



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

21 June 2024

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Cloud Computing Security Requirements Guide (SRG)

Reference: Department of Defense Instruction 8500.01, Cybersecurity, dated March 14, 2014

Department of Defense (DOD) Instruction 8500.01 directs that the Defense Information Systems Agency (DISA) “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders.” It also directs DOD Component heads to “ensure that all DOD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs.”

This version of the Cloud Computing SRG is the transition from NIST 800-53 Rev 4 to NIST 800-53 Rev 5 and addresses the requirements in CNSSP-32 for National Security Systems. This document does not contain information on NIST 800-53 Rev 4 requirements. The Cloud Computing SRG consist of two parts, a Mission Owners (MO) document and a Cloud Service Provider (CSP) document.

The MO document is in two parts: a MO Overview PDF and a STIG. Both documents contain information on the MO responsibilities for DOD CAC/PKI, Active Directory, Endpoint Security, Cloud Storage, Data-at-Rest encryption, and contract requirements for cloud activities. The MO documents focus on the MO responsibilities, while the CSP document focuses on CSP requirements. Mission Owners are highly encouraged to read and understand the CSP requirements.

The CSP document contains information that addresses the minimum requirements for security investigations, and the RMF baselines for NIST 800-53 Rev 5 based on CNSSI 1253. A significant change is that the baseline requirement for Impact Level 5 and higher requires a high baseline. The FEDRAMP+ controls focus on the difference between FEDRAMP and DOD variables/baselines for Impact Level 4 and higher. The document allows Just in Time or Just Enough Access for CSP personnel, providing the benefit of lowering the security investigation requirement. Other changes focus on clarifying requirements or removing information that is no longer relevant.

UNCLASSIFIED

In accordance with DOD Instruction 8500.01, the Cloud Computing SRG is released for immediate use. The document is available on <https://cyber.mil/> and <https://public.cyber.mil>.

Point of contact for this action is DISA STIG Support Desk, email: disa.stig_spt@mail.mil.

JACQUELINE P. SNOUFFER
Director, Risk Management Directorate
DISA Authorizing Official

UNCLASSIFIED