Kiteworks

COMPLIANCE BRIEF

Canadian Program for Cyber Security Certification (CPCSC) Compliance Support With Kiteworks

Accelerating ITSP.10.171 Certification for Canada's Defence Suppliers Through Unified Governance and Audit-Ready Evidence

The Canadian Program for Cyber Security Certification establishes mandatory cyber security certification for defence suppliers handling sensitive unclassified government information. Managed by Public Services and Procurement Canada, CPCSC is structured across three certification levels: Level 1 self-assessment (13 controls), required in select defence contracts beginning Summer 2026; Level 2 triannual third-party assessment (98 controls); and Level 3 triannual Government of Canada assessment (200 controls). Levels 2 and 3 are currently under development and will be introduced in a phased approach. The underlying standard, ITSP.10.171, is a Canadian adaptation of NIST SP 800-171 with no substantial technical changes. Certification is a contract gate: no certification, no eligibility. U.S. readiness data from the identical control set shows only 46% of defence contractors consider themselves prepared, and 62% lack adequate governance controls. Kiteworks' secure data exchange platform helps Canadian defence suppliers meet these requirements across multiple control families. Here's how:

Access Control and Identity Management—Unified Policy Enforcement Across All Channels

ITSP.10.171's Access Control and Identification and Authentication families encompass 24 controls—the largest surface in the standard and where organizations fail most often. Kiteworks addresses these through the Data Policy Engine combining RBAC and ABAC controls across email, file sharing, MFT, SFTP, secure data forms, and AI integrations. Eight admin roles enforce separation of duties. MFA supports RADIUS, PIV/CAC, time-based OTP, and enterprise authenticators. LDAP/AD, SAML 2.0, and Kerberos integration enables centralized identity management with automatic provisioning. Geofencing and IP restrictions control remote access.

Audit and Accountability—Complete Evidence Through Zero-Throttle Logging

Kiteworks supports all eight Audit and Accountability controls. The comprehensive audit log captures every event in real time with zero throttling—no gaps, no delays, no premium licensing. Records include event type, timestamp, source IP, user identity, action, object, and policy evaluation. Feeds to SIEM systems via syslog and native Splunk Forwarder. The CISO Dashboard provides analysis and the compliance reports automate framework-specific evidence. Audit access is restricted to the Compliance admin role; even Kiteworks staff cannot modify records.

Solution Highlights

- Zero-throttle audit logging
- FIPS 140-3 validated encryption
- Data Policy Engine (RBAC + ABAC)
- Single-tenant Canadian deployment
- Multi-factor authentication
- Pre-mapped NIST 800-171 controls

System and Communications Protection—Defence-in-Depth With FIPS 140-3 Encryption

Kiteworks delivers security as a product capability through a hardened virtual appliance with embedded network firewall, WAF, and AI-based intrusion detection. Deny-by-default architecture blocks all unused ports. TLS 1.3 encrypts data in transit; AES-256 double encryption protects data at rest with FIPS 140-3 validated modules and customer-owned keys. Single-tenant architecture eliminates cross-tenant exposure. One-click system updates reduce the flaw remediation window. Kiteworks supports 14 of 16 controls across these families.

Configuration Management and Media Protection—Hardened Baseline With Encrypted Data at Every State

Kiteworks ships as a hardened virtual appliance with a secure baseline (stripped-down Rocky Linux 8.10), removing unnecessary services and enforcing least functionality. All admin configuration changes are logged with full attribution. Data sovereignty controls and geofencing track information location and enforce jurisdictional boundaries—critical for specified information that must remain within Canada. Media transport is protected through TLS 1.3 and AES-256 double encryption with FIPS 140-3 validation. Backup data is encrypted with customer-owned keys. Native Kiteworks tags and Microsoft MIP tag integration support data classification and marking.

Canadian Sovereignty and Five Eyes Interoperability—One Platform for CPCSC and CMMC

According to the Kiteworks 2026 Data Security and Compliance Risk Forecast, 40% of Canadian organizations identify changes to Canada–U.S. data sharing arrangements as their top regulatory concern, and 21% flag the CLOUD Act as a direct sovereignty threat. Kiteworks resolves this through on-premises, private cloud in Canadian data centres, or hybrid deployment—combined with single-tenant isolation, customer-owned encryption keys, and geofencing ensuring specified information never leaves Canadian jurisdiction. Because ITSP.10.171 is technically equivalent to NIST SP 800-171, the same deployment certifies against both CPCSC and CMMC for U.S. DoW contracts. Kiteworks is FedRAMP Authorized with pre-mapped controls and provides CMMC 2.0 compliance reports with a Controls Addendum covering all 110 practices.

Kiteworks provides comprehensive support for CPCSC through the Private Data Network. Kiteworks supports 79 of 98 Level 2 controls (80%). The remaining 19 controls are organizational, physical, or process-based requirements. The platform addresses critical requirements through its Data Policy Engine enforcing RBAC and ABAC across all channels, zero-throttle audit logging with real-time SIEM integration, FIPS 140-3 validated AES-256 double encryption with customer-owned keys, a hardened virtual appliance with embedded firewall and intrusion detection, multi-factor authentication, Canadian deployment ensuring data sovereignty, and pre-mapped NIST 800-171 controls serving both CPCSC and CMMC simultaneously. Through these integrated capabilities, Kiteworks helps Canadian defence suppliers accelerate certification while maintaining data sovereignty and Five Eyes interoperability.