SmartSuite

Framework / Cloud Security / Other

DoD Cloud Computing Security Requirements Guide (SRG) DoD Cloud Computing Security Requirements Guide

What it is

The DoD Cloud Computing Security Requirements Guide (SRG) is a United States Department of Defense (DoD) cybersecurity framework that establishes baseline security requirements for cloud service providers handling DoD data. Its main purpose is to safeguard sensitive government information in commercial and government-operated cloud environments by enforcing rigorous security controls and compliance protocols.

Published and maintained by the Defense Information Systems Agency (DISA), the DoD Cloud Computing SRG is mandatory for any organization seeking to host, process, or store DoD information in the cloud. The framework covers areas such as cybersecurity controls, risk management processes, access controls, incident response, and data protection for Impact Levels 2 through 6, aligning with DoD information sensitivity classifications.

At a glance

PUBLISHER U.S. Department of Defense (DoD)	TYPE Control Framework	VERSION Current DISA Cloud Computing SRG
EFFECTIVE 2014	DOMAIN Cloud Security	FAMILY Other
REGION United States	INDUSTRY Aerospace & Defense	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

Source: https://public.cyber.mil/

Why it matters

The DoD Cloud Computing SRG defines mandatory security requirements for cloud service providers handling Department of Defense data.

- **Strengthen cybersecurity governance** Fosters strong oversight by requiring consistent security controls and management practices across cloud-hosted government data and workloads.
- **Enhance regulatory alignment** Aligns organizational practices with Department of Defense and federal mandates, simplifying compliance reporting and external audit interactions.
- **Increase audit readiness** Requires documented processes and evidence, enabling organizations to efficiently demonstrate compliance and maintain a state of audit preparedness.
- **Promote operational resilience** Mandates comprehensive incident response and risk management, reducing service disruption and safeguarding mission-critical operations against cyber threats.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports DoD Cloud SRG

Impact Level Scope Tracking

Document IL scope, data types, and hosting requirements with clear boundaries.

Control Mapping and Evidence Hub

Track SRG requirements mapped to controls with implementation proof.

Authorization and Approval Workflows

Manage approvals, artifacts, and decision records supporting DoD use cases.

Continuous Monitoring Operations

Schedule scanning, patching, and reporting with repeatable evidence capture.

Vendor and Subservice Provider Oversight

Track third-party dependencies, assurances, and monitoring evidence.

Readiness Reporting

Report posture, gaps, and progress by impact level and service.

Common framework mappings

CMMC 2.0 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27017 | NIST 800-171 Rev. 3 | NIST 800-53 Rev.5 | SOC 2

Official resources

DoD Cloud Computing Security Requirements Guide (SRG)

Defines security requirements for cloud service providers handling DoD data.

public.cyber.mil/dccs/srg

DISA Security Technical Implementation Guides (STIGs)

Provides implementation guidance to ensure compliance with DoD security standards.

public.cyber.mil/stigs

DoD Impact Level Authorization Requirements

Outlines the security controls applicable to various DoD impact levels.

public.cyber.mil/dccs/dod-impact-levels

DISA Risk Management Framework (RMF) Guidance

Describes the integration of SRG with DoD's RMF process for compliance.

public.cyber.mil/rmf

Frequently asked questions

What is the DoD Cloud Computing SRG used for?

The DoD Cloud Computing SRG defines security requirements for cloud service providers that store, process, or transmit Department of Defense (DoD) information. It ensures that sensitive and mission-critical DoD data in commercial and government clouds are protected according to established risk management and cybersecurity standards.

Is compliance with the DoD Cloud Computing SRG mandatory?

Yes, compliance with the DoD Cloud Computing SRG is mandatory for any organization or cloud service provider handling DoD information in the cloud. Achieving and maintaining compliance is a prerequisite for receiving a DoD Provisional Authorization to operate (PA or P-ATO) in DoD environments.

What environments or organizations does the DoD Cloud Computing SRG apply to?

The SRG applies to all cloud service providers and contractors who process, store, or manage DoD data, regardless of whether the services are operated by commercial vendors or government entities. Its requirements span multiple impact levels, corresponding to the sensitivity and criticality of the data involved.

What are the key concepts or artifacts required by the DoD SRG?

Key concepts include impact levels (IL2, IL4, IL5, IL6), security controls mapped to NIST SP 800-53 and FedRAMP, risk assessments, and continuous monitoring. Critical artifacts for compliance include control implementation summaries, security authorization packages, incident response plans, and audit evidence documentation.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does an organization implement the DoD Cloud Computing SRG?

Implementation involves selecting the appropriate impact level, performing a gap assessment against required controls, and remediating deficiencies. Organizations must document their security posture, undergo third-party assessments, and submit artifacts for review to obtain and retain the necessary DoD authorization.

How does the DoD Cloud Computing SRG relate to other frameworks like FedRAMP and NIST SP 800-53?

The SRG leverages security controls from NIST SP 800-53 and incorporates FedRAMP baselines, but tailors requirements to address DoD-specific risk tolerances and information protection needs. It often operates in conjunction with these frameworks within organizational compliance programs, especially when seeking both federal and DoD-specific authorizations.

What are the ongoing compliance requirements under the DoD Cloud Computing SRG?

Ongoing compliance includes continuous monitoring of security controls, regular vulnerability assessments, incident reporting, and updating authorization documentation as systems or environments change. Maintaining audit readiness and promptly addressing compliance gaps are essential for continued authorization status.

How would SmartSuite support DoD Cloud Computing SRG?

SmartSuite supports DoD Cloud Computing SRG management by centralizing risk and control tracking, mapping SRG baselines and evidence to a unified compliance workspace, and automating audit documentation. It streamlines evidence collection, remediation workflows, and assessment scheduling, ensuring continuous compliance, real-time monitoring, and comprehensive reporting for security leaders and authorizing officials.

License included / downloadable: Yes The DoD Cloud Computing Security Requirements Guide is published by the Defense Information Systems Agency (DISA) and is publicly available through official U.S. government resources.

Full framework page and mappings: smartsuite.com/frameworks/dod-cloud-computing-security-requirements-guide-srg