

# Leveraging Splunk for U.S. DoD IL5

Drive mission success with data-driven decisions



Data Analytics



Save time and  
resources



Rapid deployment



Compliant and  
secure

Defense and intelligence agencies succeed or fail based on their ability to collect, report, and analyze data to support enhanced decision making. But to be useful, agencies need to analyze vast amounts of data quickly and to scale their data analysis platforms to cope with rapidly evolving threats.

Cloud computing technologies allow the U.S. Department of Defense (DoD) to consolidate infrastructure, leverage commodity IT functions and eliminate functional redundancies while improving operations. But up to now, much of the information that is most valuable to defense and intelligence decision makers could not be migrated to non-government cloud providers due to stringent compliance requirements for DoD Impact Level 5 (IL5) data.

Given the gravity of security concerns when it comes to the U.S. DoD, the Defense Information Systems Agency (DISA) has developed a DoD Cloud Computing Security Requirements Guide (SRG) to define the models, requirements, and controls cloud service providers (CSPs) must meet for their cloud service offerings (CSOs) to be considered for use across respective impact levels.

According to the SRG, IL5-protection includes information categories such as critical infrastructure, defense, export controls, budget/financial, intelligence, law enforcement, nuclear energy, and individual privacy data. It also includes the requirements in NIST SP 800-171, intended for use by federal agencies in contracts or other agreements established with non-federal organizations.

IL5 authorization also applies to information systems that are identified as national security systems (NSS). An NSS, according to NIST SP 800-59, is any information system used by an agency that involves activities related to intelligence, national security cryptologic, command and control of military forces, equipment integral to weapons systems, and any other functions critical to direct fulfillment of military or intelligence missions.

## Splunk Cloud Platform Is DoD IL5

### Authorized

Splunk Cloud Platform, a SaaS cloud service offering hosted in AWS GovCloud(US), has achieved U.S. DoD authorization at IL5. The service is designated as a U.S. government community cloud, and is initially available to U.S. federal agencies who can access the service via the Defense network (NIPRnet). For this offering, service delivery and support are performed by U.S. Citizens, on U.S. soil. Splunk Cloud Platform with DoD IL5 authorization is now available for sale on the Defense Information Agency Store. Federal agencies can now use Splunk to meet the specific challenges they face when using cloud computing to address a variety of data analytics and AI use cases — with confidence, and at mission speeds.

### Rapid Deployment to the Splunk Cloud Platform

The availability of the Splunk Cloud Network on the DISA Storefront (CAC enabled: <https://www.disa.mil/Services>) simplifies procurement and accelerates migrating an agency's data and workloads to the cloud. Splunk can often build the IL5 cloud stack within a week.

### Compliance

Federal agencies must be sure the cloud products and providers they use are fully compliant with regulatory mandates. Agencies are mandated to procure and use only U.S. DoD authorized cloud service providers. They must also follow a mandate under the Defense Federal Acquisition Regulation Supplement (DFARS) to only use systems that comply with NIST SP 800-171, which protects controlled unclassified information in non-federal systems.

The NIST SP 800-53 controls that comprise FedRAMP High Impact Level baseline are a superset of NIST SP 800-171 referenced controls. Splunk Cloud Platform with FedRAMP High baseline is compliant with applicable requirements specified under DFARS section 252.204-7012(b)(2) (ii)(D) and NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).

### Splunk Single Tenant Deployment Model

Splunk Cloud Platform also adheres to some of the most rigorous security and compliance standards. Its “single tenant” deployment model offers extra protection and data isolation so that each customer has their own dedicated instance of the Splunk Cloud service. Splunk Cloud Platform is also encrypted, meeting both FedRAMP and IL5 cryptographic requirements for data protection at rest and in transit. Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules are employed for data encryption. So, no Splunk employee has access to the customer/Agency without prior approval/request by the customer for a highly limited work order engagement.

### Time and Resources

USG agencies have limited time and resources and must often manage and maintain their own infrastructures. Data ingestion, normalization, modeling, and curation take a lot of time and resources, and don't always deliver optimal results. Agencies need fast, flexible cloud solutions to save time and accelerate time-to-value and keep the total cost of ownership low.



Contact us: [splunk.com/asksales](https://splunk.com/asksales)

[splunk.com](https://splunk.com)

Splunk Cloud Platform allows users to ingest any text-based data, in any format, in near real time, providing automatic correlation and saving the time it takes to manually curate data models. With Splunk Cloud Platform, agencies can go live fast, accelerating time- to-value in as quickly as two days. As a subscription service, agencies don't need to provision or manage infrastructure and can focus their scarce and valuable resources on strategic initiatives instead. There are 700+ Splunkbase apps validated for Splunk Cloud Platform that provide analytics, alerts, dashboards, and visualizations, ready to use.

## Data analytics

In addition to being time and resource intensive, data ingestion, normalization, modeling, and curation can also be very complex activities requiring multiple analytics tools and products. A single organization-wide solution will help agencies to scale and provide holistic visibility and analytics.

Splunk Cloud Platform is a single solution that provides end-to-end visibility, tools for auditing, and complete analytics. By ingesting data from any source regardless of format and type, in real time, Splunk Cloud Platform helps agencies streamline processes and eliminate many of the manual tasks that can overcomplicate data analytics. It also provides granular, real-time situational awareness and insight across hybrid environments, eliminating any blind spots and providing an accurate picture of uptime, availability and any other relevant metrics.

## Terms and Conditions

This Solution Guide is for informational purposes only. The services described in this datasheet are governed by the applicable fully signed ordering document and any incorporated terms and conditions.

Splunk Cloud Platform is also scalable and architected to facilitate sudden or unexpected bursts in data volume, quickly expand deployment to meet mission requirements, and provide flexible time periods for data retention.

## Service and Billing

USG agencies require adequate visibility into cloud providers' service availability and other resources needed to troubleshoot potential issues. Predictable cost at the end of each billing cycle is also an important consideration for agency budget management.

Splunk Cloud Platform is operated by Splunk experts and relieves agencies of the people, processes and systems required to run Splunk on-premises. The platform offers a resilient infrastructure and services with a 24/7 NOC/SOC support team as well as independent service delivery.

Splunk Cloud Platform handles upgrades and updates and can also help monitor cloud usage so that agencies have a real-time understanding of resources consumed. This way, there are no surprises at the end of the billing period.

Splunk Cloud Platform enables US Government agencies to ingest data once and bring that data to every question, action and decision across multiple use cases. Splunk Cloud Platform meets the FedRAMP security standards, has the additional IL5 authorization, and helps U.S. federal agencies and their partners drive confident decisions and decisive actions at mission speeds. Learn more about Splunk Cloud Platform or [contact us](#) to discuss your needs and requirements.



Contact us: [splunk.com/asksales](https://splunk.com/asksales)

Learn more about Splunk Cloud Platform or contact us to discuss your needs and requirements. [splunk.com](https://splunk.com)

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2024 Splunk LLC. All rights reserved.