Advisory: Oracle Cloud Infrastructure and Criminal Justice Information Services (CJIS)

Description of Oracle Cloud Infrastructure in the Context of the CJIS Security Policy

May 2022, Version 1.0

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you assessing your use of Oracle Cloud services in the context of the requirements applicable to you under the *Criminal Justice Information Services (CJIS) Security Policy*. This document might also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document, which is not intended as and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

The CJIS Security Policy is subject to periodic changes or revisions by the US Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division. The current version, 5.9, is available at fbi.gov/services/cjis/cjis-security-policy-resource-center.

This document is based on information available at the time of drafting. It is subject to change at the sole discretion of Oracle Corporation and might not always reflect changes in the regulations.

Table of Contents

Introduction

The US Federal Bureau of Investigations (FBI) Criminal Justice Information Services Division (CJIS) sets standards for information, security, guidelines, and agreements for protecting Criminal Justice Information (CJI). The CJIS Security Policy originated within the FBI as a standard for the exchange and protection of investigatory and criminal justice data. Rather than mandate a federal standard, the FBI published their work as a policy that can be agreed to at the state, county, or city level, and by other operating partners and organizations. As a result, each law enforcement and criminal justice agency can interpret the policy requirements within the context of their own operations, and reduce risk and increase assurance of confidentiality and data protection.

The CJIS Security Policy is maintained by the FBI and provided for use by any organization handling CJI. The current version is 5.9 and is published at fbi.gov/services/cjis/cjis-security-policy-resource-center.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to assist you in determining the suitability of using OCI US Government Cloud in relation to the 13 policy areas of the CJIS Security Policy. This document describes Oracle practices and OCI services that might help you meet the requirements of the CJIS Security Policy. We provide you with links to public-facing resources to help you implement those capabilities in your efforts to meet your CJIS Security Policy requirements.

Note: This document focuses on technical security controls. CJIS might have additional policy requirements that are not covered here.

The information contained in this document does not constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle in regard to their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

Oracle's mission is to help customers see data in new ways, discover insights, and unlock possibilities. Oracle provides several cloud solutions tailored to customers' needs. These solutions provide the benefits of the cloud, including global, secure, and high-performance environments in which to run all your workloads. The cloud offerings discussed in this document include Oracle Cloud Infrastructure (OCI).

OCI is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance computing capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI also delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/iaas/Content/home.htm.

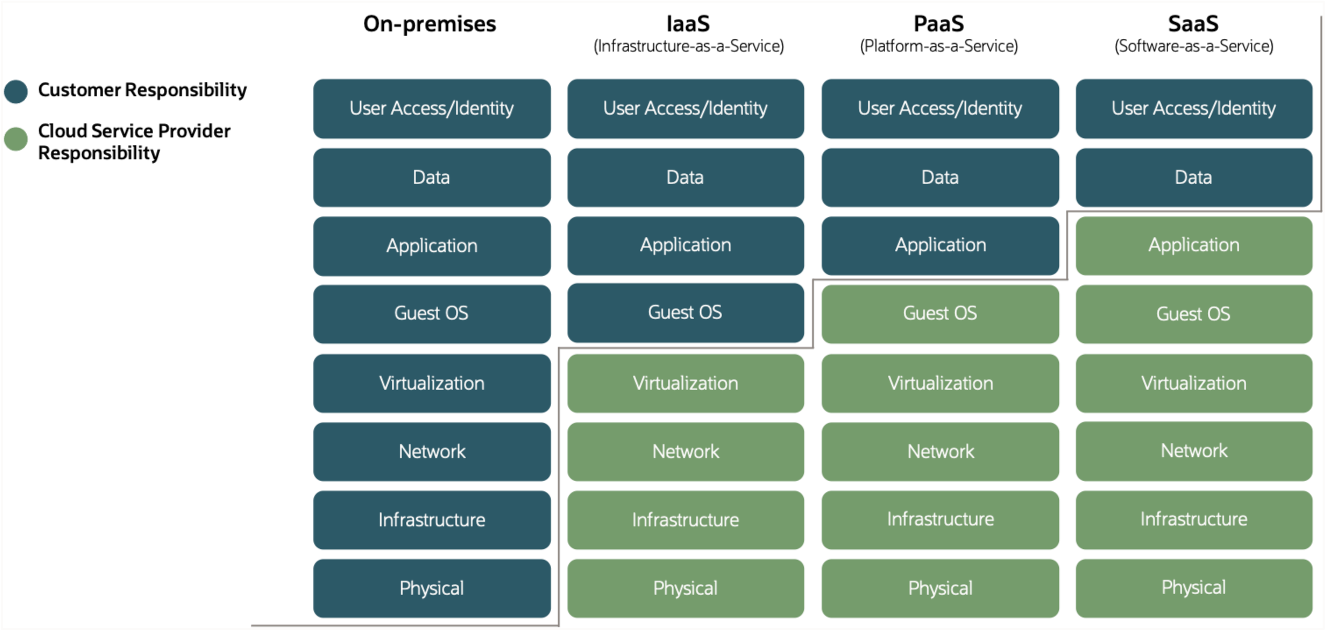
OCI US Government Cloud regions offer a highly secure, enterprise-scale cloud ecosystem that is isolated from commercial customers and built to support mission-critical public sector workloads. The OCI US Government Cloud regions are for the exclusive use of US public sector workloads and select commercial entities who support US government customers. For more information about Oracle Cloud for Government, see oracle.com/industries/government/govcloud.

The Cloud Shared Management Model

From a security management perspective, cloud computing is different from on-premises computing. On-premises customers have full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud services. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see docs.oracle.com/iaas/Content/home.htm.

The following figure illustrates this division of responsibility at a high level.



🟦 Customer Responsibility

🟩 Cloud Service Provider Responsibility

On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
🟦 User Access/Identity	🟦 User Access/Identity	🟦 User Access/Identity	🟦 User Access/Identity
🟦 Data	🟦 Data	🟦 Data	🟦 Data
🟦 Application	🟦 Application	🟦 Application	🟩 Application
🟦 Guest OS	🟦 Guest OS	🟩 Guest OS	🟩 Guest OS
🟦 Virtualization	🟩 Virtualization	🟩 Virtualization	🟩 Virtualization
🟦 Network	🟩 Network	🟩 Network	🟩 Network
🟦 Infrastructure	🟩 Infrastructure	🟩 Infrastructure	🟩 Infrastructure
🟦 Physical	🟩 Physical	🟩 Physical	🟩 Physical

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Criminal Justice Information and CJIS Security Policy

Criminal Justice Information (CJI) is the data that law enforcement, national security, and intelligence community partners need to perform their mission and enforce laws. This information includes but is not limited to biometric, identity history, person, organization, property, and case/incident history data. A Criminal Justice Information System is any application, system, network, or the underlying infrastructure that manages, stores, transmits, or otherwise is involved in the handling of CJI within or between authorized agencies and organizations.

Rules for Federal Data and Oracle Standards

The foundation for CJIS is National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53r5, a standard that defines a catalog of controls for a complete information security management system. NIST 800-53r5 establishes security and privacy controls for information systems and organizations and provides a common baseline for a complete information security program. The Federal Information Security Modernization Act (FISMA) is legislation that provides information about how to design a security program for risk, tailoring it for specific uses. The

FISMA standards denote the “high, moderate, or low impact” scale on which federal risk evaluation is based. An organization uses this scale to set a baseline for the design and implementation of an information security program.

Relationship of CJIS, NIST 800-53, and FedRAMP

The FBI puts forth the frameworks from FISMA and NIST 800-53r5 as the foundation for protection of federal CJI. FBI partner agencies use the impact labels and organization of security controls from the NIST 800-53r5 standard. The CJIS Security Policy supports and promotes interoperation and exchange of data. Many public agencies throughout the US base their own security standards and policies on this same framework because it provides consistency among states and entities requiring CJIS Security Policy adherence.

Federal Risk and Authorization Management Program (FedRAMP) is a federal government program that provides a repeatable process for certifying NIST- and FISMA-compliant cloud solutions. When one federal agency sponsors a cloud provider through the audit process, FedRAMP provides a process by which other agencies may accept the certification and acquire services quickly, rather than repeat the same audit process for themselves.

Oracle Cloud Infrastructure and FedRAMP

OCI’s US Government Cloud has been assessed by an independent third party and achieved FedRAMP High Provisional Authority to Operate (P-ATO). For the complete list of OCI US Government Cloud services that have achieved authorization, see marketplace.fedramp.gov. OCI has been assessed to meet the requirement for NIST 800-53r5 controls, plus additional controls to support “high impact” data categories, which include the government’s most sensitive unclassified data.

OCI has been assessed to meet the requirements for these standards and further undergoes regular audits to provide assurance that its security program and its supporting controls are operating effectively. OCI services and the supporting components undergo continual updates, testing, validation, and reporting within both internal and external compliance frameworks. For more information, see oracle.com/corporate/cloud-compliance.

Summary of the CJIS Security Policy

Sections 1 and 2 of the CJIS Security Policy address introductory material and the compliance approach. Section 3 provides a definition and examples of roles and responsibilities based on a shared management philosophy between agencies that handle CJI data. This shared management philosophy matches the shared management model implemented by Oracle. Section 4 provides definitions of CJI and personally identifiable information (PII).

The formal policy requirements of CJIS are presented in Section 5, “Policy and Implementation.” Each of the 13 policy areas is a subsection of Section 5. (In various official documents, these subsections are described both with and without the leading number; for example, Policy Area 3 is described as “Section 5.3” or “part 3” interchangeably.) This document evaluates each of the 13 policy areas described in Section 5 and describes OCI operational and security practices and applicable services in the context of each requirement.

Customers are solely responsible for determining the suitability of a cloud service in the context of the CJIS Security Policy requirements. Therefore, they are responsible for ensuring that their use of the cloud service and business processes meet these requirements.

Policy Area 1: Information Exchange Agreements

"The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communication mediums are vital to ensuring all parties fully understand and agree to a set of security standards." (CJIS, 2020)

As a cloud provider, Oracle generally has no insight into the data stored or processed in OCI, or whether that data is CJI. However, the contractual rights and obligations of each party are established through contract documents, which the customer and Oracle sign before the provision of cloud services. The Data Processing Agreement for Oracle Services covers key data privacy requirements for service engagements. For more information, see oracle.com/corporate/contracts/cloud-services/contracts.html.

OCI provides the following services and features that might help you meet this requirement for information exchange agreements:

- **Data Safe** is a fully integrated cloud service focused on data security. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle Cloud databases. For more information, see docs.oracle.com/iaas/data-safe/index.html.
- **Identity and Access Management (IAM)** lets you control who has access to your organization's cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

Policy Area 2: Security Awareness Training

"Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected to behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems." (CJIS, 2020)

As a cloud provider, Oracle generally has no insight into the data stored or processed in OCI, or whether that data is CJI. The customer is responsible for implementing a security awareness program to meet the requirements of Policy Area 2.

OCI employees are required to complete security awareness training when they are hired and annually thereafter. The course instructs employees on their obligations under Oracle privacy and security policies for the management of OCI systems. This course also covers data-privacy principles and data-handling practices. For more information, see oracle.com/corporate/security-practices/corporate/human-resources-security.html.

Policy Area 3: Incident Response

"The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incidental handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities." (CJIS, 2020)

Customers are solely responsible for implementing incident response plans for their environment and meeting applicable requirements to ensure protection of CJI.

OCI provides the **Cloud Guard** service, which might help you meet this requirement for incident response. Cloud Guard helps customers monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. Use the service to examine OCI resources for security weaknesses related to configuration, and to examine OCI operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist, or take corrective actions, based on how it is configured. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.

The Data Processing Agreement for Oracle Services describes Oracle's practices in the event of an incident or personal information breach. The Data Processing Agreement is available at oracle.com/corporate/contracts/cloud-services/contracts.html.

Policy Area 4: Auditing and Accountability

"Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

"Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk." (CJIS, 2020)

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements.

OCI provides the following services and features that might help you meet this requirement for auditing and accountability:

- The **Audit** service provides visibility into activities related to OCI resources and tenancy. Audit log events can be used for security audits, to track use of and changes to OCI resources, and to help ensure compliance with standards or regulations. For more information, see docs.oracle.com/iaas/Content/Audit/home.htm.
- **Data Catalog** helps consumers easily find, understand, govern, and track Oracle Cloud data assets. For more information, see docs.oracle.com/iaas/data-catalog/home.htm.
- **Identity and Access Management (IAM)** lets you control who has access to cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.
- **Logging Analytics** is a cloud solution in OCI that lets you index, enrich, aggregate, explore, search, analyze, correlate, visualize, and monitor all log data from applications and system infrastructure. For more information, see docs.oracle.com/iaas/logging-analytics/index.html.

Policy Area 5: Access Control

"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 configuration allowing access to CJIS information." (CJIS, 2020)

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements.

OCI provides the following services and features that might help you meet this requirement for access control:

- **Identity and Access Management (IAM)** lets you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

- The **Vault** key management service provides centralized management of the encryption of customer data with keys that you control. For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Oracle creates a tenancy for each customer, which is a secure and isolated partition within OCI where customers can create, organize, and administer their cloud resources. Customer isolation allows customers to deploy their application and data assets in an environment that commits full isolation from other tenants and Oracle staff.

Policy Area 6: Identification and Authentication

"The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services." (CJIS, 2020)

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements.

OCI provides the **Identity and Access Management (IAM)** service, which might help you meet this requirement for identification and authentication. IAM lets you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

Oracle manages its access to the infrastructure and the services supporting OCI by implementing controls that require multifactor authentication (MFA), a VPN connection, and an SSH connection with a user account and a password or private key.

Policy Area 7: Configuration Management

5.7.1: Access Restrictions for Changes

"Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications." (CJIS, 2020)

The customer is responsible for implementing least privilege functionality, and for security of CJI, software, and system configuration documentation as defined by Policy Area 7.

OCI provides the following services and features that might help you meet this requirement for access restrictions for changes:

- **Identity and Access Management (IAM)** lets you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.
- **Compartments** let you organize and isolate resources to make it easier to manage and secure access to them. For more information, see docs.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm.

Oracle has formal change management practices that are generally described at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html.

Oracle also employs standardized system-hardening practices across the OCI devices that it manages. These practices include the following ones:

- Alignment monitoring with base images, baselines, or both
- Restricting protocol access
- Removing or disabling unnecessary software and services
- Removing unnecessary user accounts
- Patch management and logging capabilities

For more information, see oracle.com/a/ocom/docs/oci-corporate-caiq.pdf.

Policy Area 8: Media Protection

"Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media." (CJIS, 2020)

Customers are responsible for direct CJI data storage, including physical media in its own environment and digital storage media virtualized in cloud infrastructure. Customers are responsible for data deletion and sanitization when virtual containers for CJI remain in service for reuse or repurposing.

OCI provides the following services and features that might help you meet this requirement for media protection:

- **Object Storage** lets you store unstructured data of many content types. This regional service stores data redundantly across multiple storage servers and multiple availability domains. It actively monitors and provides data redundancy. If a redundancy loss is detected, Object Storage automatically creates more data copies. For more information, see docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm.
- **Archive Storage** is a storage class tier for data objects that must be retained for long periods of time but are rarely accessed. For more information, see docs.oracle.com/iaas/Content/Archive/Concepts/archivestorageoverview.htm.
- **Block Volume** lets you use a block volume as a regular hard drive when it's attached and connected to a Compute instance. Volumes are automatically replicated to help protect against data loss. For more information, see docs.oracle.com/iaas/Content/Block/Concepts/overview.htm.
- **File Storage** lets you manage shared file systems and mount targets, and create file system snapshots. File Storage uses synchronous replication and high-availability failover for resilient data protection. For more information, see docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.

OCI secures the media used for the underlying cloud infrastructure that it manages. OCI does not transport media that contains customer data. Oracle's encryption and encoding controls prevent OCI from having visibility into customer data or the virtual containers in which it is stored and managed. Inoperable or decommissioned equipment is sanitized before disposal. For more information about media management at Oracle, see oracle.com/corporate/security-practices/corporate/data-protection/technical-controls.html.

Policy Area 9: Physical Protection

"Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access controls measures." (CJIS, 2020)

Customers are responsible for all aspects of the direct physical protection of CJI. This protection includes access to customer facilities and locations where it operates its business, and controlled areas where CJI is accessed, transmitted, or displayed to individuals.

Oracle Cloud data centers are designed to help protect the security and availability of customer data. This approach begins with Oracle's site selection process. Candidate build sites and provider locations undergo an extensive risk evaluation by Oracle. This evaluation considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations, among other criteria.

Oracle Cloud data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow an N2 redundancy methodology for critical equipment operation. Data centers that house OCI services use redundant power sources and maintain generator backups in case of widespread electrical outage. Server rooms are closely monitored for air temperature and humidity, and fire-suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address security and availability events that might arise.

Policy Area 10: System and Communications Protection and Information Integrity

"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." (CJIS, 2020)

Customers are solely responsible for determining the suitability of a cloud service in the context of this requirement. Therefore, you are responsible for ensuring that your organization's use of the cloud service and business processes meet these requirements.

The following OCI services enable at-rest data encryption by default, by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later. You can use these services and features to help meet the encryption requirements:

- **Object Storage** lets you store unstructured data of many content types. This regional service stores data redundantly across multiple storage servers and multiple availability domains. It actively monitors and provides data redundancy. If a redundancy loss is detected, Object Storage automatically creates more data copies. For more information, see docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm.
- **Block Volume** lets you use a block volume as a regular hard drive when it's attached and connected to a Compute instance. Volumes are automatically replicated to help protect against data loss. For more information, see docs.oracle.com/iaas/Content/Block/Concepts/overview.htm.
- **File Storage** lets you manage shared file systems and mount targets, and create file system snapshots. File storage uses synchronous replication and high-availability failover for resilient data protection. For more information, see docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.
- The **Vault** service lets you centrally manage encryption keys. For more information, see docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Oracle has implemented isolated network virtualization in every data center in every region, using network devices to control access between the internet and Oracle Cloud by allowing only authorized traffic. Network devices are deployed in a layered approach to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address to identify authorized sources, destinations, and traffic types.

Policy Area 11: Formal Audits

"Formal audits are conducted to ensure compliance with applicable statutes, regulations, and policies." (CJIS, 2020)

Customers are solely responsible for responding to FBI CJIS audit requests, and for supplying sufficient evidence that they are operating in accordance with applicable statutes, regulations, and policies.

Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations." These attestations can help in your compliance and reporting, providing independent assessment of the security, privacy, and compliance controls of OCI. Customers can contact their Oracle account representative to obtain copies of OCI audit reports and attestations. For additional information, see oracle.com/corporate/cloud-compliance/.

The Data Processing Agreement for Oracle Services describes the audit rights of customers and their regulators. Oracle's participation in an audit with customers or their regulators is subject to the terms of the Data Processing Agreement, available at oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf.

Policy Area 12: Personnel Security

"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 including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI." (CJIS, 2020)

Customers are solely responsible for implementing the personnel security policies that meet the requirements of this policy area.

OCI provides the **Identity and Access Management (IAM)** service for managing personnel access, which might help you meet this requirement for personnel security. IAM lets you set up groups, compartments, and policies that control which users can access which services and resources, and the type of access they have. For more information, see docs.oracle.com/iaas/Content/Identity/Concepts/overview.htm.

Oracle strongly emphasizes personnel security. The company has an ongoing initiative intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities. The initiative includes personnel screening, confidentiality agreements, security awareness training, and enforcement of disciplinary actions.

Learn more about human resources security at Oracle at oracle.com/corporate/security-practices/corporate/human-resources-security.html.

Policy Area 13: Mobile Devices

"This policy area describes considerations and requirements for mobile devices including smartphones and tables. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices." (CJIS, 2020)

Customers are solely responsible for all devices and communication between endpoint devices and CJI data and CJIS platforms and applications.

OCI has no visibility into endpoint deployment, management, or use, and does not use these technologies to provide cloud infrastructure services to the customer.

Conclusion

Oracle Cloud Infrastructure US Government Regions provide the hardware, fault tolerance, regional footprint, and infrastructure that allow CJIS Systems Agencies to meet the following goals:

- Share the management of security controls to create an effective platform
- Support the compliance of their applications within the current CJIS Security Policy
- Collaborate and extend their data sharing more easily and effectively
- Respond to requirements and changes, and dynamically manage emerging risks

Oracle is committed to helping customers operate globally in a fast-changing business environment and address their challenges of technology risks. Before deploying Oracle Cloud services, customers should analyze their cloud strategy to determine the suitability of using the applicable Oracle Cloud services in the context their own legal and regulatory compliance obligations.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find local offices at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle