ORACLE

Oracle US National Security Regions

A US Classified Workload Solution with Everything Everywhere®

Datasheet

The Next-Generation Classified Cloud

Oracle Cloud's US National Security Regions (ONSRs) are Oracle Gen 2 Cloud regions secured to the highest US Government classification standards. Identical to full-scale and full-service commercial Oracle Cloud regions, ONSRs are built in highly secured ICD 705 facilities. These regions are supported by government-cleared US Citizens, and only connected to classified US Government networks. ONSRs support Secret, Top Secret, SCI, and SAP workloads, with security controls meeting or exceeding the regulatory and compliance requirements for Department of Defense Impact Level 6 (IL6) and Intelligence Community Directive (ICD 503) accreditation.

All National Security Region operations are performed from securely managed Cloud Network Operations Centers (CNOCs) by US Government-cleared engineers.

A complete cloud for secure, mission-critical applications

Leverage the extensive range of Oracle commercial innovation. All of Oracle's Gen 2 Cloud Infrastructure, Platform, and Software-as-a-Service (IaaS, PaaS, and SaaS) and Marketplace offerings are built to operate and deliver full functionality in ONSRs. With no CapEx investment, you have complete flexibility to scale, design, and operate your workload.

24/7 operations and support by cleared US personnel

Supported and managed from dedicated CNOCs, ONSRs are staffed around the clock by Oracle employees with the highest levels of US Government security clearance. Upholding Oracle's industry-leading enterprise SLAs, the operation centers operate and maintain the cloud and provide 24/7 customer support to resolve issues. Dedicated ticketing systems on the classified networks ensure secure incident management.

Fast, secure network connectivity

Completely isolated from both the internet and internal Oracle networks, ONSRs are only connected to government-specified, isolated networks (e.g., SIPRNet and JWICS). Cross Domain Solutions are an internal service to transfer data, such as Oracle Cloud software updates, from lower to higher classification networks. No data may leave the classified enclave without customer authorization and sanitization.

Oracle National Security Region Highlights

Everything Everywhere®
Same services as public cloud, all the latest innovation—just disconnected and secure

Security-first by design
Oracle Cloud architecture is engineered with security as a foundational core—zero-trust model

Comprehensive solution for continuity of operations
Geographic survivability for mission-critical workloads

Dedicated support
24/7 support by Oracle employees with the highest levels of US Government security clearance

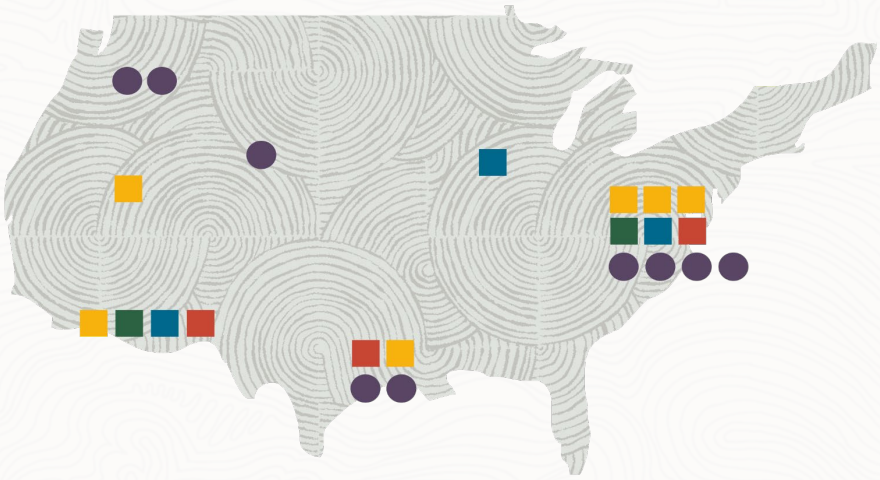
Fastest time to mission
Leverage Oracle Cloud security control inheritance to accelerate mission workload ATO with a footprint that grows with your forecasted demand

Best value proposition
Continuous cloud performance and innovation—all at the same price as commercial regions

Oracle Cloud Infrastructure for US government

Oracle Cloud's US Government regions provide a highly secure, enterprise-scale government community cloud, built to support mission-critical government workloads.

Agencies in federal, state, and local government are using Oracle's US Government regions to accelerate the migration of on-premises workloads, modernize business processes with cloud applications, and safely drive technology innovation in the cloud.



Oracle Cloud Infrastructure regions support the highest US Government compliance standards.

US Government Regions	US Department of Defense (DoD) Regions	US National Security Regions
OC2	OC3	OC6, OC7, OC11, & OC12
FedRAMP High JAB Authorized (P-ATO) IL2, IL4 Authorized	DISA IL5 Authorized (P-ATO) Connections to North, East, and West DISA BCAPs DREN East and West	Secret and Top Secret/SCI

Security-First Design

Oracle has a long history of working closely with customers to secure highly sensitive and classified data workloads—ONSRs leverage this experience to design a cloud model that meets the needs of government, intelligence, and defense agencies. Oracle's security approach is based on seven core pillars: customer isolation, data encryption, security controls, visibility, secure hybrid cloud, high availability, and verifiable secure infrastructure. Each pillar offers multiple solutions designed to enable you to confidently run mission-critical workloads and protect your data.

OCI ensures full **customer isolation and a dedicated cloud model** with comprehensive **security management**.

Our **zero-trust security** model with a robust portfolio of OCI security innovations to ensure security is simple—easy to use, deploy, and operate.

Customers have complete **visibility** with log and audit data and security analytics.

Our fault-independent data centers enable **high-availability,** scale-out architectures; and are resilient against network attacks.

OCI is third-party audited, certified, and attested **verifiable secure infrastructure**.

Learn more at **oracle.com/nationalsecurity**

Everything Everywhere®