Google Cloud Implementation Guide for CJIS Security Policy v6.0

June 2025

Table of Contents

CJIS Implementation Guide

Audience

This guide is intended for security officers, compliance officers, IT admins, and other employees who are responsible for Criminal Justice Information Security (CJIS) compliance and implementation for their Google Cloud environments. It helps customers understand how Google enables CJIS compliance and which Google Cloud tools, products, and services can help meet CJIS compliance needs. It also explains the Google Cloud shared responsibility model, highlights customer-specific responsibilities, and suggests how to meet these requirements and guidelines on Google Cloud.

Overview

Google Cloud's Data Boundary via Assured Workloads provides a modern approach for customers to achieve compliance with v6.0 of the CJIS Security Policy. Google Cloud's compliance with CJIS security controls has been validated by CJIS Systems Agencies (CSA) across the United States and by Coalfire, a Third-Party Assessment Organization (3PAO).

Google Cloud supports customers with their compliance efforts by providing the same set of security products and capabilities that Google uses to protect its infrastructure. While customers are ultimately responsible for ensuring compliance with CJIS requirements, Assured Workloads provides continuous monitoring of infrastructure and restricts available services to ensure customers can maintain their CJIS compliance. Organizations should seek independent legal advice relating to their CJIS responsibilities. Nothing in this document is intended to provide or be used as a substitute for legal advice.

More information on Google Cloud's approach to security and data protection is listed in the Google security overview whitepaper and in the Google infrastructure security design overview.

Introduction to CJIS

The U.S. Federal Bureau of Investigation's (FBI) CJIS Division provides federal, state, local, and tribal agencies with guidance on how to protect criminal justice information (CJI) when using cloud service providers (CSPs) like Google Cloud.

The FBI CJIS Division oversees many national databases that are leveraged by Criminal Justice Agencies (CJAs) across the country. Much of the data maintained in these databases is considered to be CJI, and is subject to protection from unauthorized use and release. The CJIS Security Policy ("CJISSECPOL"), published by the FBI CJIS Division, provides the minimum set of security requirements for protecting and safeguarding CJI.

The FBI also provides a Requirements Companion Document that highlights recent changes to the CJIS Security Policy and helps identify security roles and responsibilities for entities who access CJI. While the CJA accessing CJI is always ultimately accountable for ensuring CJIS compliance, the Requirements Companion Document guides the CJA in determining who (e.g., FBI CJIS Division, CJA, Service Provider, etc.) has the technical capability to ensure a particular requirement is being met.

Cloud Responsibility Model

Conventional infrastructure technology (IT) required organizations and agencies to purchase physical data center or colocation space, physical servers, networking equipment, software, licenses, and other devices for building systems and services. With cloud computing, a CSP invests in the physical hardware, data center, and global networking, while also providing virtual equipment, tools, and services for customers to use.

Three cloud computing models exist: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS):

- In the IaaS model, CSPs essentially supply a virtual data center in the cloud, and they deliver virtualized computing infrastructure such as servers, networks, and storage. Although CSPs manage the physical equipment and data centers for these resources, customers are responsible for configuring and securing any of the platform or application resources that customers run on the virtualized infrastructure.
- In the PaaS model, CSPs not only provide and manage the infrastructure and virtualization layer, they also provide customers with a pre-developed, pre-configured platform for creating software, applications, and web services. PaaS makes it easy for developers to create applications and middleware without worrying about security and configuration of the underlying hardware.
- In the SaaS model, CSPs manage the physical and virtual infrastructure and the platform layer while delivering cloud-based applications and services for customers to consume. Internet applications that run directly from the web browser or by going to a website are SaaS applications. With this model, organizations and agencies don't have to worry about installing, updating, or supporting applications; they simply manage system and data access policies.

Google Cloud and CJIS compliance

Data Boundary via Assured Workloads

Google Cloud's Data Boundary via Assured Workloads provides a modern approach for customers to achieve compliance with v6.0 of the CJIS Security Policy. Assured Workloads is Google Cloud's regulatory cloud and enables compliance with frameworks such as CJIS, FedRAMP High, and Department of Defense IL2 / IL4 / IL5.

Assured Workloads takes a zero-trust, software-driven approach to regulatory compliance. It allows customers to meet strict government cloud compliance requirements, while providing the performance, scale, service availability, cost, and reliability benefits that customers forgo when using physically separated cloud architectures.

Assured Workloads simplifies security and compliance for state, local, tribal and federal law enforcement (and any other criminal justice or non-criminal justice users of CJI) by:

- Setting data location controls to restrict CJIS workloads to US-only regions ("data residency")
- Restricting unescorted access to unencrypted CJI to US persons located in the US who have completed fingerprint-based background checks by a state CJIS Systems Agency (CSA) or a criminal justice agency (CJA).
- Enabling the use of customer-managed encryption keys (CMEK), hosted either on Google Cloud or using an External Key Manager
- Allowing customers to gain control and visibility over administrative access
- Continuously monitoring customer environments for compliance violations

Assured Controls for Google Workspace

Assured Controls for Google Workspace allows organizations to meet organizational and compliance requirements, whether that involves limiting Google personnel access to customer data, or ensuring that the location of customer data is restricted to the United States.

Customers looking to deploy CJIS solutions using Google Workspace can use Assured Controls to set policies in alignment with the CJIS Security Policy. A configuration guide for CJIS solutions on Google Workspace is separately documented here.

Google Cloud services in scope for CJIS

A full list of up-to-date services that are in-scope for CJIS is maintained on our public CJIS compliance page.

Customer Implementation Guidance

Compliance with the CJIS Security Policy is a shared responsibility between a Service Provider (also referred to as "Customers") and its CSP (such as Google Cloud). This document provides guidance on how customers can utilize Google Cloud's capabilities to support customer compliance with v6.0 of the CJIS Security Policy. Organizations should seek independent legal advice relating to their responsibilities under CJIS. Nothing in this document is intended to provide or be used as a substitute for legal advice.

#1 Access Control and Account Management

<table>
<tr><th>Control Domain</th><th>Access Control and Account Management</th></tr>
<tr><td><b>Relevant Control</b></td><td>CJIS Security Policy v6.0 contains several controls pertaining to Access Control and Account Management (mostly under the AC family).

The introduction to the Access Control section states that "Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing, and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information."</td></tr>
<tr><td colspan="2"><b>Customer Implementation Guidance</b></td></tr>
<tr><td colspan="2">Customers are responsible for managing all aspects of access control for customer users of GCP. To manage access control and account management in Google Cloud, customers can use Identity and Access Management (IAM) to assign roles and permissions to administrative groups, implementing least privilege and separation of duties. Specifically, customers can:
● Define organization admins who will manage information system accounts in the cloud.
○ Admins can be placed in access control groups using Cloud Identity, Admin Console, or another identity provider (e.g., Active Directory or LDAP), ensuring that third-party identity providers are federated with Google Cloud.
● Develop an organization-wide access control policy for information system accounts in the cloud.
○ Customers can also define the parameters and procedures by which the organization creates, enables, modifies, disables, and removes information system accounts.
● Define the parameters and procedures by which the organization will create, enable, modify, disable, and remove information system accounts in the access control policy.
○ The conditions under which information system accounts should be used can also be defined.
● Identify the time period of inactivity in which users will be required to log out of a system (for example, after *x* minutes, hours, or days).
○ Customers can use Cloud Identity, Admin Console, or application configurations to force users to sign out or re-authenticate after the defined time period.</td></tr>
</table>

- Define what actions should be taken when privileged role assignments are no longer appropriate for a user in the organization.
  - Google's Policy Intelligence has an IAM Recommender feature that helps organizations remove unwanted access to Google Cloud resources by using machine learning to make smart access control recommendations.
- Define conditions under which groups accounts are appropriate.
  - Use Cloud Identity or Admin Console to create groups or service accounts.
  - Use service accounts whenever possible.
  - Assign roles and permissions to shared groups and service accounts by using IAM.
- Specify what atypical use of an information system account is for the organization.
  - When atypical use is detected, use tools such as Google Cloud Observability or Security Command Center to alert information system admins.

Control Domain	Access Control and Account Management
Relevant Control	AC-1 requires development of an access control policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Customer Implementation Guidance

To address access control requirements in Google Cloud, customers should:

- Define organization admins who will manage information system accounts in the cloud.
- Place those admins in access control groups using Cloud Identity, Admin Console, or some other identity provider (for example, Active Directory or LDAP), ensuring that third-party identity providers are federated with Google Cloud.
- Use Identity and Access Management (IAM) to assign roles and permissions to administrative groups, implementing least privilege and separation of duties.
- Develop an organization-wide access control policy for information system accounts in the cloud.
- Define the parameters and procedures by which the organization creates, enables, modifies, disables, and removes information system accounts.

To address account management, separation of duties, and least privilege, customers should:

- In the access control policy, define the parameters and procedures by which the organization will create, enable, modify, disable, and remove information system accounts. Customers should also define the conditions under which information system accounts should be used.
- Identify the time period of inactivity in which users will be required to log out of a system (for example, after *x* minutes, hours, or days).
- Use Cloud Identity, Admin Console, or application configurations to force users to sign out or re-authenticate after the defined time period.
- Define what actions should be taken when privileged role assignments are no longer appropriate for a user in the organization.

- Google's Policy Intelligence has an IAM Recommender feature that helps remove unwanted access to Google Cloud resources by using machine learning to make smart access control recommendations.
- Define conditions under which groups accounts are appropriate.
- Use Cloud Identity or Admin Console to create groups or service accounts.
- Assign roles and permissions to shared groups and service accounts by using IAM.
- Use service accounts whenever possible.
- Specify what atypical use of an information system account is for the organization.
- When atypical use is detected, use tools such as Google Cloud Observability or Security Command Center to alert information system admins.

To address information flow enforcement and remote access, customers should:

- In the access control policy, define information-flow control policies for the organization. Customers should also identify prohibited or restricted ports, protocols, and services, and define requirements and restrictions for interconnections to internal and external systems.
- Use tools such as Virtual Private Cloud to create firewalls, logically isolated networks, and subnetworks.
- Help control the flow of information by implementing Cloud Load Balancing, Cloud Service Mesh, and VPC Service Controls.
- When setting information-flow control policies, identify controlled network access points for the organization.
- Use tools such as Identity-Aware Proxy to provide context-based access to cloud resources for remote and onsite users.
- Use Cloud VPN or Cloud Interconnect to provide secure, direct access to VPCs.
- Set organization-wide policies for executing privileged commands and accessing secure data over remote access.
- Use IAM and VPC Service Controls to restrict access to sensitive data and workloads.

To address logon attempts, system-use notification, and session termination, customers should:

- In the access control policy, specify how long a user should be delayed from accessing a login prompt when 3 unsuccessful login attempts have been attempted in a 15-minute period. Customers should also define conditions and triggers under which user sessions are terminated or disconnected.
- Use Cloud Identity Premium Edition or Admin Console to manage mobile devices that connect to the network, including BYOD.
- Create organization-wide security policies that apply to mobile devices.
- Outline requirements and procedures for purging and wiping mobile devices after consecutive unsuccessful login attempts.
- Develop organization-wide language and system-use notifications that provide privacy policies, terms of use, and security notices to users who are accessing the information system.
- Define the conditions under which organization-wide notifications are displayed before granting users access.
    - Pub/Sub is a global messaging and event ingestion system that can be used to push notifications to applications and end users.

  - ○ Customers can also use Chrome Enterprise Suite, including Chrome Browser and Chrome OS, with the Push API and Notifications API to send notifications and updates to users.

To address permitted actions, mobile devices, and information sharing, customers should:

- In the access control policy, define user actions that can be performed on an information system without identification and authentication.
- Use IAM to regulate user access to view, create, delete, and modify specific resources.
- Develop organization-wide policies for information sharing.
- Determine circumstances under which information can be shared and when user discretion is required for sharing information.
- Employ processes to assist users with sharing information and collaborating across the organization.
- Google Workspace has a great feature set for controlled collaboration and engagement across teams.

#2 Awareness and Training

Control Domain	Awareness and Training
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Awareness and Training (mostly under the AT family). The introduction to the Awareness and Training section states that "All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI."
Customer Implementation Guidance	
Customers are responsible for making all users with authorized access to CJI aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. This includes providing security and privacy literacy training to system users (including as part of initial training for new users prior to accessing CJI and annually thereafter), documenting and monitoring information security and privacy training activities, and more.	

Control Domain	Awareness and Training
Relevant Control	AT-1 requires development of an awareness and training policy that must be reviewed annually and following changes to the information system operating environment or when security incidents occur.
Customer Implementation Guidance	
To address awareness and training requirements in Google Cloud, customers should:	

- Create security policies and associated training materials to disseminate to users and security groups across the organization.
- Leverage our offered Professional Services options for educating users on cloud security, including but not limited to a Cloud Discover Security engagement and a Google Workspace Security Assessment.

#3 Audit and Accountability

Control Domain	**Audit and Accountability**
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Audit and Accountability (mostly under the AU control family).
Customer Implementation Guidance	
GCP allows customer developers to write code and manage cloud resources to determine what audit logs are generated and for how long they are retained. It is the customer's responsibility to ensure that customer developed systems hosted on GCP and managed by the customer are capable of auditing the appropriate auditable events. This includes compliance with Audit and Accountability requirements, such as limiting collection of personally identifiable information to the minimum data necessary to achieve the purpose for which it is collected, monitoring and remediating audit processing failures, and more.	

Control Domain	**Audit and Accountability**
Relevant Control	AU-11 in CJIS Security Policy v6.0 states organizations must “Retain audit records for a minimum of one (1) year or until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.”
Customer Implementation Guidance	
For each Google Cloud project, billing account, folder, and organization, Cloud Logging automatically creates two log buckets: **_Required** and **_Default**. Cloud Logging automatically creates sinks named _Required and _Default that, in the default configuration, route log entries to the correspondingly named buckets. Customers can also create **user-defined log buckets** in any Google Cloud project. Details about each type of log bucket are as follows: ● **_Required** - Cloud Logging retains the log entries in the _Required bucket for 400 days, in compliance with the CJIS Security Policy. ○ Cloud Logging automatically routes the following types of log entries to the _Required bucket: ■ Admin Activity audit logs	

        - System Event audit logs
        - Google Workspace Admin Audit logs
        - Enterprise Groups Audit logs
        - Login Audit logs
        - Access Transparency logs. For information about enabling Access Transparency logs, see the Access Transparency logs documentation.
    - Customers cannot:
        - Modify or delete the _Required bucket.
        - Disable the _Required sink, which routes log entries to the _Required bucket.
        - Change routing rules or the retention period for the _Required bucket.

- **_Default -** Any log entry that isn't stored in the _Required bucket is routed by the _Default sink to the _Default bucket, unless the _Default sink is disabled or otherwise edited. For instructions on modifying sinks, see Route logs to supported destinations | Cloud Logging.
    - For example, Cloud Logging automatically routes the following types of log entries to the _Default bucket:
        - Data Access audit logs
        - Policy Denied audit logs
    - Cloud Logging retains the log entries in the _Default bucket for 30 days by default. Customers can change the behavior of the _Default sinks created for any new Google Cloud projects or folders, including configuring custom retention rules to store logs for a longer period of time.

- **User-defined log buckets**
    - Customers can also create user-defined log buckets in any Google Cloud project. By applying sinks to user-defined log buckets, customers can route any subset of log entries to any log bucket, letting them choose the Google Cloud project in which log entries are stored, and letting them store log entries from multiple resources in one location.
    - Customers can also configure custom retention for user-defined log buckets.

It is the customer's responsibility to configure custom retention rules (for both the _Default bucket and for any user-defined buckets) in compliance with the CJIS Security Policy and any state-specific logging retention requirements. See more details at Route log entries | Cloud Logging.

Control Domain	Audit and Accountability
Relevant Control	AU-1 requires development of an audit and accountability policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	
To address audit and accountability requirements in Google Cloud, customers should:	

- Create organization-wide auditing policies and accountability controls that address procedures and implementation requirements for auditing personnel, events, and actions that are tied to cloud information systems.
- In the organization-wide auditing policy, outline events that should be audited in the organization's information systems, and the auditing frequency.
  - Examples of logged events include successful and unsuccessful account login events, account management events, object access, policy change, privilege functions, process tracking, and system events.
  - For web applications, examples include admin activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
- Define additional events of interest for the organization.
- Specify indications of inappropriate or unusual activity for the organization and monitor, log, and flag these activities regularly (at least weekly).
- Use Google Cloud Observability to manage logging, monitoring, and alerting for Google Cloud, on-premises, or other cloud environments.
- Use Google Cloud Observability to configure and track security events affecting the organization.
- Cloud Monitoring can also be used to set custom metrics to monitor for organization-defined events in audit records.
- Enable information systems to alert admins of audit processing failures. Customers can implement these alerts by using tools like Pub/Sub and alerting.
- Set standards for alerting admins within a set time period (for example, within 15 minutes), in the event of a system or functional failure, to include when audit records reach a set threshold or volume capacity.
- Determine an organization-wide granularity of time measurement, by which audit records should be time-stamped and logged.
- Define the level of tolerance for time-stamped records in the information system audit trail (for example, nearly real-time or within 20 minutes).
- Set VPC resource quotas to establish the capacity thresholds for audit record storage.
- Configure budget alerts to notify admins when a percentage of a resource limit has been reached or exceeded.
- Define organization-wide storage requirements for audit data and records, to include audit log availability and retention requirements.
- Use Cloud Storage to store and archive audit logs, and BigQuery to perform further log analysis.

#4 Assessment, Authorization, and Monitoring

Control Domain	Assessment, Authorization, and Monitoring
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Assessment, Authorization, and Monitoring (mostly under the CA control family). CA-1 requires development of an assessment, authorization, and monitoring policy that must be reviewed annually and following changes to the assessment criteria.

Customer Implementation Guidance
To address assessment, authorization, and monitoring requirements in Google Cloud, customers should: ● Develop an organization-wide security assessment and authorization policy that defines the procedures and implementation requirements of organization security assessments, security controls, and authorization controls. ● In the security assessment and authorization policy, define the level of independence required for security assessment teams to conduct impartial assessments of information systems in the cloud. ● Identify the information systems that need to be assessed by an independent assessor. ● Security assessments should minimally cover the following: ○ In-depth monitoring ○ Vulnerability scanning ○ Malicious user testing ○ Insider threat assessment ○ Performance and load testing ● The organization should define additional requirements and forms of security assessment. ● Make sure that the security assessment and authorization policy specifies security system classifications and requirements, including requirements for unclassified and non-national security systems. ● In the information flow control policies for the organization, outline requirements and restrictions for interconnections to internal and external systems. ● Set VPC firewall rules to allow and deny traffic to information systems, and use VPC Service Controls to protect sensitive data by using security parameters. ● Set organization-wide auditing and accountability policies that enforce continuous monitoring requirements (CA-7).

#5 Configuration Management

Control Domain	Configuration Management
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Configuration Management (mostly under the CM control family).
Customer Implementation Guidance	
Customers are responsible for developing, documenting, and maintaining under configuration control the baseline configurations of their GCP information system resources. Customers may elect to use the GCP's Cloud Deployment Manager which allows customers to develop a repeatable process for creating and managing configuration baselines. Customers are also responsible for developing, documenting, and maintaining a current and complete topological drawing depicting the interconnectivity of the network to criminal justice information systems and services, retaining previous versions of baseline configurations to support rollback, and more.	

Control Domain	Configuration Management
Relevant Control	CM-1 requires development of a configuration management policy that must be reviewed annually and following any changes to systems which process, store, or transmit CJI.

Customer Implementation Guidance

To address configuration management requirements in Google Cloud, customers should:

- Create an organization-wide configuration management policy that defines the procedures and implementation requirements for organization-wide configuration management controls, roles, responsibilities, scope, and compliance.
- Standardize configuration setting requirements for organization-owned information systems and system components.
- Provide operational requirements and procedures for configuring information systems.
- Explicitly call out how many previous versions of a baseline configuration the system admins are required to retain for information system rollback support.
- Use Google's suite of configuration management tools to control IT system configurations as code, and monitor configuration changes by using Policy Intelligence or Security Command Center.
- Specify configuration requirements for each type of information system in the organization (for example, cloud, on-premises, hybrid, unclassified, controlled unclassified information (CUI), or classified).
- Define security safeguard requirements for organization-owned and Bring Your Own Device (BYOD) devices to include identifying safe and unsafe geographic locations.
- Use Identity-Aware Proxy to enforce context-based access controls to organization-owned data, including access controls by geographic location.
- Use Cloud Identity Premium edition or Admin Console to enforce security configurations on mobile devices that connect to the corporate network.
- In the configuration management policy, define an organization-wide configuration change-control element, such as a change-control committee or board. Document how frequently the committee meets and under which conditions. Establish a formal body for reviewing and approving configuration changes.
- Identify the configuration management approval authorities for the organization. These admins review requests for changes to information systems.
- Define the time period that authorities have to approve or disapprove change requests. Provide guidance for change implementers to notify approval authorities when information system changes have been completed.
- Set restrictions on the use of open source software across the organization, to include the specification of what software is approved and not approved for use.
- Use Cloud Identity or Admin Console to enforce approved applications and software for the organization. With Cloud Identity Premium, customers can enable single sign-on and multi-factor authentication for third-party applications.
- Use tools such as alerting to send notifications to security admins when configuration changes are logged.

- Give admin access to tools like Security Command Center to monitor configuration changes in near real-time.
- Using Policy Intelligence, use machine learning to study configurations defined by the organization, raising awareness about when configurations change from the baseline.

#6 Contingency Planning

Control Domain	Contingency Planning
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Contingency Planning (mostly under the CP control family). CP-1 requires development of a contingency planning policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Customer Implementation Guidance

To address contingency planning requirements in Google Cloud, customers should:

- Develop a contingency plan that defines the procedures and implementation requirements for contingency planning controls across the organization.
- Identify key contingency personnel, roles, and responsibilities across organizational elements.
- Highlight the mission-essential and business-essential information system operations within the organization.
- Outline recovery time objectives (RTO) and recovery point objectives (RPO) for resuming essential operations when the contingency plan has been activated.
- Document critical information systems and associated software.
- Identify any additional security-related information, and provide guidance and requirements for storing backup copies of critical system components and data.
- Deploy Google's global, regional, and zonal resources and world-wide locations for high availability.
- Use Cloud Storage classes for multi-regional, regional, backup, and archive options.
- Implement global network autoscaling and load balancing with Cloud Load Balancing.

#7 Identification and Authentication

Control Domain	Identification and Authentication
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Identification and Authentication (mostly under the IA control family). The introduction to the Identification and Authentication section states that "Identification is a unique, auditable representation of an identity within an information system usually in the form of a simple character string for each individual user, machine, software component, or any other entity. Authentication refers to mechanisms or processes to verify the identity of a user, process, or device, as a prerequisite to allowing access to a system's resources."
Customer Implementation Guidance	
Customers are responsible for managing all aspects of authentication for customer users of GCP. This includes compliance with Identity and Authentication requirements such as implementing multi-factor authentication, ensuring that replay-resistant authentication mechanisms are used, and more. Compliance may be achieved by using a customer managed SAML-based Single Sign-On system and synchronizing this system with GCP via Google Cloud Directory Sync.	

Control Domain	Identification and Authentication
Relevant Control	IA-12(3) includes guidance that states "TLS version 1.2 or greater is recommended". Some state CJIS Systems Agencies require the restriction of TLS to TLS 1.2 or TLS 1.3 with non-compromised ciphers/authentication only.
Customer Implementation Guidance	
Assured Workloads does not restrict TLS to version 1.2 today but this restriction is on our 2025 roadmap and is scheduled to become a default, required configuration. API protection for GCP services will be included. Customer workloads can be protected with TLS version controls by interposing a cloud load balancer and enforcing protocol controls. In the meantime, customers can deny usage of TLS versions by configuring an org policy at the folder level (e.g., denying usage of TLS versions 1.0 and 1.1 restricts TLS to version 1.2+). See more at Restrict TLS versions | Assured Workloads | Google Cloud.	

Control Domain	Identification and Authentication
Relevant Control	IA-1 requires development of an identification and authentication policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Customer Implementation Guidance

To address identification and authentication requirements in Google Cloud, customers should:

- Create an identification and authentication policy for the organization that specifies identification and authentication procedures, scopes, roles, responsibilities, management, entities, and compliance.
- Specify identification and authentication controls that the organization requires.
- Use Cloud Identity Premium or Admin Console to identify corporate and personal devices that can connect to the organization's resources.
- Use Identity-Aware Proxy to enforce context-aware access to resources.
- Include guidance around authenticator content for the organization, authentication reuse conditions, standards for protecting authenticators, and standards for changing or refreshing authenticators.
- Capture requirements for using cached authenticators.
- Specify time limits for using cached authenticators and create definitions for when to expire cached authenticators.
- Define the minimum and maximum lifetime requirements and refresh time periods that should be enforced by information systems in the organization.
- Use Cloud Identity or Admin Console to enforce password policies for sensitivity, character usage, new password creation or reuse, password lifetime, storage, and transmission requirements.
- Outline hardware and software token authentication requirements for authentication across the organization, including but not limited to PIV card and PKI requirements. Titan Security Keys can be used to enforce additional authentication requirements for admins and privileged personnel.
- In the identification and authentication policy, outline the Federal Identity, Credential, and Access Management (FICAM) information system components that are allowable for accepting third parties in the organization.
  - Google's Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to applications that are being accessed by external entities.

#8 Incident Response

Control Domain	Incident Response
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Incident Response (mostly under the IR control family).

Customer Implementation Guidance

Customers are responsible for their own incident response capabilities. This includes providing employees with incident response training, testing the effectiveness of their incident response capabilities, and more.

Google will send a notification email to customers following the discovery of a data incident. Customers are responsible for providing up-to-date contact information in the Google Cloud Console and for

notifying the CSO, SIB Chief, or Interface Agency Official when suspected incidents affecting CJI are detected within products and applications built using GCP. It is the customer's responsibility to determine if notice to other organizations, including oversight organizations, is needed.

Control Domain	Incident Response
Relevant Control	IR-1 requires development of an incident response policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	
To address incident response requirements in Google Cloud, customers should: ● Establish an organization-wide incident response policy, including procedures to facilitate and implement incident response controls. ● Create security groups for the organization's incident response teams and authorities. ● Use tools such as Google Cloud Observability or Security Command Center to share incident events, logs, and details. ● Develop an incident response test plan, procedures and checklists, and requirements and benchmarks for success. ● Specify classes of incidents that the organization should recognize, and outline the associated actions to take in response to such incidents. ● Define the actions that authorized personnel are expected to take if an incident occurs. These actions might be steps for managing information spills, cybersecurity vulnerabilities, and attacks. ● Take advantage of capabilities in Google Workspace to scan and quarantine email content, block phishing attempts, and set restrictions on attachments. ● Use Sensitive Data Protection to inspect, classify, and de-identify sensitive data to help restrict exposure. ● Specify organization-wide requirements for incident response training, including training requirements for general users and privileged roles and responsibilities. ● Enforce time-period requirements for taking training (for example, within 30 days of joining, quarterly, or annually).	

#9 Maintenance

Control Domain	Maintenance
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Maintenance (mostly under the MA control family). MA-1 requires development of a maintenance policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Customer Implementation Guidance
To address system maintenance requirements in Google Cloud, customers should: ● Create an organization-wide system maintenance policy, documenting system maintenance controls, roles, responsibilities, management, coordination requirements, and compliance. ● Define parameters for controlled maintenance, including approval processes for conducting off-site maintenance and repairs, and organization-wide turnaround times for replacing failed devices and parts. Organizations benefit from Data deletion on Google Cloud data and equipment sanitization, and Google's data center security and innovation for off-site maintenance and repairs.

#10 Media Protection

Control Domain	Media Protection
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Media Protection (mostly under the MP control family). The introduction to the Media Protection section states that "Documented and implemented media protection policies and procedures ensure that access to digital and non-digital media in all forms is restricted to authorized individuals using authorized methods and processes."
Customer Implementation Guidance	
Customers are responsible for ensuring that access to digital and non-digital media in all forms is restricted to authorized individuals using authorized methods and processes. This includes sanitizing or destroying digital and non-digital media in compliance with control MP-6. As part of Google Cloud's FedRAMP ATO, Google meets media protection requirements for physical infrastructure. Review Google's Infrastructure Security Design and Security Overview. Customers are subsequently responsible for meeting virtual infrastructure security requirements.	

Control Domain	Media Protection
Relevant Control	MP-1 requires development of a media protection policy that must be reviewed annually and following any security incidents involving digital and/or non-digital media.
Customer Implementation Guidance	
To address media protection requirements in Google Cloud, customers should:	

- Develop an organization-wide media protection policy, documenting media controls, protection policies and procedures, compliance requirements, and management roles and responsibilities.
- Document procedures for facilitating and implementing media protections across the organization.
- Create security groups that identify personnel and roles for managing media and their protections.
- Specify approved media types and accesses for the organization, including digital and nondigital media restrictions.
- Set media markings and media-handling exceptions that must be implemented across the organization, including security marking requirements inside and outside of controlled access areas.
- Use Data Catalog to manage cloud resource metadata, simplifying data discovery.
- Control cloud resource compliance across the organization, regulating the distribution and discovery of cloud resources with Service Catalog.
- Identify how to sanitize, dispose, or reuse media that the organization manages.
- Outline use cases and circumstances where sanitization, disposal, or reuse of media and devices is required or acceptable.
- Define the media safeguard methods and mechanisms that the organization deems acceptable.

Customers benefit from data deletion on Google Cloud data and equipment sanitization, and Google's data center security and innovation. In addition, Cloud KMS and Cloud HSM provide FIPS-validated cryptographic protection, and customers can use Titan Security Keys to enforce additional physical authentication requirements for admins and privileged personnel.

#11 Physical and Environmental Protection

Control Domain	Physical and Environmental Protection
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Physical and Environmental Protection (mostly under the PE control family).
Customer Implementation Guidance	
As part of Google Cloud's FedRAMP ATO, Google meets physical and environmental protection requirements for physical infrastructure. Review Google's Infrastructure Security Design and Security Overview. Customers are subsequently responsible for meeting virtual infrastructure security requirements.	

Control Domain	Physical and Environmental Protection
Relevant Control	PE-1 requires development of a physical and environmental protection policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Customer Implementation Guidance

To address physical and environmental protection requirements in Google Cloud, customers should:

- Establish an organization-wide physical and environmental protection policy, outlining protection controls, protection entities, compliance standards, roles, responsibilities, and management requirements.
- Outline how to implement physical and environmental protection across the organization.
- Create security groups that identify personnel and roles for managing physical and environmental protections.
- Require admins who are accessing sensitive computational resources to use Titan Security Keys or some other form of MFA to verify access integrity.
- In the physical and environmental protection policy, define physical access control requirements for the organization.
- Identify facility entry and exit points for information system sites, access-control safeguards for such facilities, and inventory requirements.
- Take advantage of tools such as Google Maps Platform to visually display and track facilities and entry and exit points for locational mappings.
- Use Resource Manager and Service Catalog to control access to cloud resources, making them organized and easily discoverable.
- Use Cloud Monitoring to configure loggable events, accesses, and incidents.
- Define organization-wide physical access events that should be logged in Cloud Logging.
- Use the physical and environmental protection policy to account for emergency situations, such as emergency shutoff of information systems, emergency power, fire suppression, and emergency response.
- Identify points of contact for emergency response, including local emergency responders and physical security personnel for the organization.
- Outline requirements and locations for alternate work sites.
- Specify security controls and personnel for primary and alternate work sites.
- Deploy Google's global, regional, and zonal resources and world-wide locations for high availability.
- Use Cloud Storage classes for multi-regional, regional, backup, and archive options.
- Implement global network autoscaling and load-balancing with Cloud Load Balancing.
- Create declarative deployment templates to establish a repeatable, template-driven deployment process.

#12 Planning

Control Domain	Planning
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Planning (mostly under the PL control family).
Customer Implementation Guidance	
Customers are responsible for developing and maintaining a system security plan for their information systems, establishing and providing rules of behavior to individuals that require access to their systems, developing and maintaining an information security architecture, and more.	

Control Domain	Planning
Relevant Control	PL-1 requires development of a planning policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	
To address system security planning requirements in Google Cloud, customers should: ● Develop an organization-wide security planning policy, outlining compliance requirements and security planning controls, roles, responsibilities, and entities for the organization. ● Outline how security planning is expected to be implemented across the organization. ● Create groups to define security-planning personnel accordingly. ● Specify security groups for security assessments, audits, hardware and software maintenance, patch management, and contingency planning for the organization. ● Use tools such as Google Cloud Observability or Security Command Center to monitor security, compliance, and access control across the organization.	

#13 Personnel Security

Control Domain	Personnel Security
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Personnel Security (mostly under the PS control family). The introduction to the Personnel Security section states that “Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section’s security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI. Regardless of the implementation model – physical data center, virtual cloud solution, or a hybrid model – unescorted access to unencrypted CJI must be determined by the

	criminal and noncriminal justice agency taking into consideration if those individuals have unescorted logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI.”
Customer Implementation Guidance	
Customers are responsible for ensuring the system access of customer personnel that have unescorted access to unencrypted CJI is disabled within twenty-four (24) hours of termination of employment (or when individuals are reassigned or transferred to other positions). Customers are also responsible for establishing screening criteria for CJIS-scoped personnel, establishing and documenting personnel security requirements, and more.	

Control Domain	Personnel Security
Relevant Control	PS-1 requires development of a personnel security policy that must be reviewed annually and following any audit findings, changes in laws and policies, and security incidents or breaches.
Customer Implementation Guidance	

To address personnel security requirements in Google Cloud, customers should:

- Create an organization-wide personnel security policy that identifies security personnel, their roles and responsibilities, how personnel security is expected to be implemented, and what personnel security controls to enforce.
- Capture conditions that would require individuals to go through organizational security screening, re-screening, and investigation.
- Outline requirements for security clearances in the organization.
- Include guidance for addressing personnel termination and transfer.
- Define needs and parameters for exit interviews and the security topics that should be discussed during such interviews.
- Specify when security and admin entities in the organization are expected to be notified of personnel termination, transfer, or reassignment (for example, within 24 hours).
- Specify the actions that personnel and the organization are expected to complete for a transfer, reassignment, or termination.
- Cover requirements for enforcing formal employee sanctions.
- Explain when security personnel and admins are expected to be notified of employee sanctions, and explain sanction processes.
- Use IAM to assign roles and permissions to personnel.
- Add, remove, disable, and enable personnel profiles and accesses in Cloud Identity or Admin Console.
- Enforce additional physical authentication requirements for admins and privileged personnel using Titan Security Keys.

#14 Risk Assessment

Control Domain	Risk Assessment
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Risk Assessment (mostly under the RA control family).
Customer Implementation Guidance	
Customers are responsible for conducting and managing their own risk assessments to identify threats to and vulnerabilities in their system. Customers are also responsible for scanning for vulnerabilities in their information system and hosted applications, operating system/infrastructure, web applications, and databases on a monthly basis and when new vulnerabilities potentially affecting the system/applications are identified and reported. Customers must remediate legitimate vulnerabilities in compliance with the number of days listed in control RA-5.d.	

Control Domain	Risk Assessment
Relevant Control	RA-1 requires development of a risk assessment policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	
To address risk assessment requirements in Google Cloud, customers should: ● Implement an organization-wide risk assessment policy that identifies risk assessment personnel, risk assessment controls that are expected to be enforced across the organization, and procedures for carrying out risk assessments in the organization. ● Define how risk assessments are expected to be documented and reported. ● Use tools such as Security Command Center to automatically notify security personnel of security risks and the overall security posture of the organization. ● Leverage Google's suite of risk assessment tools such as Web Security Scanner, Artifact Analysis, Google Cloud Armor, and Google Workspace phishing and malware protection to scan for and report on vulnerabilities across the organization's information systems. ● Make risk assessment tools available to risk assessment personnel and admins to help identify and eliminate vulnerabilities.	

#15 System and Services Acquisition

Control Domain	System and Services Acquisition

Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to System and Services Acquisition (mostly under the SA control family).
Customer Implementation Guidance	
Customers are responsible for determining information security requirements for the information system, managing the information system using a system development life cycle that incorporates information security considerations, and more.	

Control Domain	System and Services Acquisition
Relevant Control	SA-9 in CJIS Security Policy v6.0 states “Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.”
Customer Implementation Guidance	
Customer personnel who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function. They shall also acknowledge, via signing of the Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.	

Control Domain	System and Services Acquisition
Relevant Control	SA-1 requires development of an information systems and services acquisition policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	
To address information systems and services requirements in Google Cloud, customers should: ● Develop an organization-wide system and services acquisition policy that outlines key personnel's roles and responsibilities, acquisition and services management, compliance, acquisition procedures, implementation guidelines, and entities. ● Define the organization's system development lifecycle for information systems and information security. ● Outline information security roles and responsibilities, personnel, and how the organization's risk assessment policy is expected to drive and influence system development life-cycle activities. ● Highlight procedures that are expected to be carried out within the organization when information system documentation is not available or undefined. ● Engage the organization's information system admins and system services personnel as required. ● Define any required training for admins and users that are implementing or accessing information systems in the organization.	

- Use tools such as Security Command Center to track security compliance, findings, and security control policies for the organization.   ○ Google outlines all of its security standards, regulations, and certifications to help educate customers on how to meet compliance requirements and laws on Google Cloud.   ○ In addition, Google offers a suite of security products to help customers continuously monitor their information systems, communications, and data both in the cloud and on-premises. - Specify any locational restrictions for the organization's data, services, and information processing, and under which conditions data can be stored elsewhere.   ○ Google offers global, regional, and zonal options for data storage, processing, and services utilization in Google Cloud. - Leverage the configuration management policy to regulate developer configuration management for system and services acquisition controls, and use the security assessment and authorization policy to enforce developer security testing and evaluation requirements.

#16 Systems and Communications Protections

Control Domain	Systems and Communications Protections
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Systems and Communications Protections (mostly under the SC control family). The introduction to the section states that “Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency’s virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the requirements for protecting systems and communications infrastructures.”
Customer Implementation Guidance	
Customers are responsible for separating user functionality from information system management functionality, preventing unauthorized and unintended information transfer via shared system resources, ensuring information systems built on GCP mitigate Denial-of-Service attacks, and more.	

Control Domain	Systems and Communications Protections
Relevant Control	SC-1 requires development of a system and communications protection policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	

To address system and communications protection requirements in Google Cloud, customers should:

- Create an organization-wide system and communications protection policy that outlines key personnel's roles and responsibilities, implementation requirements for systems communication protection policies, and required protection controls.
- Identify the types of denial of service attacks the organization recognizes and monitors for, and outline DoS protection requirements for the organization.
- Use Google Cloud Observability to log, monitor, and alert on predefined security attacks against the organization.
- Implement tools such as Cloud Load Balancing and Google Cloud Armor to safeguard the cloud perimeter, and leverage VPC services such as firewalls and network security controls to protect the internal cloud network.
- Identify the organization's resource availability requirements; define how cloud resources are expected to be allocated across the organization and what constraints to implement in order to restrict over-utilization.
- Use tools such as Resource Manager to control access to resources at the organization, folder, project, and individual resource level.
- Set resource quotas to manage API requests and resource utilization in Google Cloud.
- Establish boundary protection requirements for the information systems and system communications.
- Define requirements for internal communications traffic and how internal traffic is expected to engage with external networks.
- Specify requirements for proxy servers and other network routing and authentication components.
- Take advantage of Cloud Service Mesh to manage network traffic and communications flow for the organization.
- Use Identity-Aware Proxy to control access to cloud resources based on authentication, authorization, and context—including geographic location or device fingerprint.
- Implement Private Google Access, Cloud VPN, or Cloud Interconnect to secure network traffic and communications between internal and external resources.
- Use VPC to define and secure the organization's cloud networks; establish subnetworks to further isolate cloud resources and network perimeters.
- Google offers global software-defined networks with multi-regional, regional, and zonal options for high availability and failover.
    - Define failure requirements for the organization to ensure that information systems fail to a known state.
    - Capture requirements for preserving information system state information.
    - Use managed instance groups and Deployment Manager templates to re-instantiate failed or unhealthy resources.
    - Give admin access to Security Command Center to actively monitor the organization's confidentiality, integrity, and availability posture.
- In the policy, outline the organization's requirements for managing cryptographic keys, including requirements for key generation, distribution, storage, access, and destruction.
- Use Cloud KMS and Cloud HSM to manage, generate, use, rotate, store, and destroy FIPS-validated security keys in the cloud.

- Google encrypts data at rest by default; however, customers can use Cloud KMS with Compute Engine and Cloud Storage to further encrypt data by using cryptographic keys.
- Deploy Shielded VMs to enforce kernel-level integrity controls on Compute Engine.

#17 System and Information Integrity

Control Domain	System and Information Integrity
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to System and Information Integrity (mostly under the SI control family).
Customer Implementation Guidance	
Customers are responsible for installing security-relevant software and firmware updates in compliance with timelines in control SI-2, for centrally managing malicious code protection mechanisms, for monitoring inbound and outbound communications traffic continuously for unusual or unauthorized activities, and more.	

Control Domain	System and Information Integrity
Relevant Control	SI-1 requires development of a system and information integrity policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	

To address system and information integrity requirements in Google Cloud, customers should:

- Implement an organization-wide system and information integrity policy that outlines key personnel's roles and responsibilities, integrity implementation procedures and requirements, compliance standards, and security controls.
- Create security groups for the personnel in the organization that are responsible for system and information integrity.
- Outline flaw-remediation requirements for the organization, to include guidelines for monitoring, assessing, authorizing, implementing, planning, benchmarking, and remediating security flaws across the organization and its information systems.
- Take advantage of Google's suite of security tools, including but not limited to the following:
  - Chrome Browser
  - Web Security Scanner
  - Artifact Analysis
  - Google Workspace phishing and malware protections
  - Google Workspace security center
  - Google Cloud Armor
- Use these tools to do the following:

  - Protect against malicious code, cyber attacks, and common vulnerabilities.
  - Quarantine spam and set spam and malware policies.
  - Alert admins about vulnerabilities.
  - Gain insights across the organization for central management.
- Use tools such as Google Cloud Observability or Security Command Center to centrally manage, alert on, and monitor the organization's security controls and findings.
  - More specifically, use Google Cloud Observability to log administrative actions, data accesses, and system events initiated by privileged users and personnel across the organization.
  - Notify admins about error messages and information system error handling.
- Define security-relevant events relative to the organization's software, firmware, and information (for example, zero-day vulnerabilities, unauthorized data deletion, installation of new hardware, software, or firmware).
  - Explain the steps to take when these types of security-relevant changes occur.
  - Specify monitoring objectives and indicators of attack for admins to pay special attention to, to include essential information that should be monitored within information systems across the organization.
- Define system and information monitoring roles and responsibilities, as well as monitoring and reporting frequency (for example, real-time, every 15 minutes, every hour, or quarterly).
- Capture requirements for analyzing communications traffic for information systems across the organization.
- Specify requirements for discovering anomalies, including system points for monitoring.
  - Google's Network Intelligence Center services make it possible to conduct in-depth network performance and security monitoring.
  - Google also has strong third-party partnerships that integrate with Google Cloud for scanning and protecting cloud endpoints and hosts, such as Aqua Security and Crowdstrike.
  - Shielded VMs make it possible to harden devices, verify authentication and ensure secure boot processes.
- Define how the organization is expected to check and safeguard against security anomalies and integrity violations.
- Use tools such as Security Command Center or Policy Intelligence to monitor and detect configuration changes.
- Use configuration management tools or Deployment Manager templates to re-instantiate or to halt changes to cloud resources.
- In the system information and integrity policy, specify requirements for authorizing and approving network services in the organization.
- Outline approval and authorization processes for network services.
  - VPC is essential for defining cloud networks and subnetwork using firewalls to protect network perimeters.
  - VPC Service Controls makes it possible to enforce additional network security perimeters for sensitive data in the cloud.

On top of all of this, customers automatically inherit Google's secure boot stack and trusted, defense-in-depth infrastructure.

#18 Supply Chain Risk Management

Control Domain	Supply Chain Risk Management
Relevant Control	CJIS Security Policy v6.0 contains several controls pertaining to Supply Chain Risk Management (mostly under the SR control family). SR-1 requires development of a supply chain risk management policy that must be reviewed annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.
Customer Implementation Guidance	
Customers are responsible for developing and maintaining their supply chain risk management plan. This includes establishing their own supply chain risk management team, employing acquisition tools and processes to protect against, identify, and mitigate supply chain risks, and more.	

Conclusion

Security and compliance in the cloud is a shared responsibility between customers and their CSP. While Google Cloud ensures that its CJIS-scoped services and underlying infrastructure support compliance with the CJIS Security Policy, customers should independently evaluate each requirement to ensure CJIS compliance.

What's next

- Visit Google Cloud's CJIS compliance page to learn more.
- Review an independent, third-party assessment organization's attestation of Google's compliance with v6.0 of the CJIS Security Policy.
- Explore reference architectures, diagrams, and best practices about Google Cloud at our Cloud Architecture Center.