Google Cloud Whitepaper
July 2026

Canada Controlled Goods: A Guide for Organizations Using Google Cloud

Authors: Rob Samuel

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of June 2026 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Abstract

As Canada's aerospace, defence, and security sectors increasingly adopt cloud computing, organizations must navigate a complex regulatory framework designed to protect strategic assets. This guide empowers executive leaders and technical engineers in organizations regulated under Canada's Controlled Goods Program (CGP) and the Export and Import Permits Act (EIPA) to confidently architect their Google Cloud environments.

This whitepaper highlights Google Cloud's commitment to security and details how our advanced cryptographic and confidential computing services align with the strict examination and possession boundaries mandated by the Government of Canada. By using this guide, you can learn how to leverage Google Cloud's secure infrastructure including Assured Workloads, External Key Manager (Cloud EKM), Key Access Justifications (KAJ), and Confidential Computing (including Confidential VMs and Confidential Space) to meet your regulatory obligations while maintaining operational agility.

While Google Cloud provides a secure-by-default infrastructure and advanced compliance tools, customers are responsible for independently assessing their own compliance with the Defence Production Act, the Export and Import Permits Act, the Controlled Goods Regulations, and any other applicable laws. Organizations should consult with their own legal counsel to validate their legal and regulatory obligations, as well as the legal effect and enforceability of their architectural and compliance strategies.

Google Cloud's Commitment to Security and Compliance

At Google Cloud, security and compliance are integral to the design and operation of our platform. We understand that for defense and aerospace institutions, trust is paramount, and independent verification of security controls is essential. Our fundamental approach is to deliver a highly secure and resilient infrastructure, complemented by a comprehensive suite of tools and services that empower you to protect your data and applications effectively.

To offer this assurance, Google Cloud undergoes regular, independent third-party audits. We are committed to adhering to key international standards that provide a robust framework for meeting the requirements of the Controlled Goods Regulations, Defence Production Act (DPA), and Export and Import Permits Act (EIPA). These certifications validate our rigorous controls over information security, cloud-specific security, privacy for personal data in the cloud, and AI management systems, establishing a credible basis for your own compliance initiatives.

You can access Google's current certifications and audit reports at any time via our Compliance Reports Manager, which provides streamlined, on-demand access to these crucial compliance resources. For Canadian workloads, Google Cloud operates multiple regions entirely within Canada (such as northamerica-northeast1 in Montréal and northamerica-northeast2 in Toronto), providing robust data residency options for strategic assets.

Inheriting a Secure Foundation: Operating Under Shared Fate

Securing Canada's strategic assets requires more than just meeting compliance checklists; it demands a trusted foundation built on digital sovereignty and continuous operational resilience. At Google Cloud, our infrastructure is designed, built, and operated with security integrated throughout the entire information processing lifecycle. Rather than treating security as an afterthought or a bolted-on perimeter, we engineer protection directly into our custom hardware, global network, and deployment processes from the ground up.

While traditional shared responsibility models define strict boundaries of accountability, Google Cloud operates under a Shared Fate model, actively partnering with you to achieve your target risk and security outcomes by providing secure-by-default blueprints and verifiable guardrails. While maintaining the clear, legally auditable demarcation of responsibilities required by regulators, we actively share the operational burden of defending your controlled goods. By embedding automated guardrails, continuous posture monitoring, and secure-by-default configurations directly into the platform via Assured Workloads, we shift the dynamic from a fragmented division of labor to a unified, verifiable security partnership. You inherit Google Cloud's globally scaled, defense-in-depth infrastructure, and we actively partner with you to achieve your target risk and security outcomes.

By delivering a secure-by-default public cloud environment, we provide the foundational assurance necessary for you to confidently architect, deploy, and protect your controlled goods workloads. Inherited security measures include but are not limited to:

- **Physical Security:** Access to Google's data centers is tightly controlled through multiple physical security layers, including biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems. This establishes the physical perimeter necessary for housing defense articles and technical data.
- **Hardware Design and Provenance:** Google controls its entire hardware stack. We custom-design our server boards, networking equipment, and custom security chips (Titan). The Titan chip establishes a hardware root of trust, cryptographic identity, and secure boot process for our machines, ensuring that the infrastructure running your workloads has not been tampered with.
- **Default Data Protection:** Google proactively protects your data without requiring any configuration. We encrypt all customer content stored at rest by default using the Advanced Encryption Standard (AES-256). Data is logically chunked, and each chunk is independently encrypted with a unique data encryption key, significantly limiting the risk of a potential compromise. Furthermore, Google encrypts and authenticates all data in-transit at one or more network layers when it moves outside physical boundaries controlled by Google.
- **Global Network Security & Threat Monitoring:** Your data travels on Google's private global network. This massive capacity has allowed us to absorb and mitigate the world's largest Distributed Denial of Service (DDoS) attack. Our internal vulnerability management process continuously scans for threats using advanced telemetry, automated testing, and extensive Red Team exercises.

- **Zero Trust Architecture & Insider Risk Reduction:** The CGP requires strict control over who can examine data. Google operates on a Zero Trust security model, enforcing strict logical access controls for our own personnel. Access to internal systems is cryptographically authenticated, logged, and granted only on a strict need-to-know basis. This systemic mitigation of insider threats forms the foundation upon which features like Assured Support and Key Access Justifications are built.

To validate this assurance, Google Cloud undergoes regular, independent third-party audits and maintains compliance with global standards such as: ISO/IEC 27001, SOC 2, and SOC 3. Google Cloud has also undergone assessment by the PSPC CSP's organizational, physical, and personnel security requirements, completed the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) IT Security Assessment and Supply Chain Integrity (SCI) processes, and has been approved to support a full range of government workloads including Protected B Medium and Protected B High Value Asset workloads. For more information, see Google Cloud's Protected B Compliance.

Governing Regulations and Security Guidance for Controlled Goods in the Cloud

Safeguarding controlled goods in the cloud involves navigating a spectrum of legal requirements and official security directives. These frameworks collectively enforce strict boundaries around data residency, cryptographic controls, and unauthorized examination. Key requirements are drawn from:

- **Defence Production Act (R.S.C., 1985, c. D-1).** Establishes the legislative framework for regulating access to controlled goods in Canada to enhance national defence and security. Organizations are responsible for ensuring that private individuals and entities do not unlawfully gain access to, examine, possess, or transfer controlled goods without proper registration or exemption.
- **Controlled Goods Regulations (SOR/2001-32).** Details the specific requirements for the Controlled Goods Program (CGP), including registration conditions, security assessments, record-keeping, and security plans for safeguarding controlled data. Registrants are responsible for continuous monitoring of their information systems, restricting cloud access exclusively to security-assessed personnel, and immediately reporting any security breaches involving controlled data.
- **Technical Data Control Regulations (SOR/86-345).** Established under the Defence Production Act, these regulations govern the control, access, and dissemination of unclassified technical data that discloses critical technology. Certified Canadian contractors must agree not to disseminate such data in any manner that would contravene the export control laws of Canada. In a cloud context, organizations are strictly responsible for enforcing access boundaries, ensuring that unclassified technical data is not provided to anyone other than their direct employees or authorized personnel acting on their behalf. Failure to adequately safeguard this data and control access can result in the immediate suspension or revocation of a contractor's certification.
- **Export and Import Permits Act (EIPA).** This Act governs the export, transfer, and brokering of controlled technology and goods outside of Canada. While the EIPA governs the export,

transfer, and brokering of controlled technology outside of Canada, Google Cloud's CGP architecture is intentionally designed to strictly enforce domestic data residency within Canadian data centers. Google Cloud constrains data storage and processing to Canadian regions and offers Customer-Managed Encryption Keys (CMEK), Cloud External Key Manager (Cloud EKM), Key Access Justifications (KAJ), and Assured Support, designed to help customers meet their obligations. However, customers remain independently responsible for assessing their regulatory compliance, evaluating potential export control obligations, and determining whether formal export permits or legal authorizations are required for their specific operational workflows and data access patterns.

- Notice to Exporters No. 1159 **(Guidance on the movement to and storage of controlled technology in the Cloud).** This notice provides specific guidance on the movement to and storage of controlled technology in the cloud under the EIPA, defining when the use of cloud services constitutes a transfer. Customers are responsible for assessing if storing data outside Canada creates a "reasonable possibility" of foreign examination, and must implement strict cryptographic safeguards (such as customer-managed encryption keys and access controls) to mitigate this risk.
- Guidance on using or providing cloud solutions for controlled goods data. This publication outlines how controlled goods program registrants and cloud service providers can safeguard controlled goods data using cloud storage and computing models. Organizations are responsible for determining if cloud solutions are appropriate, ensuring data residency, establishing secure connections, and verifying that any required technical support is provided solely by security-assessed personnel.

Architecting for CGP Compliance on Google Cloud

For aerospace and defence organizations, digital sovereignty is a strategic imperative to protect national security assets and strengthen the Canadian defence industrial base. Google Cloud approaches this requirement through three foundational pillars: Data Sovereignty (control over encryption and data access), Operational Sovereignty (visibility and control over provider operations), and Software Sovereignty (the ability to run workloads without locking into proprietary provider software).

Operating within the bounds of the CGP requires an architecture that prevents unauthorized examination of controlled data. To help navigate regulatory requirements and provide robust, verifiable assurance to executive leadership, regulatory bodies, and federal technical auditors, Google Cloud offers the Data Boundary for Canada Controlled Goods Program (CGP) solution. This control package transforms complex regulatory requirements into automated, verifiable governance. Detailed deployment prerequisites, in-scope service endpoints, and architectural guardrails are maintained in the official Google Cloud CGP Control Package Documentation. Data Boundary is part of our Sovereign Cloud solutions designed to help governments and enterprises achieve greater control, choice, and security in the cloud without compromising functionality. This solution delivers a scalable, enterprise-ready approach to help customers with their CGP compliance obligations.

Sovereign Data Boundaries via Software-Defined Folders

The Data Boundary for CCG via Assured Workloads is a layer of software-defined controls built directly on top of existing commercial Google Cloud services. This approach ensures organizations do not have to choose between stringent compliance and access to modern capabilities like generative AI.

- **Folder-Level Inheritance:** CGP workloads are deployed within a dedicated compliant folder within the Google Cloud organization. All projects nested under this folder automatically inherit the data residency and access controls set at the folder level, enabling repeatable deployments and mitigating the risk of manual configuration errors.
- **Dynamic Resource Usage Restrictions:** To ensure environment integrity, Assured Workloads dynamically restricts resource usage, allowing enterprise administrators to curate an allow-list of only compliant Google Cloud APIs. This ensures developers cannot inadvertently spin up non-compliant services.
- **Continuous Monitoring:** Assured Workloads Monitoring provides real-time scanning to detect drift and platform misconfigurations. Any deviation from the defined compliance posture triggers immediate alerts, providing continuous auditability for customers and regulators.

Operational & Administrative Guardrails for CGP Workloads

To maintain compliance when deploying and administering CGP workloads in Assured Workloads, organizations must enforce the following operational guardrails:

- **Jurisdictional Web Access:** Administrative access to the Google Cloud console for CGP workloads must be conducted exclusively through approved Jurisdictional Google Cloud console URLs: console.ca.cloud.google or console.ca.cloud.google.com.
- **Metadata & Label Protection:** Controlled goods technical data must reside exclusively within CMEK-encrypted data storage layers. Unencrypted metadata fields such as resource names, project IDs, console output, error messages, resource labels, and network packet headers must never contain controlled goods data.
- **Service Restriction Enforcement**: Organizations should enforce the Assured Workloads resource usage restriction organization policy to prevent the accidental deployment or configuration of GCP services that have not been validated for the CGP control package.

Cryptographic Control and Key Management

All data is encrypted at-rest and in-transit by default. However, data sovereignty requires that decrypting customer data is only possible with the customer's explicit consent.

- **Customer-Managed Encryption Keys (CMEK):** Organizations can manage their own encryption keys using Cloud KMS, ensuring cryptographic boundaries are locked to Canadian regions.
- **External Key Management (EKM):** Digital sovereignty dictates that a cloud provider must never hold the ultimate keys to your restricted data. Unlike legacy 'Bring Your Own Key' (BYOK) models where the provider still caches your keys within their infrastructure, Google Cloud

empowers Canadian organizations to host their root encryption keys on physical hardware located entirely outside of Google's perimeter.
- **Key Access Justifications (KAJ):** While External Key Manager (EKM) maintains the separation between your data at-rest and your encryption keys, Key Access Justifications works with Cloud EKM to make you the ultimate arbiter of access to your data. It provides visibility into every request for an encryption key, a justification for that request, and a mechanism to approve or deny decryption. Covered by Google's integrity commitments, this establishes a definitive technical defense, providing customers the ability to deny access for any reason, including extraterritorial data requests.

Protected Processing and Telemetry

Maintaining compliance means ensuring that data remains protected not just at rest, but during active computing and system troubleshooting.

- **In-Country Processing:** By enforcing the Assured Workloads boundary, compute instances are strictly constrained to Canadian data centers. This ensures that controlled goods data is never decrypted or processed in foreign memory, mitigating the risk of unauthorized foreign examination.
- **Automated Governance of Derived Data:** Automatically generated logs used for troubleshooting may contain derived data and must be treated as controlled goods data. Native log routing within the Assured Workloads boundary ensures that Cloud Logging and audit telemetry remain strictly within Canada, eliminating the risk of unintentional export.

Governed Human Access and Support

Under the CGP, unauthorized access by non-security assessed individuals is strictly prohibited. Operational Sovereignty requires verifiable controls over human interaction with the environment.

- **Assured Support via Dedicated Routing Signals:** The Data Boundary for Canada Controlled Goods Program (CGP) solution enables technical support cases to be routed exclusively to verified Canadian personnel, physically located in Canada, who have completed formal CGP security assessments. To enforce this, the solution applies specialized support routing controls to the Assured Workloads CGP folder. Assured Support for CGP workloads requires an active Enhanced or Premium Cloud Customer Care subscription and is delivered on a consultative, best-effort basis.
- **Verifiable Oversight:** To support direct executive and auditor oversight, Access Transparency provides comprehensive logs of any actions taken by Google personnel. For ultimate control, Access Approval requires the customer's explicit, cryptographic authorization before Google support or engineering teams can interact with the workloads.

Sovereign AI Compute and Infrastructure Control

As organizations increasingly leverage AI, they require systems that can adapt and scale while remaining under domestic governance. Google Cloud enables organizations to build and scale adaptive, Canadian-governed AI systems that serve evolving operational needs.

- **Data Sovereignty and Protection:** Sensitive CGP technical data, is managed on domestic data residency. Whether your development teams are compiling aerospace simulations, analyzing telemetry, or revising prompts for an AI project, the data remains securely within the Assured Workloads boundary. This enables you to build AI solutions, aligned with CGP compliance, without risking data spillage.
- **Infrastructure Control and Resilience:** Through features like External Key Management (EKM) and Assured Workloads, Google Cloud provides cryptographic safeguards that ensure continuous operational control by customers.
- **Governance and Access:** Through tools like Access Transparency and Access Approval, customers retain the comprehensive audit rights and deep technical agency required to enforce decision-making accountability.
- **Supply Chain Resilience and Open Innovation:** While leveraging globally leading hardware, Google Cloud mitigates proprietary lock-in risks through a commitment to open-source frameworks and open AI models. This empowers Canadian organizations to maximize domestic integration, local technical support, and sovereign installation across their supply contracts when building out their AI capabilities.

Compliance Control Mapping

The following table maps core Government of Canada requirements to Google Cloud capabilities:

Framework Reference	Requirement	Google Cloud Commentary
Provider Registration Link	"Registrants must keep in mind their legal obligations under the Act (subsection 45(2)) and the Regulations. They must also be mindful of the offence set out in subsection 37(2) of the Act for knowingly transferring a controlled good to, or permitting the examination of a controlled goods by, a person who is not registered or exempt from registration."	Google Cloud Canada Corporation has been registered in the CGP since July 2024 and a valid Certificate of Registration is maintained. Data Boundary for Canada Controlled Goods includes Assured Support, which guarantees that technical assistance is provided exclusively by personnel who have undergone a CGP security assessment.
Data Residency Link	"Program registrants should take note of any data residency options to ensure that their controlled goods data is stored on servers located in Canada."	Google Cloud Assured Workloads programmatically enforces data residency, ensuring that controlled goods data remains inside Canada at-rest and in-use. Workloads are strictly constrained to the northamerica-northeast1 (Montréal) and northamerica-northeast2 (Toronto) regions.
Restricted Access & Least Privilege Link	"Program registrants must employ a principle of least privilege by monitoring and restricting access to their cloud stored controlled goods data. Access may only be granted to employees who have been security assessed, as detailed in section 15 of the Regulations."	The CGP regulations are explicit, access may only be granted to individuals who have undergone a CGP security assessment. Through Cloud Identity or federation with an enterprise Identity Provider (IdP), Google Cloud IAM allows organizations to programmatically bind cloud access to active HR clearance statuses. Context-Aware Access ensures only these explicitly verified identities can authenticate to the Assured Workloads boundary. Google elevates this with customer oversight. Access Transparency (AXT) provides near real-time, immutable logs of any actions taken by Google personnel. Furthermore, Access Approval (AXA) requires explicit, cryptographic customer consent before Google personnel can access customer data. Any support access granted via Assured Workloads is technically constrained exclusively to verified Canadian personnel holding valid CGP adjudications.

Framework Reference	Requirement	Google Cloud Commentary
Secure Connections Link	Program registrants should ensure that access to their cloud solution is obtained only through a secure connection using, for example, a virtual private network (VPN) or transport layer security (TLS) with user login profiles. Multi-factor authentication and password policies, with audit and logging capabilities, are also recommended."	Google Cloud far exceeds traditional perimeter security by embedding a Zero Trust architecture (BeyondCorp) across its global network. Google elevates this using VPC Service Controls to create a strict, software-defined perimeter that prevents data exfiltration. Identity-Aware Proxy (IAP) enforces granular, context-aware access policies (evaluating identity, location, and device health) before granting access. All data in transit is authenticated and encrypted using FIPS 140-2 validated cryptographic modules, while Cloud Identity enforces phishing-resistant MFA backed by exhaustive Cloud Logging.
Technical Support Link	"When seeking technical support, program registrants should inform their cloud service provider if controlled goods data is at risk. Program registrants should also: - determine the nature of the support needed and the scenarios where the provider can deploy security assessed support personnel".	Standard 'follow-the-sun' cloud support models can introduce compliance risks for CGP requirements. Google Cloud mitigates this by applying automated support routing for Assured Workloads CGP folders. When configured with an active Enhanced or Premium Cloud Customer Care subscription, technical support cases are routed exclusively to Canadian personnel, physically located in Canada, who have completed CGP security assessments (delivered on a consultative, best-effort basis).
Encryption Link	"Program registrants should ensure that controlled goods data is encrypted when uploaded or transferred to the cloud. For example, the U.S. Federal Information Processing Standard (FIPS) encryption standard is used by federal departments and agencies".	Google Cloud encrypts all data at rest and in transit by default. To exceed baseline requirements, customers utilize Customer-Managed Encryption Keys (CMEK) via Cloud KMS to maintain absolute cryptographic control. For ultimate sovereignty, Cloud External Key Manager (Cloud EKM) allows organizations to hold the root of trust in an external HSM located physically in Canada. Combined with Key Access Justifications (KAJ)—which provides automated and auditable justification evaluation per decryption request—and Confidential Computing, which encrypts data in-use while being processed within a hardware-based Trusted Execution Environment (TEE), Google Cloud empowers customers to maintain cryptographic authority over their data and prevent unauthorized examination.

Framework Reference	Requirement	Google Cloud Commentary
Third-Party Audits Link	"Program registrants should also request to review any formal, independent, third-party certifications and security assessments to ensure that the cloud service provider is complying with industry standards, such as the International Organization for Standardization (ISO) and System and Organisation Controls (SOC)."	Google Cloud maintains an industry-leading Third-Party Risk Management (TPRM) posture. We provide independent third-party security assessments and certifications via the Compliance Reports Manager, validating continuous adherence to ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II, and SOC 3 standards. Furthermore, Google Cloud's security is validated domestically through assessment by the Canadian Centre for Cyber Security (CCCS) for secure government workloads. This local assurance is bolstered by accreditations across stringent global defense frameworks (e.g., FedRAMP High, IL4/IL5), providing demonstrable assurance of our robust, globally tested, and domestically verified security infrastructure."
Sovereign AI & Innovation Technical Data Control Regulations (SOR/86-345)	"Contractors must agree not to disseminate such [unclassified technical] data in any manner that would contravene the export control laws of Canada."	Google Cloud enables organizations to deploy Sovereign AI securely. By utilizing Vertex AI within the Assured Workloads boundary, organizations can leverage advanced foundation models and generative AI without risk of data leakage. Google maintains strict intellectual property separation: customer data, prompts, and fine-tuned model weights are never used to train Google's public foundational models, ensuring technical data remains exclusively under customer control.
Domestic Operational Resilience Link	"The cloud service provider's plan should acknowledge that data should be stored in Canada and include procedures for safeguarding controlled goods data in the event of emergency maintenance."	High availability and disaster recovery must not come at the expense of data residency. Google Cloud enables Domestic Operational Resilience by allowing organizations to architect multi-region failovers exclusively across our two distinct Canadian regions (northamerica-northeast1 and northamerica-northeast2). Services like Cloud Spanner and Cloud Storage dual-region configurations ensure mission-critical uptime during regional emergencies without ever routing controlled data across international borders.

Partnering on Your Compliance Journey

Google Cloud is more than a technology provider; we are your partner in navigating the complexities of regulatory compliance. We are dedicated to continuously enhancing our platform and services to help regulated customers meet evolving requirements and innovate securely.

We encourage you to explore Google Cloud's comprehensive compliance resource center to access whitepapers, compliance guides, and detailed documentation relevant to the defence industrial base and data governance, including the Google Cloud Trust Center, Security documentation, Geography and Regions documentation, Security Best Practices, and Privacy information. For guidance on how Google Cloud can support your journey to comply with specific export control regulations, please do not hesitate to contact your Google Cloud account team. We are here to help you build and operate secure, compliant, and transformative solutions in the cloud.