GOVDATAHOSTING
POWERED BY IT-CNP, INC.

FEDRAMP HIGH (CLASS D) CERTIFIED CLOUD PLATFORM

DOD IMPACT LEVEL 4 & 5
REQUIREMENTS GUIDE

Your Complete Guide to DoD Cloud Authorization

2026 EDITION • **DOD CLOUD COMPUTING SRG · NIST 800-53 REV 5**

INSIDE THIS GUIDE

DoD Cloud Computing SRG overview • IL4 vs. IL5 requirements • Data categories & classifications • FedRAMP-to-DoD mapping • Authorization process • CMMC alignment • Implementation roadmap

FOR

Defense Contractors • DoD Agencies • Mission Partners

GovDataHosting

FedRAMP High (Class D) Certified • DoD IL2 Authorized • U.S. Cloud Data Centers Only

www.govdatahosting.com | 800-967-1004

What's Inside

Understanding DoD Impact Levels

The Department of Defense (DoD) Cloud Computing Security Requirements Guide (CC SRG), maintained by the Defense Information Systems Agency (DISA), establishes the security requirements for cloud service offerings (CSOs) that host DoD missions. Impact Levels (ILs) categorize the sensitivity of the information involved and the corresponding controls required to protect it.

What Is the DoD Cloud Computing SRG?

The CC SRG is the authoritative framework governing cloud security for DoD workloads. It builds on the FedRAMP baselines and layers on DoD-specific ("FedRAMP+") controls, CNSSI 1253 overlays, jurisdiction and personnel requirements, and network connection requirements. The current SRG aligns to NIST 800-53 Revision 5.

DoD Impact Levels in Use

The SRG defines four impact levels in active use — IL2, IL4, IL5, and IL6 — each escalating in data sensitivity and security rigor. Earlier levels IL1 and IL3 have been retired; IL3 was consolidated into IL4.

LEVEL	DATA TYPES	BASELINE	TYPICAL USE CASE
IL2	Non-CUI; publicly releasable / non-critical mission data	FedRAMP Moderate (DoD reciprocity)	Public-facing sites, low-sensitivity apps
IL4	CUI, FOUO, PII/PHI, export-controlled data	FedRAMP Moderate baseline + CUI controls + DoD overlays	Most DoD CUI and contractor workloads
IL5	Higher-sensitivity CUI, mission-critical data, unclassified NSS	FedRAMP High baseline + NSS overlays	Mission-critical and national security systems
IL6	Classified information up to SECRET	FedRAMP High + classified (SIPRNet) overlay	Classified national security systems

This guide focuses on **IL4 and IL5**, which together cover the majority of defense-contractor and DoD-agency cloud requirements for sensitive but unclassified information.

> **KEY POINT: FEDRAMP IS THE FOUNDATION**
> DoD IL authorizations build on a FedRAMP authorization. IL4 requires at minimum a FedRAMP Moderate baseline (a FedRAMP High authorization is accepted toward IL4 without re-assessing the additional control enhancements), while IL5 requires the full FedRAMP High baseline plus NSS overlays. Partnering with a **FedRAMP High (Class D) Certified** provider such as GovDataHosting — and, for IL4/IL5, GovDataHosting-managed AWS GovCloud infrastructure that holds DISA IL4/IL5 Provisional Authorization — accelerates your authorization timeline.

Impact Level 4 (IL4) Requirements

Impact Level 4 is designed for Controlled Unclassified Information (CUI) that requires safeguarding or dissemination controls pursuant to law, regulation, or government-wide policy. IL4 is the most common impact level for defense contractors handling sensitive but unclassified DoD data.

Data Types Authorized for IL4

- **Controlled Unclassified Information (CUI):** information requiring safeguarding per Executive Order 13556 and the NARA CUI Registry
- **For Official Use Only (FOUO):** legacy marking now consolidated under CUI
- **Privacy Act / PII:** personal information protected under the Privacy Act of 1974
- **Protected Health Information (PHI):** health data subject to HIPAA
- **Proprietary data:** contractor proprietary and business-sensitive information
- **Export-controlled information:** ITAR / EAR controlled technical data

IL4 Security Requirements

IL4 builds on the FedRAMP Moderate baseline with additional DoD-specific (FedRAMP+) controls and requirements:

REQUIREMENT	IL4 SPECIFICS
Baseline Controls	FedRAMP Moderate baseline plus roughly three dozen CUI-specific controls and enhancements and DoD overlays. A FedRAMP High authorization also satisfies the IL4 control baseline.
Physical Location	Data stored and processed within the United States or U.S. territories, in facilities under exclusive U.S. legal jurisdiction
Personnel	Access limited to U.S. persons (U.S. citizens, U.S. nationals, or lawful U.S. persons) with appropriate background investigations; no foreign-person access
Encryption	FIPS 140-2 / 140-3 validated cryptographic modules for data at rest and in transit
Network	Strong virtual/logical separation from non-DoD tenants; NIPRNet connectivity through a DISA Cloud Access Point (CAP/BCAP) — no direct public-internet path
Incident Response	Cyber-incident reporting to DoD within 72 hours of discovery (DFARS 252.204-7012); coordination with the DoD CIRT
Vulnerability Mgmt	ACAS-compatible scanning and DISA STIG compliance, with remediation timelines per the SRG

IL4 Authorization Process

- **FedRAMP baseline first:** the CSO must hold a current FedRAMP authorization (Moderate minimum; High accepted)
- **DoD SRG gap analysis:** identify the additional FedRAMP+ controls and requirements beyond the FedRAMP baseline
- **DISA assessment:** DISA reviews the CSP documentation and assesses non-inherited requirements
- **Provisional Authorization (PA):** DISA grants an IL4 PA, generally aligned to the FedRAMP authorization cycle (typically up to three years)
- **Continuous monitoring:** ongoing compliance monitoring aligned with DoD requirements

Impact Level 5 (IL5) Requirements

Impact Level 5 is designed for higher-sensitivity CUI and unclassified National Security Systems (NSS). It is the highest unclassified impact level and applies to mission-critical DoD workloads where compromise would cause serious damage.

Data Types Authorized for IL5

IL5 environments may process all IL4 data types, plus:

- **Higher-sensitivity CUI:** CUI requiring enhanced protection based on organizational and mission assessment
- **Unclassified National Security Systems (NSS):** unclassified NSS information categorized per CNSSI 1253
- **Mission-critical data:** information essential to DoD operations where compromise would cause serious damage

IL5 Enhanced Security Requirements

IL5 adds significant requirements beyond IL4:

REQUIREMENT	IL5 ENHANCED REQUIREMENTS
Baseline Controls	Full FedRAMP High control baseline plus NSS overlays and DoD FedRAMP+ parameter adjustments
Physical Isolation	Dedicated, physically separated infrastructure — no shared tenancy with non-DoD or non-federal-government tenants
Network	NIPRNet connectivity via a DISA Boundary Cloud Access Point (BCAP); no direct internet; CAC/PIV authentication for DoD users
Personnel	Access restricted to U.S. citizens — stricter than IL4's U.S.-persons allowance — with DoD-approved background investigations
Encryption	FIPS 140-2 / 140-3 validated modules (AES-256); NSA-approved cryptography where required for NSS data
Monitoring	Enhanced continuous monitoring with SIEM integration and 24/7 SOC operations
Incident Response	72-hour cyber-incident reporting (DFARS) with expedited coordination for critical and NSS events; direct engagement with the DoD CIRT / US-CERT

IL4 vs. IL5: Key Differences

ASPECT	IL4	IL5
Tenant separation	Strong virtual / logical separation	Physically dedicated, isolated infrastructure

ASPECT	IL4	IL5
Network	NIPRNet via CAP/BCAP (no direct internet)	NIPRNet via BCAP (no direct internet)
Personnel	U.S. persons	U.S. citizens only
Data types	Standard CUI, FOUO, PII/PHI	Higher-sensitivity CUI, mission-critical, unclassified NSS
Baseline	FedRAMP Moderate + CUI controls	FedRAMP High + NSS overlays
Typical timeline*	~90–120 days on IL-authorized infrastructure	~120–180 days on IL-authorized infrastructure

** Estimates assume deployment on already-authorized IL infrastructure. Actual timelines vary by mission owner, sponsor, scope, and assessor availability.*

FedRAMP & DoD IL Relationship

FedRAMP authorization is the foundation for DoD cloud authorization. Understanding how the FedRAMP baselines map to the DoD Impact Levels is critical for planning your pathway.

FedRAMP Baseline to DoD IL Mapping

FEDRAMP BASELINE	SUPPORTS DOD IL	ADDITIONAL DOD REQUIREMENTS
FedRAMP Moderate	IL2 (reciprocity); IL4 minimum	DoD reciprocity for IL2; CUI controls, DoD overlays, and NIPRNet/CAP connectivity for IL4
FedRAMP High	IL5 (required); also satisfies IL4	NSS overlays, physical isolation, U.S.-citizen access, and BCAP connectivity for IL5

Reciprocity and Inheritance

When you deploy on DoD-authorized infrastructure, you benefit from:

- **Control inheritance:** inherit 300+ infrastructure and platform controls already assessed under the provider's DISA authorization
- **Reduced assessment scope:** your assessment focuses only on customer-responsible, application-layer controls
- **Accelerated timeline:** months rather than the 12–18+ months typical of a greenfield authorization
- **Continuous compliance:** the provider maintains underlying infrastructure compliance and continuous monitoring

> **INFRASTRUCTURE VS. APPLICATION CONTROLS**
> GovDataHosting guarantees the infrastructure- and platform-layer controls and provides inheritance documentation. Customers remain responsible for implementing and documenting their **application-layer** controls within the shared-responsibility model.

CMMC Alignment

The Cybersecurity Maturity Model Certification (CMMC) is related to, but distinct from, DoD IL requirements:

- **CMMC Level 2:** aligns with NIST 800-171 and is required for CUI — supported by IL4 infrastructure
- **CMMC Level 3:** adds a subset of NIST 800-172 enhancements for critical programs — supported by IL5 infrastructure
- **Infrastructure vs. organization:** CMMC certifies a contractor's practices, while an Impact Level certifies the hosting infrastructure. Both may be required.

GovDataHosting DoD Authorization Status

GovDataHosting's own platform is authorized at DoD IL2. For IL4 and IL5 workloads, GovDataHosting deploys and manages your environment on AWS GovCloud, which holds DISA IL4/IL5 Provisional Authorization — all under one managed, single-source engagement.

GOVDATAHOSTING CLOUD PLATFORM (NATIVE IAAS)	GOVDATAHOSTING-MANAGED AWS GOVCLOUD (IAAS)
• FedRAMP High (Class D) Certified • DoD IL2 Authorized • 300+ NIST 800-53 Rev 5 controls inherited • CMMC Level 2–ready infrastructure	• FedRAMP High authorized IaaS • DoD IL4 & IL5 Provisional Authorization (DISA) • Supports CUI, mission-critical, and unclassified NSS workloads • CMMC Level 2/3–ready infrastructure

DoD Authorization Process

This section outlines the process for achieving DoD authorization for your mission system when deploying on IL4/IL5-authorized infrastructure.

Phase 1 — Preparation (Weeks 1–4)

- **Determine the Impact Level:** analyze data types and mission requirements to select IL4 or IL5
- **Define the system boundary:** clearly separate CSP-inherited and customer-responsible scope
- **Gather documentation:** collect IaaS inheritance documentation and the Customer Responsibility Matrix (CRM)
- **Secure sponsorship:** identify the DoD sponsoring organization and Authorizing Official

Phase 2 — Documentation (Weeks 4–10)

- **System Security Plan (SSP):** develop the SSP leveraging the GovDataHosting compliance team and CSP control-inheritance statements
- **Control implementation:** document customer-responsible control implementations
- **Supporting plans:** develop IR, Contingency, and Configuration Management plans referencing inherited capabilities
- **POA&M:** document any findings requiring remediation

Phase 3 — Assessment (Weeks 10–14)

- **3PAO engagement:** engage a DoD-recognized Third Party Assessment Organization
- **Assessment execution:** the 3PAO assesses customer-responsible implementations (inherited controls excluded)
- **SAR development:** the Security Assessment Report documents findings
- **Remediation:** address assessment findings before authorization

Phase 4 — Authorization (Weeks 14–18)

- **Package submission:** submit the authorization package to the DoD Authorizing Official (AO)
- **AO review:** the AO reviews the package and accepts residual risk
- **ATO issuance:** Authority to Operate granted (typically a three-year term)
- **Operational status:** the system is authorized for DoD mission operations

Timeline Summary

SCENARIO	IL4 TIMELINE	IL5 TIMELINE
Using IL-authorized infrastructure (GovDataHosting-managed AWS GovCloud)	~90–120 days	~120–180 days
Using a FedRAMP High provider without a DoD IL PA	6–12 months	12–18 months

SCENARIO	IL4 TIMELINE	IL5 TIMELINE
Building in your own data center (no prior authorization)	12–24 months	18–36 months

Estimates only. Actual timelines depend on the sponsor, mission, scope, and assessor availability.

Implementation Checklist

Use this checklist to track your DoD authorization progress when deploying on GovDataHosting IaaS (IL2) or GovDataHosting-managed AWS GovCloud IaaS (IL4/IL5).

Pre-Authorization

- ☐ Determine the required Impact Level (IL4 or IL5) based on data sensitivity
- ☐ Identify the DoD sponsoring organization and Authorizing Official
- ☐ Obtain the GovDataHosting Customer Responsibility Matrix (CRM)
- ☐ Define the system authorization boundary
- ☐ Identify interconnections and data flows
- ☐ Engage a DoD-recognized 3PAO for assessment

Documentation

- ☐ System Security Plan (SSP) with inheritance documentation
- ☐ Security Assessment Plan (SAP)
- ☐ Incident Response Plan
- ☐ Contingency Plan
- ☐ Configuration Management Plan
- ☐ Privacy Impact Assessment (if applicable)
- ☐ Plan of Action and Milestones (POA&M)
- ☐ Interconnection Security Agreements (ISAs)

Technical Implementation

- ☐ Deploy the system on DoD-authorized IL4/IL5 cloud infrastructure
- ☐ Implement FIPS 140-2 / 140-3 validated encryption
- ☐ Configure CAC/PIV authentication (IL5)
- ☐ Apply DISA STIG configurations to all applicable components
- ☐ Configure audit logging and SIEM integration
- ☐ Implement ACAS-compatible vulnerability scanning
- ☐ Test incident-response procedures

Post-Authorization

- ☐ Implement a continuous monitoring program
- ☐ Schedule recurring vulnerability scans

- ☐ Establish a POA&M review cadence
- ☐ Configure DoD incident-reporting procedures
- ☐ Plan the annual security assessment
- ☐ Document change-management procedures

Next Steps with GovDataHosting

Ready to deploy your DoD mission system on authorized infrastructure? GovDataHosting provides the foundation you need for rapid DoD authorization.

Why GovDataHosting for DoD Workloads?

- **Authorized infrastructure:** the FedRAMP High (Class D) Certified GovDataHosting platform at DoD IL2, plus GovDataHosting-managed AWS GovCloud IaaS carrying DISA IL4/IL5 Provisional Authorization
- **Control inheritance:** 300+ infrastructure and platform controls inherited — you document only your application-layer controls
- **Accelerated timeline:** an estimated ~90–120-day IL4 path versus 12+ months without inheritance
- **24/7 U.S.-based SOC:** continuous monitoring — vulnerability scanning, POA&M management, and monthly ConMon reporting — staffed by U.S. citizens
- **U.S. data residency:** U.S. cloud data centers only, with U.S.-citizen support staff
- **CMMC support:** infrastructure that supports CMMC Level 2/3 requirements
- **Bundled, single-source:** infrastructure, security, monitoring, and compliance support in one engagement

FREE DOD AUTHORIZATION READINESS ASSESSMENT

Schedule a complimentary consultation with our DoD compliance experts to determine your required Impact Level and a realistic authorization timeline.

800-967-1004

www.govdatahosting.com/contact-us • **info@govdatahosting.com**

Additional Resources

- **NIST 800-53 Rev 5 High Baseline Control Matrix —** complete control mapping with inheritance guidance
- **FedRAMP Certification Playbook —** methodology for FedRAMP certification
- **Complete FISMA Authorization Guide —** step-by-step FISMA compliance guide
- **CMMC Compliance Overview —** understanding CMMC requirements for contractors

A Division of IT-CNP, Inc. • Founded 2001
FedRAMP High (Class D) Certified • DoD IL2 Authorized • NIST 800-53 Rev 5 High • SOC 2 Type II

DISCLAIMER

The information in this guide is accurate as of the date of publication. DoD cloud-security requirements — including the DoD Cloud Computing SRG, DISA Impact Level definitions and connection requirements, FedRAMP policy (notably the FedRAMP 20x transition and the 2026 Consolidated Rules), CMMC, and NIST 800-53 guidance — evolve over time and are subject to change. This guidance can change rapidly. Always verify the latest requirements at authoritative sources such as the DoD Cyber Exchange (public.cyber.mil), fedramp.gov, and nist.gov before making compliance decisions.