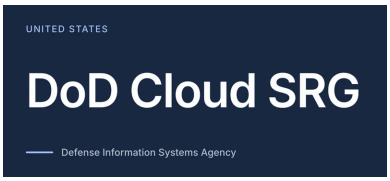
SmartSuite

Framework / Cloud Security / Other

DoD Cloud Computing Security Requirements Guide (SRG)

The DoD Cloud Computing SRG, issued by DISA, sets the controls cloud providers need for a DoD Provisional Authorization at Impact Levels 2, 4, 5 and 6, from public data up to SECRET.



What it is

The DoD Cloud Computing Security Requirements Guide (SRG) sets the security controls and conditions a cloud service provider must meet before it can host Department of Defense (DoD) information, and a DoD Provisional Authorization (PA) is the approval that records it. Providers need a PA at the right Impact Level before a DoD cloud contract is awarded, under DFARS 239.7602-1. The guide first appeared in 2015.

At a glance

PUBLISHER
Defense Information Systems Agency (DISA)

TYPE
Control Framework

VERSION
Cloud Service Provider SRG V1R1 (June 14, 2024) and Cloud Computing Mission Owner SRG; see the DoD Cyber Exchange for the current release

EFFECTIVE
January 2015 (first Cloud Computing SRG)

DOMAIN
Cloud Security

FAMILY
Other

REGION
United States

INDUSTRY
Aerospace & Defense

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: cyber.mil/dccs/dccs-documents

Why it matters

- **Authorization before award** Off-premises commercial services need a DoD PA at the appropriate Impact Level before contract award, or evidence that one can be achieved (section 4.5).
- **Impact Levels match data sensitivity** Levels 2, 4, 5 and 6 range from publicly releasable data to classified information up to SECRET (section 3.7).
- **U.S. data location** DoD data not on DoD premises stays in the 50 states, the District of Columbia and outlying areas unless the authorizing official approves otherwise (section 5.2.1).
- **Fast incident reports** Initial incident reports are due within one hour of the provider's triage deciding the incident is reportable (section 6.2.2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports DoD Cloud SRG

Impact Level Register

Record each cloud offering, its target Impact Level and the data categorization behind it (section 3.7).

FedRAMP+ Control Library

Track the FedRAMP baseline and DoD parameter value additions per control, with owner and evidence (section 5.1 and Appendix D).

Authorization Package Tracker

Keep the FedRAMP authorization, PA request, subcontracted offerings disclosed and supply chain risk management plan together (sections 3.6 and 5.12).

Continuous Monitoring Calendar

Schedule annual assessments, monthly vulnerability scans and plan of action and milestones reviews (sections 5.3.1 and 6.4).

Incident Reporting Workflow

Time each incident against the one-hour initial report rule and record the required notification fields (section 6.2.2).

Data Location and Provider Reporting

Record where DoD data can be stored, the authorizing official's approvals and a dashboard of open requirements for each offering (section 5.2.1).

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?

It is DISA's set of security requirements for cloud service providers that host Department of Defense information. Since June 2024 it has been issued as a Cloud Service Provider SRG and a Cloud Computing Mission Owner SRG. DoD uses it to decide whether to grant a DoD Provisional Authorization.

What are the DoD Impact Levels?

Impact Level 2 covers non-controlled unclassified information, Level 4 controlled unclassified information, Level 5 controlled unclassified information and unclassified National Security Systems, and Level 6 classified information up to SECRET (section 3.7). They are a DoD construct, not FedRAMP levels.

Does a FedRAMP authorization satisfy the SRG?

No. The SRG builds on FedRAMP baselines but adds the DoD's FedRAMP+ controls and parameter values, and the DoD PA is granted separately for each cloud service offering (sections 3.6 and 5.1). A PA is revocable if the FedRAMP authorization is lost.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Where must DoD data be stored?

Data not on DoD premises must stay in the 50 states, the District of Columbia and outlying areas of the United States, in facilities under U.S. legal jurisdiction, unless the authorizing official approves another location (section 5.2.1).

How fast must a cloud provider report an incident?

The initial report is due within one hour of the provider's internal triage deciding that the incident is reportable. It may be incomplete, with fuller information following as details emerge (section 6.2.2).

License included / downloadable: Yes The SRG is a U.S. Government document published by DISA on the DoD Cyber Exchange and is included with the platform for reference.

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