ARMIS® FEDERAL

WHITE PAPER

Understanding DISA's 2025 IL4/IL5 Changes

How Mission Owners Evaluate SaaS Vendors Like Armis

Understanding DISA's IL4/IL5 Changes

How Mission Owners Evaluate SaaS vendors like Armis

Recent updates released by the Defense Information Systems Agency (DISA) have simplified the long-standing confusion between FedRAMP and Department of Defense Impact Levels (IL) requirements for IL4 and IL5. The update provides clear boundaries moving forward:

- IL5 is to be used only for Non-Classified Internet Protocol Router (NIPR) Systems that are officially designated as a National Security System (NSS) by the sponsoring organization or mission owner.
- If a NIPR System is not designated as a national security system (NSS), IL4 is the authorized level.
- Mission Owners who choose to use Armis Government Cloud at the DoD IL4 will receive the enhanced benefits from the DoD IL5 uplift.

Overview

In July 2025, DISA updated the DoD Cloud Computing Security Requirements Guides (CC-SRGs), simplifying how Impact Levels are determined and applied. Previously, some Mission Owners requested "IL5 (non-NSS)" for added assurance, even when their systems were not National Security Systems. The new CC-SRG guidance eliminates this option and aligns IL levels directly to system mission type.

2025 releases:

- SRG V1R3: July 02, 2025
- SRG V1R4: August 13, 2025
- SRG V1R5: September 03, 2025
- Cloud Computing Mission Owner SRG: January 30, 2025
- DoD Rev 5 SSP Addendum Controls V1.2 (December 03, 2025)
- Committee on National Security Systems Instruction (CNSSI) No. 1253 (July 29, 2022)

Before July 2025 (CC-SRG v1R2)

Impact Level	Applicable Systems	Data Classification Alignment
IL4	Non-NSS systems processing CUI	Controlled Unclassified Information (CUI) (moderate–high confidentiality)
IL5 (Non-NSS) *Removed*	Sensitive but non-NSS systems (common misinterpretation)	CUI requiring higher protection; not mission-tied to NSS
IL5 (NSS)	National Security Systems	CUI in NSS + some mission-critical functions

After July 2025 (CC-SRG v1R4)

Impact Level	Applicable Systems	Data Classification Alignment	# of Applicable Controls
IL4	All non-NSS systems processing CUI	CUI (all types) in non-NSS enclaves	IL4 Moderate – 345 IL4 High- 430
IL5 (NSS Only)	Systems formally designated as NSS	NSS mission data; CUI supporting intelligence, C2, crypto, weapons, or classified missions	IL5 NSS - 588

What Does This Mean for Mission Owners Evaluating DISA Authorized SaaS Solutions?

For Mission Owners, the 2025 CC-SRG updates provide a far simpler path for determining whether an IL4 or IL5 Provisional Authorization (PA) is needed when selecting a SaaS CSP. The decision now comes down to one primary question:

Is the system connecting to the CSP/CSO officially designated as a National Security System, or not?

- **Yes?** - IL5 is required
- **No?** - IL5 is **not** required

What is NSS, NSI, and CUI?

Armis by function does not act in the capacity of an NSS and the Mission Owner ultimately makes the determination based on the capabilities they are using Armis for. Understanding whether your system handles National Security Information (NSI) or performs missions associated with National Security Systems (NSS) is the key factor in determining whether IL4 or IL5 applies when evaluating SaaS solutions.

National Security Systems (NSS)

A system is considered a National Security System when it performs one or more of the following mission types:

- Intelligence activities
- Cryptologic operations
- Command and control of military forces
- Weapons systems or direct support to weapons systems
- Processing classified National Security Information (NSI)

National Security Information (NSI)

National Security Information (NSI) refers to information formally classified under Executive Order 13526 because its unauthorized disclosure could harm national security. NSI falls into three levels:

- Top Secret (Not in scope of this document)
- Secret (IL6 - Not in scope of this document)

Confidential - (IL4/5) Examples:

- Defense system performance data
- Controlled strategic assessments or intelligence summaries
- Some classified procurement or logistics information
- Lower-level operational planning details
- Certain protected foreign government information
- Any system that stores, processes, or transmits NSI is, by definition, an NSS and must use accredited classified or IL5/IL6 cloud environments, depending on classification level

Controlled Unclassified Information (CUI)

CUI is unclassified information that requires safeguarding because its unauthorized release could impact operations, privacy, or mission execution. It is defined at the federal level under 32 CFR Part 2002 and implemented in the DoD through DoDI 5200.48.

CUI is common across most DoD enclaves and includes information such as:

- Unclassified medical or clinical system data
- Operational or logistical information
- Technical, engineering, or acquisition data
- Cybersecurity and system vulnerability information
- Facility, FRCS, or infrastructure data
- Personnel or privacy-related records

Who Governs NSS, NSI, and CUI?

The governing authorities that publish, define, and enforce these categories include:

- **U.S. Congress** - Provides the statutory definition of NSS in 44 U.S.C. § 3552.
- **Executive Office of the President / ISOO** - Establish classification rules for NSI under EO 13526 and oversee government-wide implementation.
- **Committee on National Security Systems (CNSS)** - Publishes CNSSI 1253, defining NSS mission categories and security requirements.
- **Department of Defense (DoD)** - Implements NSS and NSI rules via DoDI 8500.01, DoDI 8510.01, and DoDM 5200.01; implements CUI rules through DoDI 5200.48.
- **National Archives and Records Administration (NARA)** - Governs the Federal CUI Program under 32 CFR Part 2002 and maintains the CUI categories.

How do you check if your system is NSS?

To determine whether the enclave you're connecting from - or sending data to - is considered a National Security System (NSS), the easiest approach is to verify its official designation through your existing RMF and cybersecurity channels. An enclave is only NSS if it has been formally designated as one. Mission owners can reach out to their cybersecurity divisions that are generally aligned within the J6 or S6 directorates within the organization. They can assist with identifying the data collected and aggregated by Armis if it is considered sensitive enough in nature to support an NSS designation.

Who to ask or where to look:

- **Component cybersecurity offices** - (e.g., Army G-6, AF A6, USN N2/N6, DHA, COCOM J6) - maintain authoritative lists of NSS systems
- **System Authorizing Official (AO)** — the final authority on whether an enclave is formally designated as NSS
- **ISSM/ISSO** — maintains system classification records and can confirm NSS status immediately
- **Risk Management Framework (RMF) documentation** — check your System Security Plan (SSP) or Categorization Worksheet for any NSS designation

Evaluating Armis Government Cloud

When evaluating Armis and the Armis Government Cloud to enhance cybersecurity and visibility for your system, there are three main components that provide a secure, streamlined, reliable, and authorized connection:

- The Secure Cloud
- DISA SCCA Boundary Cloud Access Point (BCAP)
- Data Collection Options

The Secure Cloud

Armis Government Cloud is a secure, scalable, and DoD-dedicated SaaS environment hosted in AWS GovCloud (US) and purpose-built to meet the stringent controls of the DoD cloud requirements.

Armis maintains an active IL5 conditional Provisional Authority (PA), with full NSS controls implemented with a completion date of June 2026.

Armis Government Cloud Security Controls:

- **Security & Compliance:** NIST 800-53 Rev 5 IL5 compliant, administered by U.S. persons, aligned with DoD and SCCA.
- **VDSS:** Full encryption for data in transit and at rest.
- **Continuous Monitoring:** Platform integrity, behavioral anomaly detection, intrusion detection, and security analytics.
- **Access Control & Zero Trust:** Mission Owners use Public Key Infrastructure (PKI) and Role-Based Access Control (RBAC); least privilege, continuous identity validation, and Zero Trust enforced.
- **Auditing & Compliance:** Routine 3PAO assessments and testing. Monthly audit submissions to DISA RE2.

DISA SCCA BCAP

Note: *Mission Owners may also use their own DISA-authorized BCAP.*

The DISA Secure Cloud Computing Architecture (SCCA) Boundary Cloud Access Point (BCAP) provides the authorized policy-enforced gateway enabling connectivity from Mission Owner systems into Armis Government Cloud dedicated tenants. The BCAP ensures data integrity and ownership from end-to-end, without breaking the system air gap.

Key Advantages for Mission Owners:

- Pre-Validated, DISA-Aligned Architecture
  - Armis Government Cloud's design aligns to SCCA requirements and Virtual Data Security Stack (VDSS) standards
  - Reduces engineering effort for Mission Owners

- Faster Connection Authorization
  - Pre-established templates and technical artifacts accelerate BCAP approval steps
  - Minimizes delays commonly associated with new cloud integrations

Data Collection Options

To provide full visibility and intelligence into on-premises assets, Mission Owners can deploy a lightweight and non-disruptive Armis Virtual Collector that gathers and forwards integration and network asset data through the secure BCAP to the dedicated Armis Government Cloud tenant.

The collector performs three complementary types of asset data collection:

1. REST API Integrations

Secure, automated connections with existing systems, such as:

- Endpoint Detection and Response (EDR) platforms
- Identity/Access Management (IAM)
- Active Directory, SCCM, Tanium
- Vulnerability scanning tools
- Virtualization and OT/Facility-related Control Systems (FRCS) management platforms

2. Passive Network Traffic Analysis (SPAN/TAP)

- Identifies unmanaged/rogue devices and communication patterns
- Enables deep network behavior visibility without disruption
- Collector ingests raw network traffic from SPAN ports or TAP architectures
- Payloads containing classified data (PHI, PII, C2, etc.) do not leave the enclave

3. Safe, Mission Owner–Controlled Active Querying (Optional)

All queries are non-disruptive and controlled by the Mission Owner. Used to safely enrich device profiles with:

- OS and firmware versions
- Running services and open ports
- Basic configuration details

Data Flow Summary: What is Sent and Stored in Armis Government Cloud

Armis Virtual Collectors ingest network traffic and integration data, removes sensitive and classified information, and securely forwards only necessary header, metadata, and integration data such as:

- IP/MAC, hostnames, device identifiers
- OS/firmware versions
- Ports, protocols, network behavior
- Vulnerability summary data
- Certificate and posture attributes.

The Armis Asset Intelligence Engine then analyzes the data and automatically organizes and reports the findings into the user interface.

Example Current Systems Armis can Support (IL4 + IL5 non-NSS Controls)

Mission Owners can use Armis Government Cloud today if their system is not registered as NSS and handles data within IL4 limits (primarily CUI). Examples of NIPR non-NSS networks include:

- **Enterprise NIPR IT environments** (e.g., base/installation networks, enterprise workstations, servers, VoIP, WLAN)
- **FRCS / OT operational networks** (HVAC, power, security systems, building automation)
- **Medical enclaves handling unclassified patient-care systems** (IoMT devices, medical equipment, and blended IT systems)
- **Logistics, readiness, and installation-support systems** (unclassified logistics, inventory, fleet management, maintenance systems)

Conclusion

The DISA 2025 CC-SRG updates have successfully clarified the path for Mission Owners, establishing a simple binary choice: IL5 is now reserved exclusively for formally designated National Security Systems (NSS) on NIPR, while IL4 is the standard for all non-NSS systems processing CUI. The Armis Government Cloud is strategically positioned to meet this new guidance, offering a secure, DoD-dedicated environment with an active IL5 conditional Provisional Authorization, with full NSS controls implemented with a completion date of June 2026. By choosing Armis Government Cloud, Mission Owners can future-proof their cybersecurity posture, ensuring compliance and superior asset visibility regardless of their system's specific IL4 or IL5 NSS status.

ARMIS® FEDERAL

Operationalize these insights.

See how Armis Centrix™ delivers the situational awareness and risk management demanded by this report.

Book a Federal Demo

Armis Centrix™ is a FedRAMP and IL authorized solution for the U.S federal government.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armisfederal.com