



DEFENSE INFORMATION SYSTEMS AGENCY

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

IN REPLY
REFER TO: Risk Management Executive (RME)

12 January 2015

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Cloud Computing (CC) Security Requirements Guide (SRG) Version 1

Reference: DoD Directive 8500.1

1. DoD Instruction 8500.01 tasks DISA to develop security requirements guides (SRGs) that implement DoD cybersecurity policies, standards, architectures, security controls, and validation procedures. This SRG defines the baseline security requirements for commercial and DoD Cloud Service Providers hosting DoD Information, Systems, and Applications; and for DoD Mission Owner's use of commercial and DoD cloud Services. This guidance is based on the DOD Instruction 8510.01, Risk Management Framework, leveraging the processes defined as part of the Federal Risk and Authorization Management Program FedRAMP V2 using NIST SP 800-53 Rev 4 control requirements.
2. This first version of the CC SRG incorporates comments from industry and DoD, recognizing that a number of inputs were deferred for additional research. Every attempt was made to fully incorporate inputs that would impact cost or speed of delivery with the primary focus on achieving the right risk balance for level 2 and level 4 processing (see section 4 for level definitions).
3. We project quarterly SRG updates with the next update focused on requirements for Impact Level 5 processing and considerations for hosting DoD workloads outside of US facilities.
4. In accordance with DoD Instruction 8500.01, the CC SRG Version 1 is released for immediate use. The document is available on <http://iase.disa.mil>.
5. Point of contact for this action is FSO STIG Support Desk, email: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

MARK S. ORNDORFF
Risk Management Executive