SmartSuite
Framework / Cybersecurity / Other

ITSP.10.171 — Protecting Specified Information in Non-Government of Canada Systems and Organizations

ITSP.10.171 is the Cyber Centre's Canadian version of NIST SP 800-171 for protecting specified information held by suppliers under Government of Canada contracts.



What it is

ITSP.10.171, Protecting Specified Information in Non-Government of Canada Systems and Organizations, sets the security requirements that Government of Canada departments and agencies put into contracts with suppliers who handle government information that is not classified but must be safeguarded. It is the Canadian version of NIST SP 800-171, took effect April 2, 2025, and its second release was issued on October 28, 2025.

The Canadian Centre for Cyber Security (Cyber Centre), part of the Communications Security Establishment, issues it under the authority of the Head of the Cyber Centre. It binds suppliers through the contract or agreement that cites it, not as a free-standing law. Public Services and Procurement Canada names it as the Canadian industrial security standard for its cyber security certification program for defense suppliers.

At a glance

PUBLISHER Canadian Centre for Cyber Security (CCCS), Communications Security Establishment	TYPE Framework	VERSION ITSP.10.171, second release (October 28, 2025)
EFFECTIVE April 2, 2025	DOMAIN Cybersecurity	FAMILY Other
REGION Canada	INDUSTRY Aerospace & Defense	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY High		

Source: cyber.gc.ca/en/guidance/protecting-specified-information-non-government-canada-systems-and-organizations-itsp10171

Why it matters

- **Defined scope for suppliers** The requirements apply only to the components of non-GC systems that handle, process, store or transmit specified information, or that protect those components (section 1.1).
- **Isolation limits the cost** Organizations can narrow scope by isolating those components in a separate security domain, using physical separation, logical separation or both (section 1.1).
- **Familiar to NIST users** There are no substantial technical changes from NIST SP 800-171, so a supplier already aligned to it carries over most of the work (section 1).
- **Parameters make requirements specific** Organization-defined parameters let departments and suppliers fill in values, such as frequencies, so requirements are testable (section 2.2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ITSP.10.171

Requirement Library with Parameters

Load the 17 families as controls, each carrying its organization-defined parameter values and its ITSP.10.033 source reference.

Specified Information Inventory and Boundary

Record the systems, security domains, data flows and subcontractors that store, process or transmit specified information (section 1.1).

System Security Plan and Plan of Action

Keep the plan, open gaps, remediation milestones and approvals in one set of linked records.

Evidence and Assessment Tracking

Attach logs, access reviews, training records and assessment results to each requirement, and record results from 800-171A-style assessments.

Subcontractor Flow-Down

Track which subcontractors hold specified information and their attestations against the requirements (family 3.17).

Contract and Certification Readiness Reporting

Report implementation by family, open plan items and readiness for contract reviews or certification assessments.

Common framework mappings

NIST 800-171 Rev. 3 | NIST 800-171A Rev.3 | NIST 800-53 Rev.5 | CMMC 2.0 | CMMC 2.0 L2 | ISO 27001:2022 | CIS Controls v8.1 | NIST CSF 2.0

Official resources

ITSP.10.171 — Protecting Specified Information in Non-Government of Canada Systems and Organizations

The Cyber Centre publication: 17 families of security requirements with tailoring criteria and organization-defined parameters (second release, October 28, 2025).

cyber.gc.ca/en/guidance/protecting-specified-information-non-government-canada-systems-and-organizations-itsp10171

NIST SP 800-171 Rev. 3

The U.S. publication ITSP.10.171 is derived from; useful for suppliers that serve both governments.

csrc.nist.gov/pubs/sp/800/171/r3/final

NIST SP 800-171 Rev. 3 (CSRC)

The U.S. publication that ITSP.10.171 adapts; the technical content is the same.

csrc.nist.gov/pubs/sp/800/171/r3/final

Frequently asked questions

What is ITSP.10.171 used for?

It sets the security requirements that Government of Canada departments include in contracts with suppliers that handle specified information, meaning unclassified information a GC authority identifies in a contract as requiring safeguarding. It is the Canadian version of NIST SP 800-171.

Who must comply with ITSP.10.171?

Non-GC organizations, mainly suppliers, contractors and subcontractors, whose system components handle, process, store or transmit specified information under a contract or agreement that cites the publication. It applies only to those components and does not cover classified information (section 1.1).

How does ITSP.10.171 differ from NIST SP 800-171?

There are no substantial technical changes. The differences reflect Canadian laws, policies and directives, including the term specified information instead of controlled unclassified information and references to ITSP.10.033 instead of NIST SP 800-53 (section 1).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are organization-defined parameters?

They are bracketed values in a requirement, such as a frequency or a list, that the GC department or the supplier fills in. If a department leaves a parameter blank, the supplier must assign the value (section 2.2 and Annex B).

How can a supplier reduce the scope of the requirements?

By designating the components that handle specified information and isolating them in a separate security domain, using physical separation, logical separation or both, for example subnetworks with firewalls and information flow controls (section 1.1).

License included / downloadable: Yes ITSP.10.171 is published free by the Canadian Centre for Cyber Security at cyber.gc.ca and is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/canada-itsp-10-171-cyber-security-risk-management-cyber-security

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.