Kiteworks Supports 80% of Canada's CPCSC Cyber Security Certification Controls, Accelerating Defense Supplier Readiness

Platform supports 79 of 98 ITSP.10.171 Level 2 controls, with Canadian deployment options for data sovereignty and dual-framework support for CPCSC and CMMC

SAN MATEO, CA, UNITED STATES, April 23, 2026 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today announced comprehensive platform support for the Canadian Program for Cyber Security Certification (CPCSC)—Canada's mandatory cyber security certification framework for defense suppliers. With Level 1 self-assessment requirements entering select defense contracts beginning Summer 2026, and Level 2 and Level 3 under development for phased introduction, Kiteworks' pre-mapped ITSP.10.171 controls, Canadian deployment options, and audit-ready evidence generation enable defense suppliers to accelerate certification and maintain contract eligibility.

> "CPCSC is built on the same foundational standard [as CMMC], which means our pre-mapped controls, FedRAMP-validated security architecture, and compliance evidence generation work for both programs."
>
> *Frank Balonis, CISO and SVP of Operations at Kiteworks*

The CPCSC, managed by Public Services and Procurement Canada in partnership with the Department of National Defence, the Standards Council of Canada, and the Canadian Centre for Cyber Security, requires defense suppliers handling specified information—sensitive unclassified Government of Canada information—to certify against ITSP.10.171, a Canadian adaptation of NIST SP 800-171.

The program establishes three progressive certification levels:

- Level 1 requires annual self-assessment against 13 foundational controls
- Level 2 introduces triannual third-party assessments by accredited certification bodies across 98 controls, plus annual affirmation
- Level 3 adds 200 controls assessed tri-annually by the Government of Canada

Suppliers that cannot certify will be excluded from defense procurement. U.S. readiness data

from the identical NIST 800-171 control set reveals the scale of the challenge: Only 46% of defense contractors consider themselves prepared for Level 2, 57% have not completed a gap analysis, and 62% lack adequate governance controls.

CPCSC's alignment with NIST SP 800-171 is deliberate, supporting interoperability across Canada's Five Eyes allies and enabling Canadian defense suppliers to demonstrate equivalent security posture to U.S. CMMC-certified contractors. For suppliers bidding on both Canadian and U.S. defense contracts, the two programs share the same foundational control set—and investment in one directly accelerates certification for the other.

"Canadian defense suppliers face the same NIST 800-171 control requirements that have challenged U.S. contractors for years—but with the added complexity of Canadian data sovereignty obligations and the reality that Levels 2 and 3 are still under development," said Frank Balonis, CISO and SVP of Operations at Kiteworks. "Kiteworks has been helping defense contractors navigate CMMC certification since the program's inception. CPCSC is built on the same foundational standard, which means our pre-mapped controls, our FedRAMP-validated security architecture, and our compliance evidence generation work for both programs from a single deployment. Canadian suppliers don't need to start from scratch—they need a platform that's already proven against these exact requirements."

Key Kiteworks capabilities supporting CPCSC certification include:

- Pre-Mapped ITSP.10.171 Controls: Kiteworks supports 79 of 98 Level 2 controls (80% coverage), spanning the ITSP.10.171 security requirement families most relevant to data exchange governance—including Access Control, Audit and Accountability, Identification and Authentication, Media Protection, System and Communications Protection, System and Information Integrity, and Supply Chain Risk Management. The 19 controls Kiteworks does not address are organizational, physical, or process-based—training, personnel screening, physical access, and policy documentation—areas that inherently require human governance.

- Zero-Throttle Audit Evidence: Complete audit logging captures every file access, transfer, and policy decision in real time with no throttling, no delays, and no premium licensing. SIEM integration via syslog and native Splunk Forwarder delivers evidence to security operations. When accredited certification bodies arrive, assessment evidence is ready in hours.

- Canadian Data Sovereignty: On-premises, private cloud in Canadian data centers, or hybrid deployment—combined with single-tenant isolation, customer-owned encryption keys, and geofencing—ensures specified information never leaves Canadian jurisdiction. This addresses the 40% of Canadian organizations that cite changes to Canada–U.S. data sharing arrangements as their top regulatory concern, and the 21% who flag the U.S. CLOUD Act as a direct sovereignty threat.

- FIPS 140-3 Validated Encryption: Uses AES-256 double encryption at rest and TLS 1.3 in transit,

with validated cryptographic modules that meet ITSP.10.171 transmission and storage confidentiality requirement.

- Dual CPCSC-CMMC Certification: Because ITSP.10.171 and NIST SP 800-171 are technically equivalent, the same Kiteworks deployment supports certification against both CPCSC for Canadian contracts and CMMC for U.S. Department of War contracts. Kiteworks is FedRAMP Authorized and provides CMMC 2.0 compliance reports with a Controls Addendum covering all 110 practices, supporting Five Eyes interoperability and cross-border procurement.

- Defense-in-Depth Architecture: Hardened virtual appliance with embedded network firewall, WAF, and AI-based intrusion detection delivers security as a product capability, not a customer responsibility. Deny-by-default network architecture and zero-trust internal tiering address boundary protection and system integrity requirements.

- The Control Plane for Secure Data Exchange: Kiteworks consolidates email, file sharing, managed file transfer, SFTP, web forms, APIs, and AI integrations into a single platform governed by one policy engine, one audit log, and one security architecture. Defense suppliers map controls once and enforce everywhere—across every channel through which specified information moves.

Kiteworks' Solution Guide to CPCSC, including a complete control-by-control mapping of all 98 ITSP.10.171 Level 2 requirements, is available here.

About Kiteworks
Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

David Schutzman
Kiteworks
+1 203-550-8551
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X