task; the same finding discovered by the assessor is a result.

The Calendar Math

Work backward from the contract you want. If Level 2 clauses reach solicitations you care about in spring 2027, and the assessment engagement takes a quarter end to end, and your remediation tail is 6 to 18 months by Chapter 7's honest reckoning, then the start dates land between "already" and "immediately" for most shops reading this. Add queue risk in a forming assessor market and the margin thins further. The suppliers who treat spring 2027 as the date to be finished, rather than the date to start worrying, are the ones who'll bid that season.

```
// SPEC · BACKWARD SCHEDULE, SPRING 2027 TARGET
Contract-ready:      Q2 2027
Assessment complete: Q1 2027
Assessment engaged:  Q4 2026 (book the CB early)
Rehearsal pass:      Q3-Q4 2026
Remediation tail:    now to Q3 2026 (or longer; see gap register)
Gap assessment:      now
```

Small Shop Realities: MSPs, Cloud, Cost, and Sequencing

The program was designed with the whole supply chain in mind. The whole supply chain is mostly companies with 8 to 80 people.

// LEARNING OBJECTIVES

How to run a readiness program without a security department, what the MSP relationship has to become, and how cloud choices interact with Canadian contracts.

You Without a Security Team

// SCENARIO

The full arc, compressed. A small manufacturer on a consumer modem-router combo, CAD and CNC control software mashed onto one network with the office. Over 2 quarters: scope map first, then a real firewall and segmentation, an enclave for customer technical data, MFA and backups sorted, and then the documentation pass, SSP, policies, procedures, and evidence folder, written against the network as rebuilt rather than the network as remembered. Technical readiness and documentation readiness were 2 halves of the same engagement, and neither would have passed anything alone.

A small supplier's advantage in this program is real and underused: the environment is knowable. Twelve workstations, one server rack, one cloud tenant, and the person who knows where everything is sits 20 feet away. Scoping that takes a prime 6 months takes you an afternoon. The disadvantage is capacity, since nobody's job is this and it becomes everybody's someday task, and someday has a habit of arriving as a bid deadline.

The fix is structural, and it's cheap. One named owner, even at 4 hours a week. A standing monthly hour where the gap register gets reviewed and dates get honest. Evidence generated as exhaust from the register's processes, per Chapter 9. That cadence, held for a year, outperforms any burst of compliance enthusiasm, because certification rewards the boring accumulation of true things.

The MSP Relationship Grows Up

Most small suppliers will meet Level 2 through their managed service provider, and the relationship as it usually exists isn't ready. "They handle our IT" is not a control description. What the program forces into existence is a responsibility matrix: requirement by requirement, who operates the control, who holds the evidence, and who answers the assessor. The MSP patches, the MSP runs the firewall, the MSP holds the logs; fine, then the MSP produces the patch reports, the rule set review, and the log samples, on a schedule, as deliverables, in the contract.

Have that conversation early and in writing, because it surfaces 2 uncomfortable discoveries at a survivable moment. Some MSPs can't support this work; better to learn that in 2026 than mid-assessment. And your MSP's own security posture is inside your risk story; their remote access into your enclave is one of your attack paths, and an assessor will treat it as exactly that. Ask them the questions you're learning to answer. The good ones have answers ready, and increasingly, marketing built on them.

// EXAMPLE · SHARED RESPONSIBILITY MATRIX, SAMPLE ROWS

Requirement	Operates	Evidence held by	Deliverable / cadence
Patch management	MSP	MSP	patch report, monthly
Firewall rule set	MSP	MSP + client copy	rule review, quarterly
Log collection/review	MSP	client mailbox	weekly log digest
Access reviews	Client	Client	review record, quarterly
MFA enrolment	MSP	Client	enrolment list, on change
Backup and restore test	MSP	MSP + client copy	restore test log, quarterly
Awareness training	Client	Client	sign-off sheet, annual
Incident reporting	Client	Client	per contract

Cloud, Sovereignty, and the Fine Print

Cloud is usually the right answer for a small supplier; managed identity, logging, and encryption arrive as configuration rather than construction. Two cautions keep it the right answer. Configuration is still yours: the tenant's defaults are not the standard's requirements, and "it's in the cloud" has never once satisfied an assessor. And Canadian contracts bring Canadian data governance: expectations about where Specified Information resides and who can access it, expressed contract by contract. An architecture that sailed through an American assessment can need rework under Canadian clauses. Read the data handling requirements in each solicitation before assuming your tenant's region settings are anyone's problem but yours. Contract language on data residency and cloud hosting of Specified Information was still settling as of this printing, and it differs between contracts.

What This Costs

Precise figures would be invented, so here are the shapes. Level 1 costs attention: an afternoon of scoping, a day of evidence, remediation measured in days if your basics are sound. Level 2 costs a program: months of part-time internal effort against the gap register, some capital where the architecture needs the enclave built or MFA licensed, MSP deliverables that will show up on the invoice, and the assessment engagement itself, priced by a market that's still forming. The register from Chapter 7 is your only honest estimator; anyone quoting you a number before seeing your scope is quoting their margin, not your cost.

// STUDY NOTE

The owner's laptop is where small-shop scoping goes to die. Every shop has the folder; it's named "DND stuff" or "Project X" or just "Drawings," it lives on the machine that also does the banking and the kids' homework, and it's synced to a personal cloud account for convenience. Nobody wants to tell the owner their laptop is in scope, so the map omits it, and the enclave is fiction from day one. Tell the owner. I've had that conversation a dozen times this year; it's 5 awkward minutes, the fix is a managed workstation and a habit change, and it beats an assessor finding the folder in minute 20 of the first interview.

Spend in this order: scoping first because it divides every later cost, the risky gaps second because they're the point, documentation third, tooling last and only where a register line demands it. Inverting that order is the \$40,000 mistake from the preface, and it's popular.

Staying Certified: Life After the First Attestation

The certificate captures one day; the affirmations ask about every day after it.

// LEARNING OBJECTIVES

What the annual cycle requires, what changes re-open your scope, and how to keep the program alive between assessments.

The Recurring Clocks

Every level carries an annual clock. Level 1 re-attests each year through CanadaBuys. Level 2 files an annual affirmation between 3-year assessments, a signed statement that the certified posture still holds. The affirmation is quick to file and slow to earn: signing it requires knowing your environment still matches the SSP, your controls still generate evidence, and your remediation register hasn't fossilized. Calendar the clocks, and calendar the month of verification before each one; the signature ceremony is the last step of a review, not a replacement for it.

What Re-Opens Scope

Environments move, and 4 kinds of movement reach your certification. New systems touching Specified Information: a workstation added to the enclave, a new cloud service adopted by engineering, a file transfer tool someone found useful. Organizational change: a new site, an acquisition, a merger, a new MSP. New contracts, whose clauses may name different levels or different handling requirements than the ones you built for. And departures of the load-bearing people, because a program that lived in one person's head leaves with them.

Wire the triggers into processes that already exist. The change control record from Chapter 8 gets one added question: does this touch the enclave? Procurement gets one: does this contract carry Specified Information clauses? Onboarding and offboarding get the access and knowledge-transfer steps. Continuous compliance comes down to 4 questions added to 4 existing routines.

Incidents and Obligations

An incident touching Specified Information activates the reporting obligations in your contract, on the contract's timeline, alongside whatever breach obligations already apply to you. Know both before you need them; the middle of an incident is a bad time to discover a 72-hour clause. After the incident, the program logic continues: containment and recovery per your Chapter 8 plan, then an honest look at whether the affected controls need to change, recorded in the register, because the assessor at your next cycle will ask what happened and what you did about it, and "we fixed the control and here's the record" is the strong answer.

Watching the Program Move

CPCSC will not hold still. Level 2 clauses arrive in 2027, Level 3 details are still emerging, conditional certification rules weren't public at this printing, and the mutual recognition question with CMMC stays open. Assign the watching to your program owner: the PSPC program page quarterly, your prime's flow-down bulletins as they arrive, and your contracts as they renew. This book's companion pages at hans.study/cpcsc carry the current program state with a verification date, precisely because a printed book can't chase a moving program, and pretending otherwise would break the series' one rule about telling you the truth.

The posture worth building toward, and the note this book ends on, is quiet: an environment where the controls run because they're how work gets done, evidence accumulates because processes exhale it, and the annual signature is boring. The suppliers who get there stop experiencing CPCSC as a compliance program; it becomes a Tuesday, which is where this book started.

Appendix A: Level 1 Readiness Checklist

The 13 requirements CPCSC Level 1 assesses, by ITSP.10.171 identifier, with the evidence an assessor's examine, interview, and test methods will reach for. Work the preparation items first; they decide what the 13 are assessed against.

// CHECKLIST · LEVEL 1 PREPARATION

- [] Contracts reviewed for Specified Information clauses
- [] Data flow mapped; system boundary drawn and dated
- [] Evidence folder started, one subfolder per requirement below
- [] Active CanadaBuys account and supplier profile
- [] Self-assessment completed; results page with expiry date saved
- [] Result and expiry date confirmed in the CanadaBuys profile questionnaire
- [] Proof attached to bids requiring Level 1; renewal calendared

// CHECKLIST · LEVEL 1 REQUIREMENTS AND EVIDENCE

- [] 03.01.01 Account management account list with owners; disable/notify periods set
- [] 03.01.02 Access enforcement group permissions on enclave shares; screenshots
- [] 03.01.20 Use of external systems policy on personal and external systems; agreements
- [] 03.01.22 Publicly accessible content review record of website and social posts
- [] 03.05.01 User identification and authentication unique IDs; no shared logins; re-auth rules
- [] 03.05.02 Device identification device list; 802.1X or equivalent where used
- [] 03.05.03 Multi-factor authentication MFA enrolment list, privileged and non-privileged
- [] 03.08.03 Media sanitization sanitization and destruction log with evidence
- [] 03.10.01 Physical access authorizations approved access list; review date; removals
- [] 03.10.07 Physical access control door control, visitor log, key control, output devices
- [] 03.13.01 Boundary protection firewall rule set; managed interfaces; segmentation
- [] 03.14.01 Flaw remediation patch windows defined; patch reports
- [] 03.14.02 Malicious code protection endpoint console: current, scanning, blocking

Appendix B: Terminology Translation, Canada and the US

The same ideas carry different names on each side of the border, and documentation written for one program reads wrong to an assessor on the other. The table pairs them. Where a Canadian term has no exact American equivalent, the nearest working counterpart is given.

Canada (CPCSC)	United States (CMMC)	What it is
Specified Information (SI)	Controlled Unclassified Information (CUI)	Sensitive but unclassified government data identified in a contract as needing safeguarding on supplier systems
No separate category; ordinary contract information falls under the same clauses	Federal Contract Information (FCI)	Information provided by or generated for the government under contract, not for public release; the CMMC Level 1 data class
CPCSC	CMMC	The certification program
Public Services and Procurement Canada (PSPC)	Department of Defense, now Department of War	Program owner
Department of National Defence (DND)	DIBCAC and the DoD CIO	Government-led assessment at the top level
Canadian Centre for Cyber Security (Cyber Centre, part of CSE)	NIST	Author of the technical standard
ITSP.10.171	NIST SP 800-171	The control standard; ITSP.10.171 adapts Revision 3
ITSP.10.033 (successor to ITSG-33 Annex 3A)	NIST SP 800-53 Revision 5	The full control catalogue the standard is tailored from
Level 1 criteria (Canadian version of 800-171A Revision 3)	NIST SP 800-171A	Assessment procedures: determination statements, examine, interview, test
No separate Canadian document published yet; CPCSC Level 3 adapts these directly	NIST SP 800-172	Enhanced requirements for higher-sensitivity work; the source of Level 3's controls beyond the 98
Standards Council of Canada (SCC)	Cyber AB (the CMMC Accreditation Body)	Accredits the assessors
Accredited certification body	C3PAO (CMMC Third-Party Assessment Organization)	Performs third-party assessments
Annual affirmation	Annual affirmation by an affirming official	The yearly signed statement between assessments
CanadaBuys supplier portal	SPRS (Supplier Performance Risk System)	Where attestations and assessment results are filed

Canada (CPCSC)	United States (CMMC)	What it is
Contract clauses in the RFP and contract	DFARS 252.204-7021 (clause) and 252.204-7025 (provision)	How the required level reaches a contract
Contract Security Program (PSPC)	NISPOM and the Defense Counterintelligence and Security Agency	Personnel screening and facility security regime
Company Security Officer (CSO)	Facility Security Officer (FSO)	The named security role inside the supplier
Criminal record and judicial matters check	Background investigation	The personnel check behind screening
Controlled Goods Program (CGP)	ITAR and EAR	Controls on possession and transfer of controlled technical data; separate from cyber certification
Treasury Board Secretariat policy; PIPEDA	FAR and DFARS; US privacy frameworks	The policy and privacy references the standard points at
Not allocated (identifier retained)	Withdrawn (Revision 3)	Requirement numbers removed in Revision 3 and kept in the Canadian numbering for interoperability
Organization-defined parameter (ODP)	Organization-defined parameter (ODP)	The bracketed value the organization sets unless a contract specifies it
Level 1: 13 requirements, self-assessed	Level 1: 15 requirements, self-assessed	Basic safeguarding
Level 2: 98 requirements, third party	Level 2: 110 requirements, self or C3PAO per solicitation	The main tier
Level 3: 130-plus requirements, DND	Level 3: 110 plus 24 from SP 800-172, government-assessed	The top tier

Counts reflect NIST SP 800-171 Revision 2 (110) on the CMMC side and ITSP:10.171, the Canadian version of Revision 3 (98), on the CPCSC side.

Appendix C: Primary Sources and Where the Current State Lives

PSPC, Canadian Program for Cyber Security Certification: program overview, Level 1 announcement and back-grounder, and program evaluation report (canada.ca). Canadian Centre for Cyber Security, ITSP.10.171, Protecting Specified Information in Non-Government of Canada Systems and Organizations, second release, October 28, 2025. Standards Council of Canada, certification body accreditation materials. PSPC, How to meet Level 1 cyber security certification requirements, the online Level 1 self-assessment tool, and the CPCSC Level 1 Scoping Guide. For the US side: 32 CFR Part 170, the 48 CFR CMMC acquisition rule, DFARS 252.204-7012, -7021, and -7025, and DoD CIO CMMC program materials.

Living companion pages, with the current program state and a last-verified date: hans.study/cpcsc and hans.study/cpcsc-vs-cmmc.

Appendix D: Templates and Examples

The examples in the chapters, the change request record, the password policy paragraph, the physical security checklist, the group hierarchy, the incident response skeleton, and the responsibility matrix, are collected on the companion site as editable templates. The records below round out the set. Each is a working shape, sized for a small shop, to be adjusted to your contract rather than copied as-is.

```
// TEMPLATE · ACCESS REVIEW RECORD
Review date:      2026-10-03      Reviewer: (name, role)
Scope:           ENCLAVE-USERS and all PROJ-* groups
Method:          group membership export compared to HR active list
Findings:        1 departed employee still in PROJ-A-QUALITY (removed same day)
                 1 contractor account past end date (disabled)
Changes made:    listed with ticket numbers
Next review:     2027-01-05
Signed:          (name)           Evidence: export attached
```

```
// TEMPLATE · OFFBOARDING CHECKLIST
[ ] HR notifies IT within (X) hours of departure decision
[ ] Accounts disabled (not deleted); password reset; sessions revoked
[ ] Mailbox frozen; forwarding set per policy; no logins as the user
[ ] Removed from all groups; group export saved as evidence
[ ] Card access revoked; badge and keys collected
[ ] Laptop, phone, tokens returned; devices wiped or reimaged
[ ] Personal-device access removed (mail, VPN, cloud)
[ ] Clearance sponsor notified where the contract requires it
[ ] Checklist signed by IT and HR; filed with the date
```

```
// TEMPLATE · MEDIA SANITIZATION AND DESTRUCTION LOG
```

Date	Asset / serial	Media type	Data class	Method	Verified by
Evidence					
2026-09-12	FS01-HDD2 / WX41...	3.5" HDD	SI	degauss+shred	(name)
photo, cert #					
2026-09-12	USB-07	flash	SI	crypto erase	(name)
tool log					

// TEMPLATE · BACKUP RESTORE TEST LOG

Date	System	Restore point	Method	Result	Time to restore
------	--------	---------------	--------	--------	-----------------

Tested by

2026-09-20	FS01	2026-09-19	full VM restore	pass	42 min
------------	------	------------	-----------------	------	--------

(name)

2026-09-20	PROJ share	2026-09-18	file-level restore	pass	6 min
------------	------------	------------	--------------------	------	-------

(name)

Next test: 2026-12-20. Backup policy: 3 copies, 2 media types, 1 offsite.

// TEMPLATE · SYSTEM SECURITY PLAN, OUTLINE

1. System name, owner, and purpose
2. Scope and boundary (what is in, what is out, and why)
3. Network diagram (matches the running network; dated)
4. Asset inventory (in-scope systems, security protection assets)
5. Data flows for Specified Information (arrive, rest, work, leave, echo)
6. Roles and responsibilities (including MSP and cloud, with the matrix)
7. Control implementation, requirement by requirement: how, where, evidence
8. Open items: remediation register reference
9. Change log and review triggers

// EXAMPLE · ACCEPTABLE USE, ONE PARAGRAPH

Enclave systems are for contract work only. No personal email, browsing, messaging, or file sync on enclave workstations. Specified Information stays on enclave systems and the approved transfer tool; never on personal devices, personal cloud accounts, or unencrypted removable media. Report lost devices and suspected incidents to the incident lead the same day. Signed on hire and annually; violations handled under HR policy.

Appendix E: ITSP.10.171 Requirement Index

All 98 requirements by family and identifier, for use as a gap register spine or an evidence folder structure. The 13 Level 1 requirements are marked (L1) and set in orange. Not allocated identifiers are omitted.

// INDEX • ACCESS CONTROL

- [] 03.01.01 Account management (L1)
- [] 03.01.02 Access enforcement (L1)
- [] 03.01.03 Information flow enforcement
- [] 03.01.04 Separation of duties
- [] 03.01.05 Least privilege
- [] 03.01.06 Least privilege (privileged accounts)
- [] 03.01.07 Least privilege (privileged functions)
- [] 03.01.08 Unsuccessful logon attempts
- [] 03.01.09 System use notification
- [] 03.01.10 Device lock
- [] 03.01.11 Session termination
- [] 03.01.12 Remote access
- [] 03.01.16 Wireless access
- [] 03.01.18 Access control for mobile devices
- [] 03.01.20 Use of external systems (L1)
- [] 03.01.22 Publicly accessible content (L1)

// INDEX • AWARENESS AND TRAINING

- [] 03.02.01 Literacy training and awareness
- [] 03.02.02 Role-based training

// INDEX • AUDIT AND ACCOUNTABILITY

- [] 03.03.01 Event logging
- [] 03.03.02 Audit record content
- [] 03.03.03 Audit record generation
- [] 03.03.04 Response to audit logging process failures
- [] 03.03.05 Audit record review, analysis, and reporting
- [] 03.03.06 Audit record reduction and report generation
- [] 03.03.07 Time stamps
- [] 03.03.08 Protection of audit information

// INDEX · CONFIGURATION MANAGEMENT

- [] 03.04.01 Baseline configuration
- [] 03.04.02 Configuration settings
- [] 03.04.03 Configuration change control
- [] 03.04.04 Impact analyses
- [] 03.04.05 Access restrictions for change
- [] 03.04.06 Least functionality
- [] 03.04.08 Authorized software (allow by exception)
- [] 03.04.10 System component inventory
- [] 03.04.11 Information location
- [] 03.04.12 System and component configuration for high-risk areas

// INDEX · IDENTIFICATION AND AUTHENTICATION

- [] 03.05.01 User identification, authentication, and re-authentication (L1)
- [] 03.05.02 Device identification and authentication (L1)
- [] 03.05.03 Multi-factor authentication (L1)
- [] 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

// INDEX · INCIDENT RESPONSE

- [] 03.06.01 Incident handling
- [] 03.06.02 Incident monitoring, reporting, and response assistance
- [] 03.06.03 Incident response testing
- [] 03.06.04 Incident response training
- [] 03.06.05 Incident response plan

// INDEX · MAINTENANCE

- [] 03.07.04 Maintenance tools
- [] 03.07.05 Non-local maintenance
- [] 03.07.06 Maintenance personnel

// INDEX · MEDIA PROTECTION

- [] 03.08.01 Media storage
- [] 03.08.02 Media access
- [] 03.08.03 Media sanitization (L1)
- [] 03.08.04 Media marking
- [] 03.08.05 Media transport
- [] 03.08.07 Media use
- [] 03.08.09 System backup (cryptographic protection)

// INDEX · PERSONNEL SECURITY

- [] 03.09.01 Personnel screening
- [] 03.09.02 Personnel termination and transfer

// INDEX · PHYSICAL PROTECTION

- [] **03.10.01 Physical access authorizations (L1)**
- [] 03.10.02 Monitoring physical access
- [] 03.10.06 Alternate work site
- [] **03.10.07 Physical access control (L1)**
- [] 03.10.08 Access control for transmission

// INDEX · RISK ASSESSMENT

- [] 03.11.01 Risk assessment
- [] 03.11.02 Vulnerability monitoring and scanning
- [] 03.11.04 Risk response

// INDEX · SECURITY ASSESSMENT AND MONITORING

- [] 03.12.01 Security assessment
- [] 03.12.02 Plan of action and milestones
- [] 03.12.03 Continuous monitoring
- [] 03.12.05 Information exchange

// INDEX · SYSTEM AND COMMUNICATIONS PROTECTION

- [] **03.13.01 Boundary protection (L1)**
- [] 03.13.04 Information in shared system resources
- [] 03.13.06 Network communications, deny by default, allow by exception
- [] 03.13.08 Transmission and storage confidentiality
- [] 03.13.09 Network disconnect
- [] 03.13.10 Cryptographic key establishment and management
- [] 03.13.11 Cryptographic protection
- [] 03.13.12 Collaborative computing devices and applications
- [] 03.13.13 Mobile code
- [] 03.13.15 Session authenticity

// INDEX · SYSTEM AND INFORMATION INTEGRITY

- [] **03.14.01 Flaw remediation (L1)**
- [] **03.14.02 Malicious code protection (L1)**
- [] 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

// INDEX · PLANNING

- [] 03.15.01 Policy and procedures
- [] 03.15.02 System security plan
- [] 03.15.03 Rules of behaviour

// INDEX · SYSTEM AND SERVICES ACQUISITION

- [] 03.16.01 Security engineering principles
- [] 03.16.02 Unsupported system components
- [] 03.16.03 External system services

// INDEX · SUPPLY CHAIN RISK MANAGEMENT

- [] 03.17.01 Supply chain risk management plan
- [] 03.17.02 Acquisition strategies, tools, and methods
- [] 03.17.03 Supply chain requirements and processes

// THE STUDY GUIDE

Canada's defense supply chain has a cyber security gate on it now. CPCSC Level 1 went live in April 2026, the first contract clauses followed that summer, and Level 2 third-party assessments arrive in 2027. If your shop holds drawings, specifications, or schedules for Department of National Defence work, certification is becoming the price of bidding, and it reaches subcontractors as far down as the data flows.

This is the working manual, in the order you'd do the work. What the program is and why Ottawa built it. Whether it applies to you. The 13 Level 1 controls and the signature under them. Scoping an enclave so you assess 9 machines instead of 40. A gap assessment worth trusting, all 98 requirements family by family with a plain reading of what each one is asking at a 12-to-45-computer shop, documentation that survives an assessor, and the MSP conversation nobody wants to have. Written from readiness engagements with real suppliers, with the vendor pitches left out.

// ABOUT THE AUTHOR

Hans Study, CISSP, is an independent network and security consultant in Ontario, Canada. Fifteen years across physical security integration, enterprise networking, and critical infrastructure, with compliance readiness work since 2016 spanning PCI-DSS, ISO 27001, NIST SP 800-53, ITSG-33, and CMMC. He writes The Study Guide series for the people who do the work.

// CONNECT

hans.study · contact@hans.study · [@studybyt3s](https://twitter.com/studybyt3s)

The Study Guide series · CPCSC companion pages and templates at hans.study/cpcsc

CODES · STANDARDS · PRACTICE**// REVISION 1.3 · OCTOBER 2026**

Includes the September 29, 2026
program changes

ISBN 978-1-0680175-2-0



9781068017520