Google Cloud

Google Cloud Whitepaper
April 2022

Google Cloud & NERC CIP

Google User Guide to Support Compliance with NERC CIP

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at https://cloud.google.com/. The content contained herein is correct as of April 2022 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.

Introduction

Most of the world runs on utilities, transportation, communications, and other critical infrastructure that helps businesses and homes operate smoothly on a daily basis. Although it can be easily overlooked, the security, protection and efficient operation of such critical infrastructure forms the backbone of a country's stability and economy.

The North American Electric Reliability Corporation (NERC) is a nonprofit international regulatory organization that strives to enhance the reliability and security of North America's Bulk Electric System (BES) i.e., the power grid. To achieve this, NERC has developed a set of standards to secure and protect critical cyber assets supporting the BES known as Critical Infrastructure Protection (CIP) standards 002-014.

Google is committed to helping our customers meet their obligations under NERC CIP by offering a secure foundation on which to build systems, tools to aid in the security of those systems and education on how to utilize these tools. Google does not directly control the power system, is not a Registered Entity, and is not the Responsible Entity for a NERC Audit. This whitepaper is intended to help customers of Google Cloud understand Google's infrastructure protection features and provide insight into how Google Cloud Platform (GCP) and Google Workspace service offerings (collectively referred to as Google Cloud) may help organizations achieve compliance with NERC CIP Standards while running their workloads on Google infrastructure. This paper is intended to be for informational purposes only and nothing stated here is intended to provide you with or should be used as a substitute for legal advice.

Scope

The NERC is the federal entity responsible for the oversight of the BES for North America and Its jurisdiction applies to all owners, users, producers, and suppliers of the BES in the United States, and parts of Canada and Mexico. The focus of the NERC-CIP standards is to help strengthen the cybersecurity of each utility operator connected to the BES and each utility operator contributing to the BES is thus subject to these compliance mandates.

What are NERC CIP Standards?

NERC CIP standards were introduced in 2008 to address cybersecurity of the BES and continue to evolve, covering uncharted areas like the use of removable media, transient assets, and supply chain risk management. As of today, NERC CIP version 5 standards have 12 critical infrastructure protection standards delving into various cyber security domains such as physical security, access control, network security and recovery planning, among others. In the sections that follow, we will analyze each of the enforceable NERC CIP Standards, their associated requirements, and how Google Cloud can help achieve compliance with the standards.

Please visit the NERC website for more information on NERC CIP Standards and FAQs.

NERC CIP Standards & Google Security Measures

1. **CIP-002-5.1a — BES Cyber System Categorization**

   Purpose

   To Identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES cyber assets could have on the reliable operation of the BES.

Key Requirements	**Google Security Measures**
Identify, categorize, and review BES cyber system assets relevant to NERC CIP	BES Cyber System Asset Identification & Categorization

BES Cyber System Asset Identification & Categorization

Google Cloud services may be leveraged in response to this standard however the ownership and management of the underlying asset classification requirement will be covered by policies, procedures or plans specific to each customer. Customers may need to adjust their asset classifications to reflect use of Google Cloud services, and will need to abide by their compliance program in order to satisfy this requirement.

2. CIP-003-8 — Security Management Controls

Purpose

To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems and BES Cyber System Information against compromise that could lead to misoperation or instability in the BES.

Key Requirements	Google Security Measures
Establish and periodically review cyber security policies.	Cyber Security Policies
Establish accountability of information security roles and responsibilities.	Cyber Security Policies

Cyber Security Policies

Google has established cyber security policies addressing the confidentiality, integrity, and availability of information and information systems. These policies have been approved, published on the intranet, and communicated to relevant personnel. They address domains such as access control, risk management, information exchange, data classification and labeling and acceptable use of assets, among others. Policies are reviewed at least annually and supporting procedures and guidelines are created or updated, as needed.

We have appointed a dedicated information security team and clearly defined information security roles and responsibilities. Google's Information Security Team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure and implementing Google's security policies. We also educate our employees and contractors on security policies and leading practices.

For an overview of GCP and Google Workspace security principles and practices, please see the Google Security Whitepapers and Compliance section of the Google Workspace websites and for details on how Google can support your compliance, visit Compliance Resource Center.

3. CIP-004-6 — Personnel & Training

Purpose

To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

Key Requirements	Google Security Measures
Implement cyber security awareness and training programs for personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	Security Awareness
Conduct periodic role-based training and maintain training records.	Security Awareness
Establish a personnel risk assessment program including background verification and criminal history checks for employees, contractors, and vendors.	Personnel Screening
Establish an access management program including processes for user access authorization and review.	Access Management
Establish access revocation procedures for user terminations, reassignments, or transfers.	Access Management

Security Awareness

Google personnel are required to complete a privacy and information security training program annually. The training specifically addresses responsibilities and expected behavior with respect to the protection of information and the information system. We establish agreements, including non-disclosure agreements, for preserving the confidentiality of information and software exchanges with employees, extended workforce personnel and external parties.

Some features of the security awareness program include:

- A code of conduct training program that is mandated for employees upon hire and is monitored by management through an online learning system. Employees are required to understand and acknowledge the code of conduct
- A periodic internal newsletter that is distributed with alerts and tips on security matters related to Google products, coding practices and general awareness topics such as safe remote computing
- Annually the Google Security Team organizes a security summit that includes brainstorming sessions to contribute to enhancing security in Google's products and services

Personnel Screening

Google new hires and internal transfers go through an official recruiting process that involves screening (new hires only) and interviewing to verify they are competent to fulfill their responsibilities.

As a part of the screening process background checks are performed consistent with FedRAMP requirements, in accordance with local laws and where permitted, including:

- Standard Background Checks per the Google Background Checks Procedure including identity check, employment and education verification and external and internal character reference, where applicable
- As for international employees, checks include global sanctions and enforcement checks (EMEA, APAC and LATAM)
- Contractual agreements require vendors to perform Google Vendor Background Checks on their employees based on vendor corporate policies and as allowed by local country law. Such agreements specify the type of background investigation to be performed including good repute checks, criminal background checks, credit references and two (2) previous employment references

Access Management

Google's access management policy includes processes for identity management, user access provisioning, de-provisioning and modification, privileged access management, and accounts management. Access at Google is restricted through very granular Access Control Lists (ACLs) that are periodically reviewed and modifications to which are recorded and approved by administrators. A proprietary access management system provides fine-grained access control to Google systems, applications, and data.

Google uniquely identifies, authorizes, and authenticates organizational users (or processes acting on behalf of organizational users) for access to the production environment. Physical access to facilities is also limited to individuals with a valid and approved business requirement that necessitates their physical presence.

Users no longer requiring access to information systems (including terminated and transferred individuals) are automatically removed from the access control system through synchronization with the HR system or revocation / modification process initiation by direct manager / designated personnel. According to the Google Exit Process, assets and authenticators associated with the individual are transferred or recovered and logical and physical access is modified or terminated.

While Google manages access to its data centers and facilities, customers are encouraged to use GCP services such as Cloud Identity and Access Management (IAM) and ACLs to manage access policies and permissions for their cloud workloads.

4. CIP-005-6 — Electronic Security Perimeter(s)

Purpose

To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Key Requirements	Google Security Measures
Establish network security controls such as an Electronic Security Perimeter (ESP), Electronic Access Points (EAP), connection authentication and monitoring mechanisms.	Network Security
Establish remote access controls such as multi-factor authentication (MFA), encryption and suspicious activity monitoring.	Remote Access Management Encryption At Rest and In Transit Access Management

Network Security

Google's Network and Computer Security policy aims to reduce the risk of compromise to its network, data, and infrastructure. Access to Google networks and network devices, production machines and support tools is restricted to authorized personnel, managed by ACLs, authenticated via user ID, password, security key, and/or certificates and periodically reviewed. Additionally, access to networks and network devices follow Google's access management procedures.

Our networks are segmented based on the nature of services, users, and information systems being accessed. Network filtering is implemented for inbound, external network traffic limiting it to authorized services, protocols, and ports. Inbound and outbound traffic is restricted to defined access paths and perimeter devices are deployed to protect the network from external network attacks. Google also limits the number of access points and traffic types permitted to its production network.

Google's Device Configuration Guidelines requires the use of a hardware or software firewall (or similar mechanism capable of filtering network traffic) to protect Internet exposed devices from inbound malicious traffic. Additionally, Google Cloud has flexible firewall rules that can be applied to individual or groups of resources and hierarchical firewall policies that can be applied across projects at folder or organization level.

Centrally managed up-to-date detection, prevention, and recovery controls are employed against malicious mobile code along with spam protection at relevant production entry and exit points for networks and on devices including timely installation and upgrade of anti-malware software and regular automatic updates of malware definitions when available in accordance with Google’s security policies and procedures.

Dedicated teams are responsible for monitoring, maintaining, managing, and securing the network and network monitoring can be further improved using the Network Intelligence Center that provides visibility into the network along with proactive network verification.

Remote Access Management

The Google Security Team only authorizes remote access to production resources through the Single Sign-On (SSO) service using a workstation/laptop managed by Google. SSO is the central authentication service for accessing Google's corporate environment and requires a username, password, and second factor authenticator (2FA). SSO enforces 2FA using a memorized secret and a single-factor cryptographic device and maintains its own database of usernames and password hashes. The user then obtains a certificate that enables authentication to production resources. To connect to a remote resource using this method, the user must be in an authorized Machine ACL group as well as be using an authorized device. Additional authentication or approval and SSL or SSH certificates may be required to access critical assets.

SSO system logs and logs collected from target systems are used as a means to monitor remote access methods. Automated methods are used to limit remote connections to the production environment to Google machines with a valid machine certificate. SSO syslogs are monitored through Google's proprietary event management tool and automated analytics are employed to monitor logs for suspicious activity and generate alerts. Examples of suspicious activity include users logging in from unexpected locations or users accessing resources from outside the local domain. The Google Security Team also has the ability to expeditiously disable remote access in the case of a rare security event/emergency, lock or suspend individual accounts and isolate machines at the network level.

Encryption At Rest and In Transit

Data is encrypted between end users and Google, between Google data centers, and at rest using a combination of commercially available and proprietary encryption methods. External authentication traffic between the user's web browser and Google uses TLS encryption when users authenticate to their domain. Encryption within Google's environment utilizes BoringCrypto, a Google encryption module that is FIPS 140-2 certified and encryption between an agency customer and Google servers is dependent on the customer's client configuration. We also implement key rotation using a proprietary system that generates and rotates encryption keys used to protect user data at rest, on average at least every 90 days.

5. CIP-006-6 — Physical Security of BES Cyber Systems

Purpose

To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Key Requirements	Google Security Measures
Establish physical security plan(s) that address physical access controls, monitoring for unauthorized access, maintaining access logs and security of cabling and other network equipment.	Physical Security Access Management
Establish visitor access controls such as escorted access and maintaining visitor access logs.	Visitor Management
Maintain and test the physical access control system.	Physical Security Monitoring

Physical Security

Our Data Center Security (GDCS) team has developed operating principles that mandate physical security and resilience requirements for the protection of Google's people and assets. Google has several policies describing its physical protection measures and guidelines such as the Physical Security Policy, Data Security Policy, Google Photography Policy, Data Center Access policy, and the Data Center Compliance, Security, & Risk Management Policy.

Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas and telecommunications closets are protected by a physical access card reader and a physical key. Google authorizes, monitors, controls, and records all information systems and data center equipment entering and exiting data centers and policies and procedures are developed for working in secure areas.

Google protects its power equipment and cabling from damage and destruction by using several layers of industry standard protection. Power cables are bundled and transmitted throughout the data centers using secured cabling racks. Cabling to the equipment on the data center floors is run through bus ducts in the ceiling accessible only to authorized personnel. We also employ Uninterruptible power supply (UPS) systems to protect against power outages.

Physical access to Google's corporate offices and data centers is controlled via badge readers, physical locks and/or biometric identification mechanisms and follow access management procedures. ACLs to high-security areas in data centers are reviewed periodically and inappropriate access is removed promptly.

Compliance, Security, and Risk Management (CSRM) logs physical access (at both entry and exit points) of data center employees with its facility access control system. Entrants to the data centers are required to either sign in to this (visitors) or badge in (authorized personnel) to gain access to the facility. All visitors must obtain leadership approval and have a valid business reason to be on-site while following all Data Center Security policies .

Data center entrances and the external perimeters are monitored by an on-site security guard.

More information on Google data center security controls can be found in the Google Cloud Platform Data Processing and Security Terms, Appendix 2: Security Measures and Google Workspace Data Processing Amendment, Appendix 2: Security Measures.

Visitor Management

Visitors to Google corporate offices and data center facilities are required to have their identity verified at the perimeter and remain with an escort for the duration of their visit. Access to sensitive data center zones requires approval from authorized personnel and is controlled. Visitors are signed in by an employee before a single-day paper visitor badge can be issued and visitor badges do not have access to secure doors or high security spaces without approval. Visitor access is logged (using a proprietary ticketing system) and retained according to local retention requirements and Google's Retention Policy.

Physical Security Monitoring

Google data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems. Sensitive or restricted areas and unoccupied areas are always alarmed and intruder detection systems are installed and tested, at a minimum annually, to cover external doors and accessible windows. Alarm devices are installed at access-controlled doors and other potential entry points linked to the internal badging system that generate alarms for security monitoring and investigation of unexpected events. Google will notify customers promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure customer Data

We annually assess the security measures utilized in our data centers and the results are reviewed by executive management.

6. CIP-007-6 — System Security Management

Purpose

To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Key Requirements	Google Security Measures
Enable only necessary ports and services.	Configuration Management
Implement a patch management process for tracking, evaluating, and installing applicable cyber security patches.	Patch Management
Prevent, detect, and mitigate the threat of malicious code.	Malicious Code Protection
Establish security event monitoring to detect and investigate security incidents, alert personnel, and enable event logging.	Security Monitoring
Implement system access controls such as user account inventory, authentication, and password management.	System Access Controls Password Management Access Management Remote Access Management

Patch Management

Google's Vulnerability Priority Guidelines provide guidance on how to prioritize security vulnerabilities for remediation and apply security patches. Patches are tested prior to being rolled out and are installed in the production environment in a timely manner. Google also offers services like the OS patch management that can be leveraged to streamline patch compliance reporting and patch deployment.

Malicious Code Protection

In addition to adopting secure development lifecycle practices, change management practices, source code version control and a vulnerability management program; we secure production entry and exit points with malicious code protection mechanisms such as antivirus software and phishing detection software to prevent malware injections.

Information systems are periodically scanned and files from external sources are scanned real-time at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with Google's security policies. Malicious code is detected and blocked, quarantined or alerted to respective teams. Our malicious code protection controls cannot be disabled by employees and we also employ spam protection mechanisms to detect and act on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means, or those that are inserted through the exploitation of information system vulnerabilities. Additionally, Google conducts periodic assessments to evaluate whether systems not commonly affected by malicious software continue to not require anti-virus software.

Security Monitoring

Google’s Security Surveillance Team (SST) investigates events using our proprietary security event analysis platform and collaborates with the incident management team to determine the validity and severity of issues and handles issues accordingly. Alerts from Google's intrusion detection system (IDS) are also utilized for reporting information security events. Google production environment log activity is continually monitored by the SST and audit logs are reviewed automatically by Google's proprietary audit log system monitoring tool which generates alerts as needed. Additionally, information is ingested from machines via the syslog protocol, Windows Event Logs, and internal proprietary protocols, and the severity of alerts is analyzed and prioritized for manual review by incident analysts. Incident analysts then notify appropriate security and organizational personnel when indications of inappropriate or unusual activity are found.

Audit records are retained for 90 days and then archived for one year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational retention requirements.

Google also provides a rich set of logging and monitoring tools, such as Google Workspace Admin Console Report, Operations Suite (formerly Stackdriver) and Cloud Audit Logs to help monitor and analyze system logs and user activity.

System Access Controls

Google authorizes access to information systems and data based on the principles of least privilege, role-based access control and segregation of duties. According to Google’s Data Security Policy, confidential and need-to-know information is shared with only people who require it to fulfill their specific job responsibilities. Formal user registration and de-registration procedures are implemented for granting and revoking access. HR policies govern roles and responsibilities for transfers and terminations, including processes for account removal or change, offboarding procedures, and removal of access or return of assets.

We maintain a current listing of workforce members with access to sensitive information and all account requests go through the standard account management process. Account types are identified (individual, shared/group, system, application, guest/anonymous, emergency, and temporary), conditions for group and role membership are established, and, if used, shared/group account credentials are modified when users are removed from the group. Guest, anonymous, emergency, temporary and group accounts are not used within the authorization boundary unless exceptional circumstances exist and with both management approval and implementation of additional controls. Default accounts are disabled if possible and, if not, have their password changed, and appropriately stored.

Additionally, Google offerings such as Cloud Identity, IAM, Policy Analyzer and IAM Recommender can be used to enhance access control.

Password Management

Password guidelines are established at Google to govern the management and use of authentication mechanisms. Google passwords for the Single Sign-On System comply with the following rules:

- Passwords are case sensitive, with a minimum of eight (8) characters
- Passwords must not be made up of common words and may not be written down
- Network administrator account passwords are separate from user account passwords and have the following configuration:
    - Cannot be the same as a user's SSO password
    - Minimum Length of nine (9) characters
    - Requires at least 1 of each: lowercase, uppercase, numeric, and special characters
    - Passwords must not be found in a dictionary and expire annually

Passwords for default system accounts are changed, whenever there is an indication of password compromise, at first logon and upon account recovery.

The Google Security Team limits the number of invalid logon attempts within an organization defined time period, after which accounts are locked out and require unlocking by Google’s in-house tech support, TechStop or using a self-service option that requires MFA.

7. CIP-008-6 — Incident Reporting and Response Planning

Purpose

To mitigate the risk to the reliable operation of the BES System and BES Cyber Information as the result of a Cyber Security Incident by specifying incident response requirements.

Key Requirements	Google Security Measures
Establish incident response plan(s) (IRP) including processes to identify, classify and handle cyber security incidents with associated roles and responsibilities.	Incident Management
Establish processes for IRP implementation, testing, review, update, and communication.	Incident Management

Incident Management

Google's incident response policy outlines management responsibilities and procedures to facilitate a quick, effective, and orderly response to information security incidents. A dedicated Security Incident Response Team (SIRT) is responsible for managing investigations and dispositions of information security incidents. Audit logs are continuously monitored for security events and threats and alerts are generated for further investigation. Google also provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.

Google has detailed guidelines for incident preparation, detection, analysis, containment, eradication, recovery, coordination across teams and incident management roles and responsibilities such as that of the Incident Commander, Communications Lead, and the Operations Lead.

Google Cloud Incident Communications manages the delivery and communications process pertaining to security, trust, and privacy incidents. Notification timeframes are defined by the Product Lead and Legal Lead in accordance with regulatory and contractual obligations and managed by the Communications Lead.

Incident response exercises are conducted at a minimum, twice a year as part of Google's organizational-wide Disaster Recovery Testing (DiRT). Test exercises are designed to mimic real-life events (hacking, failover, phishing, etc.). Subsequently, IRPs are collaboratively updated by the Incident Management Team based on lessons learned from ongoing incident handling activities, recommendations from postmortem reports, changes in internal processes, or adjustments to incident response metrics and made available to relevant personnel.

Google does not maintain control over customer data in the cloud, but provides tools and guidance to handle data related incidents including Security Command Center for threat detection and a detailed Data Incident Response Process to outline customer responsibilities.

8. CIP-009-6 — Recovery Plans for BES Cyber Systems & Information

Purpose

To recover reliability functions performed by BES Cyber Systems & Information by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

Key Requirements	Google Security Measures
Establish recovery plan(s) including conditions for activation, roles and responsibilities, data preservation and backup	Recovery Planning

procedures.	
Establish processes for recovery plan implementation, testing, review, update, and communication.	Recovery Planning

Recovery Planning

Service-interrupting events can happen at any time and to combat this, Google primarily relies on online data replication for data redundancy which includes the handling of errors by design and creates a solution that is not dependent on a single server, data center or network connection. Established recovery plans are activated once a disruption is detected or appears to be imminent and begin with initial activities such as notifying recovery personnel and conducting an outage assessment post which recovery measures are performed to restore system functions. Google establishes multiple roles and responsibilities for recovery activities and these individuals collectively make up the contingency plan team that are trained annually in their duties.

Google uses a combination of synchronous and asynchronous replication methods to backup system software and data such that current backups are sharded and replicated across multiple clusters in Google in-scope data centers. In addition to online replication, Google has several systems that provide backup and restore capabilities. The default policy for backups is that snapshots of customer data are performed daily, and full backups occur at least weekly. The backups are stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site, and reasonable physical and environmental controls are in place to ensure their protection at the remote location.

Google conducts disaster recovery (DR) testing on an ongoing basis (and at least annually) to enable infrastructure and application teams to test communication plans, failover scenarios, operational transition, and other emergency responses. As part of Google's DiRT program, data restoration tests are also conducted on an annual basis. Google documents post-mortems and lessons learned and creates an organization-wide DiRT report which is made available to employees on the internal website.

Individual teams are then responsible for updating procedures to address vulnerabilities identified after DR plan testing, DR plan execution, changes to the operating environment, or significant changes to the system itself and corrective actions are logged in the internal bug tracking system.

Google has a robust, flexible, and cost-effective selection of products and features that customers may use to build or augment their disaster recovery solution. Google's Disaster Recovery Planning Guide provides further information on how Google can help customers build robust recovery plans.

9. CIP-010-3 — Configuration Change Management and Vulnerability Assessments

Purpose

To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Key Requirements	Google Security Measures
Establish configuration change management processes including baseline configurations and managing deviations from baseline configuration.	Configuration Management
Establish vulnerability assessment procedures for new and existing information systems including remediation or mitigation plans for identified vulnerabilities.	Vulnerability Assessments
Manage transient cyber assets and removable media.	Asset Management

Configuration Management

Google establishes and maintains online mandatory device specific configuration settings for all system components using Google's proprietary source control system and where appropriate, draws from industry and government security guidelines. The configuration settings reflect the most restrictive mode consistent with the operational needs of the system and are periodically updated. As a result of this, Google uses devices that have been heavily customized, and operating systems and configurations that have been modified from factory standards to eliminate unnecessary features, ports, etc.

Configuration items are maintained in a proprietary version control system and changes to these configuration items are managed using change requests subject to review and approval. Changes to network device software, ACLs, and other configurable settings are configuration controlled in the network version control system. A unit testing program is run on configuration changes that runs ‘cracklers’ to attempt to break the configuration and checks compliance with Google’s configuration policies. When changes are pushed, they are first pushed as a test image to a small number of machines in a single data center, and pending successful operation, the changes are pushed across the production environment.

Google automatically evaluates machine configurations and those found to be more than one revision history from the version listed in the version control system, unless otherwise approved, are taken out of production, deviations from the baseline configuration are corrected, and if successful, put back in production. This occurs at least daily. A set of proprietary build and configuration management tools check the machine configuration for deviations and automatically update the configuration using reference files maintained in the version control system.

For customer deployed workloads, Google offerings such as Cloud Deployment Manager, Anthos and OS Configuration Management can help create and enforce consistent configurations.

Vulnerability Assessments

Google maintains a vulnerability management program and associated processes managed by the Information Security Assurance (ISA) team that includes vulnerability assessments, detection, priority assignment, triaging (coordination with partner teams), asset tracking and remediation.

Google uses a vulnerability scan process (using a combination of Commercial Off the Shelf (COTS) tools, Google's proprietary vulnerability scanning tools and third-party assessors) that covers the breadth and depth of Google infrastructure and GCP. Since resources are identically configuration controlled, Google performs vulnerability scans regularly and uses identified weaknesses to update systems in the form of patches or new configurations.

Authorized personnel regularly scan networks, systems, and applications to discover vulnerabilities. If the discovery method is likely to impact the availability of the entity being scanned, relevant teams are notified ahead of time and once service owners have been informed about security vulnerabilities in their systems or software, they are expected to remediate them within specified timelines.

Additionally, customers can leverage Google tools such as Web Security Scanner and Security Command Center to identify and manage vulnerabilities across their Google Cloud organization.

Asset Management

Google authorizes, monitors, controls, and records all assets and equipment entering and exiting its data centers including maintenance tools, diagnostic or configuration equipment, transient assets, and removable media. Physical access to Google facilities is restricted and all assets are authorized for use, hardened to provide only necessary functionality, and access controlled to protect against unauthorized access and misuse. Google assets are regularly scanned for vulnerabilities, updated with the latest security patches and fortified with malware protection to detect security vulnerabilities and prevent malicious code injections from transient assets and removable media.

10. CIP-011-2 — Information Protection

Purpose

To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Key Requirements	Google Security Measures
Identify, protect, and securely handle BES Cyber System Information	Data Security Encryption At Rest and In Transit
Establish procedures for secure reuse and disposal of assets containing BES Cyber System Information	Asset Sanitization, Reuse and Disposal

Data Security

Google handles information according to its classification established in accordance with FIPS 199 "Standards for Security Categorization of Federal Information and Information System" and NIST SP 800-60 Rev. 1 "Guide for Mapping Types of Information and Information Systems to Security Categories". Security categorization is thus implemented as a function of the data and not the system.

Information is transmitted using reliable protocols with error correction and Google only accepts traffic that conforms to the network flow policy and established encryption requirements. Application layer verification of requests provides additional controls over the confidentiality of transmitted information.

Although Google does not control customer data, we offer services such as Cloud Data Loss Prevention and Cloud Key Management that can help customers secure their data on cloud.

Asset Sanitization, Reuse and Disposal

Google meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction. Media is sanitized prior to disposal, when released out of organizational control, or when released for reuse. Our Data Destruction Guidelines for Media and the Physical Security Policy outline the procedures for media sanitization and destruction.

We employ a static fully automated workflow tool to review, approve, and track disks through the sanitization and destruction process. The tool alerts the relevant team when it determines a part needs to be sanitized and/or destroyed. Upon alert, technicians evaluate what actions need to be taken and then perform the cryptographic erasure. Google follows the Clear method of media sanitization, tracks erase results and conducts secondary checks to verify media is erased before the erased drive is released to inventory for reuse or redeployment.

11. CIP-013-1 — Supply Chain Risk Management

Purpose

To mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems.

Key Requirements	Google Security Measures
Develop, implement, and review a supply chain cyber security risk assessment plan including procedures for planning and procurement of information systems.	Supply Chain Risk Management

Supply Chain Risk Management

While Google directly conducts the majority of data processing activities required to provide Google Workspace and GCP services, when third-party suppliers are engaged to provide services including customer and technical support, an assessment is conducted of the security and privacy practices of third-party suppliers. This includes background checks to verify they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide and may include financial and safety checks. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms including non-disclosure agreements.

A list of trusted vendors, parts, and services that are approved for use is maintained and all hardware, software, and external services are subject to security review prior to purchase and integration into the production environment. Third-party software is monitored and restricted post deployment and for its machines and network devices, Google uses approved standard images such that assets are wiped of default software and replaced with an approved standard image prior to being installed into production.

12. CIP-014-2 — Physical Security

Purpose

To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

Key Requirements	Google Security Measures
Periodically conduct and independently verify, risk assessments of Transmission stations and Transmission substations including business impact analysis and identification of primary control centers	Transmission Infrastructure Risk Assessment & Physical Security
Transmission Owner to assess / develop and an unaffiliated third party to verify: ● Potential threats and vulnerabilities of a physical attack to respective Transmission station(s), Transmission substation(s) and primary control center(s) ● Associated physical security plan(s)	Transmission Infrastructure Risk Assessment & Physical Security

Transmission Infrastructure Risk Assessment & Physical Security

The responsible entity operating the grid is largely responsible for meeting compliance to this requirement however Google implements physical security measures to protect Google infrastructure as well.

Google conducts regular risk assessments including business impact analyses of unauthorized access, use, disclosure, disruption, modification, or destruction of both Google infrastructure & GCP systems and the information it processes, stores, or transmits. Security threats, vulnerabilities and risks are analyzed through a variety of risk management activities at varying frequencies throughout the organization including security design reviews, the Objectives and Key Results (OKR) evaluation process, compliance evaluations and ad-hoc reviews in reaction to emerging industry issues.

We implement a number of security measures to secure and protect our infrastructure such as:

- Redundancy of equipment, applications, services, and data across multiple data centers such that global Google services are designed to survive the failure of data center(s)
- A private dark fiber network (lit with our own optical transport equipment) is used for transmissions between data centers. Transmissions consist of service calls between front-end and back-end machines that use secure authentication over a proprietary SSL-based protocol that supports AES-128
- Data centers participate in DiRT across the year improving Google's understanding of its contingency capabilities
- Third party assessors conduct risk assessments and the associated security assessment reports contribute to the system security plan and the plan of action & milestones

Google's CSRM team is a dedicated organization chartered with protecting the people and assets of Google's global critical infrastructure. CSRM consists of industry leading professionals who leverage advanced security systems, dedicated guarding forces, as well as rigorous risk management and compliance framework programs to support the entirety of Google Data Centers.

Shared Responsibility Model

As security and compliance is a shared responsibility between Google and its customers, it's critical to understand which security and compliance tasks are handled by Google and which tasks are to be handled by the customer. While shared responsibilities vary based on cloud service models and the product or offering in question; Google principally secures the underlying cloud infrastructure and services, and the customer secures their applications, devices, systems and data when building on top of Google infrastructure. In summary, Customers/Registered Entities are ultimately the Responsible Entity for achieving NERC CIP Compliance.

To illustrate, we analyze key domains addressed by NERC CIP standards in terms of customer responsibility versus Google responsibility below:

Domain	Customer Responsibility	Google Cloud Responsibility
Cyber Security Policies	Develop and implement cyber security and cloud security policies and associated processes and procedures.	Provide cloud services that have sufficient cyber security controls for customers to safely build upon.
Access Control	Establish and configure user identities, privileges, authentication mechanisms and other access controls using GCP services such as IAM. Conduct periodic access reviews of users with access to cloud services.	Provide cloud services for identity and access management that the customer can leverage to strengthen access control. Establish access management procedures for personnel with electronic or physical access to underlying Google infrastructure and GCP resources.
Personnel Security	Screen personnel accessing cloud services and provide training on cyber security leading practices and acceptable use of resources and services.	Screen and train personnel with logical or physical access to Google infrastructure and those responsible for the operation and maintenance of Google infrastructure and services.
Network Security	Securely configure and monitor	Secure Google networks and

	cloud networks, VPCs and subnets using Google's network protection features.	provide cloud services with sufficient network security controls for customers to safely build upon.
Physical Security	N/A	Implement physical security and environmental protection measures at Google data centers.
Security Event Monitoring	Leverage Google services such as Cloud Operation's Suite and IAM to secure and monitor cloud workloads.	Establish security monitoring at Google data centers and facilities and provide monitoring tools that customers can use to manage cloud workloads.
Malware Protection	Implement malware protection and patch management on customer deployed instances within GCP.	Implement malware protection on the underlying infrastructure and keep systems updated with the latest available security patches.
Incident Management	Implement incident response procedures for customer deployed instances and data.	Implement incident response procedures for systems and infrastructure underlying GCP.
Disaster Recovery	Implement recovery plans for customer deployed instances and data.	Implement recovery plans for Google data centers and systems and infrastructure underlying GCP.
Configuration Management	Establish and implement configuration standards for virtual machines, applications, networks, services, or databases deployed on GCP.	Manage configurations of compute resources and information systems underlying GCP. Provide configuration management tools that customers can leverage.
Data Security	Manage and protect data transmitted to or stored within instances, applications or databases on GCP.	Implement encryption by default, at rest and in transit. Provide cloud services that have sufficient data security controls for customers to safely build upon.

Training and Consultation

Google has a wide range of training and consultation support for our customers such as:

- Pre-sales resources to walk you through our services and help choose the right ones
- Training resources, Cloud on Air videos and Qwiklabs learning to train your team
- Online training partners so you can train on your own schedule
- Certification programs to level set required skills
- Online documentation in multiple languages
- Consulting services and system integrator partnerships to build and manage solutions at scale
- A lively online community of blogs, articles, and chat rooms to share ideas and derive inspiration

Conclusion

This document describes how Google secures its data centers, facilities, information systems and data in Google Cloud to enable customers to build a cloud infrastructure that is compliant with the NERC CIP Standards.

Organizations around the world are increasingly migrating to the cloud to capitalize on the business efficiencies, cost-benefits, and competitive advantages it offers. GCP and Google Workspace provide organizations with the products and services that they will need to set up secure, compliant, highly available, resilient cloud workloads.

To assist our customers in their cloud migration and compliance journey, GCP and Google Workspace technologies and services are designed keeping compliance in mind, while enabling customers to keep pace with changes in their highly competitive and regulated business environments.

To learn more about GCP and Google Workspace products and service offerings, or to contact us, please visit https://cloud.google.com/.