DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

REVISION HISTORY

For

Version 1, Release 2

18 March, 2016

Developed by the
Defense Information Systems Agency
for the
Department of Defense

Revision Date	Change Type	Description of Change
18 Mar. 2016	FINAL Version 1 Release 2	Released final signed document
	Administrative Changes	• Many administrative corrections and changes throughout • Updated the CND/CD lexicon to that defined in new Cyber Defense policy DRAFT DoDI 8530.01 and JP 3-12 (R) throughout (except in the revision history for v1r2 draft for public comment)
	Clarifications and Explanations	• Section 1 - INTRODUCTION RE: The definition of Mission Owner; Further explained the definition RE: The definition of DoD CSP; Added milCloud as an example. RE: The definition of CSO; revised for clarity and to remove circular reference; added examples RE: The definition of Commercial Cloud Service; removed it RE: The definition of DoD Cloud Service Catalog; added it RE: The definition of • Provisional Authorization (PA): added a pointer to the PA Section 2.6 • Section 1.1 - Purpose and Audience RE: use of A&A in the CC SRG • Section 1.3 - Scope and Applicability RE: CC SRG applicability to Mission Owners, CSPs, integrators, brokers and subcontracts/subcontractors, Non-DoD CSOs vs commercial CSOs, future coverage of PaaS, etc. • Section 2.1 - Cloud Computing, Cloud Service, and Cloud Deployment Models RE: the categorization of non-standard service models. • Section 2.6 - DoD Provisional Authorization RE: PA revocation WRT leveraged CSOs and contracts RE: the note on physical facilities housing CSOs to add a cross reference to classified facilities assessment/approval • Section 3.2.4 - Level 4: Controlled Unclassified Information RE: Definition of CUI and related policies and resources. • Section 4.1 - Assessment of Commercial/Non-DoD Cloud Services RE: the assessment of DoD requirements for CSOs w/ FedRAMP listed Non-DoD Agency ATOs needing to have FedRAMP+ C/CE assessed by a 3PAO and results submitted to the DoD SCA.; parallel assessments using the same 3PAO. RE: Level 6: Added/Revised assessment requirements IAW OUSD(I) and DSS guidance for commercial facilities; Added assessment of DoD on-premises facilities/CSOs • Section 4.3.1 - Cloud Computing, Authorization Boundaries RE: Authorization boundaries • Section 4.4 - CSP Transition from CSM v2.1 to CC SRG v1r1 and Subsequent Updates RE: transition between versions of the CC SRG; definition of FedRAMP v2 vs 2.0 • Section 5.1.2 - DoD FedRAMP+ Security Controls/Enhancements RE: SA-12 and SA-19 to FedRAMP + in support of SCRM, and IR-05 (01) in support of LE/CI and forensics • Section 5.1.5 - CNSSI 1253 Privacy Overlay

Revision Date	Change Type	Description of Change
		RE: explanation of the Privacy Overlay and why it is invoked by DoD. • Section 5.2.2 - Cloud Deployment Model Considerations / Separation Requirements RE: moved the last paragraph RE "ITAR" clouds to 5.2.2.3 Level 5 for a better fit. • Section 5.2.2.1 - Impact Level 2 Location and Separation Requirements AND Section 5.2.2.2 - Impact Level 4 Location and Separation Requirements RE: split previous Section 5.2.2.1 Impact Level 2 Location and Separation Requirements and further explain the strong virtual separation controls requirements • Section 5.2.2.3 - Impact Level 5 Location and Separation Requirements RE added paragraph about "ITAR" clouds; added restriction to US Citizens • Section 5.2.2.4 - Impact Level 6 Location and Separation Requirements formerly 5.2.2.3 RE Location IAW 5.2.1; virtual separation • Section 5.3.1 - Continuous Monitoring RE: continuous monitoring artifacts required to maintain a DoD PA. RE: recommendation to use NIEM based XML for CM reporting. RE: FedRAMP and DoD annual assessments being coordinated as one. • Section 5.4.1.1 - Mission Owner Credentials for CSP and Mission System Interfaces Table 4 - Mission Owner Credentials RE: clarified the column headings Section 5.6.2.2 - CSP Personnel Requirements – PS-3: Background Investigations RE: Level 6 process/requirements for getting a facilities clearance RE personnel clearances • Section 5.8 - Data Retrieval and Destruction for Off-boarding from a CSO RE: added a cross reference to Section 5.2.3 - DoD Data Ownership and CSP Use of DoD Data (Formerly 5.5.2). • Section 5.10.1 - Cloud Access Point (CAP) RE: definition, use, and applicability; DMZ extension capability bullet; Level 6 – removed BCAP requirement; addresses SIPRNet connection approval. ICAP requirements and connection approval • Section 5.10.1.1 - Mission Partner Environments or Communities of Interest Network Cloud Access Points RE: the definition of "Mission Partner" as used in the CC SRG. • Section 5.10.3 - CSP Service Architecture RE: virtualization security and defense-in-depth. • Section 5.10.4 - Internet Protocol (IP) Addressing and Domain Name Services (DNS) RE: updated DoDI 8410.01 language and applicability to cloud; added a note RE public/private IP addresses • Section 5.10.4.1 - IP Addressing RE: addressing requirements for Level 2 and Levels 4/5; CSO not being able to use DoD IP addresses. • Section 5.10.6 - Mission Owner System/Application Requirements using IaaS/PaaS RE: the provisioning of DMZ protections in Level 4.

Revision Date	Change Type	Description of Change
		• Section 6.3 - Cyber Defense Roles and Responsibilities and Appendix C - Roles and Responsibilities RE: BCD providing MCDs timely access to BCD-collected indications and warnings relevant to MCD subscribers. • Section 6.8 - PKI for Cyber Defense Purposes RE: The use of DoD PKI for Cyber Defense communications. • Appendix D - CSP Assessment Parameter Values for PA RE: clarified the value for AC-8 RE DoD banner. RE: The value for AU-11 added link to NARA web site RE: The value for MA-6 WRT CSO SLA RE: The value of PE-4, 5, and 7 to qualify and replace the time frame of immediately which is not realistic. Adjusted IAW Privacy overlay focus group. RE: The value for SC-10 WRT replaced "in-band management" with "privileged sessions" • Appendix F - FUTURE Privacy Overlay RE: Deleted the annex content and renamed it Appendix F FUTURE Privacy Overlay Guidance
	Added Information or Expanded Guidance / Requirements	• Section 3.2 - Information Impact Levels RE updated Figure 1 – Impact Level Comparison for the following: o Level 4 - Limited "Public" Community Cloud o Level 6 – removal of SIPRNet CAP and restriction to on-premises • Section 3.2.6 - Level 6: Classified Information up to SECRET RE: removed references to applicable controls and NISPOM since this is the definition of Level 6 only • Section 3.2.7 - Beyond Level 6: CSOs for Classified Information above SECRET RE: removed the section to alleviate confusion and any potential inaccuracy • Section 4.1 - Assessment of Commercial/Non-DoD Cloud Services RE: changes in CSP ownership; removed L6 from L4/5/6 topic; added a level 6 section for off-premises CSOs; clarified A&A policy references; added a note about the need for coordination between DoD RMF and OUSD(I)/DSS Industrial security policies, procedures, and requirements for A&A. • Section 4.2 - Assessment of DoD Cloud Services and Enterprise Services Applications RE: added a separate Level 6 assessment section for on-premises CSOs • Section 4.5 - DoD PA in Relation to RFP Response and Contract Award RE: DISA SCA involvement in the contracting process if a CSO does not already have a DoD PA on contract award. • Section 5.1.5.3 - CSO Assessment of Privacy Overlay Control/Control Enhancements RE: Assessment of PaaS CSOs intended to handle PII/PHI against the Privacy Overlay. • Section 5.1.4.1 - NSS Level 6 Classified Overlay Applicability RE: revised so existing CC SRG requirements are for on-premises CSOs and discussed NISP policies and general

Revision Date	Change Type	Description of Change
		requirements for off-premises CSOs • Section 5.1.6 - Security Controls/Enhancements to be optionally addressed in the Contract/SLA RE: Moved SA-12 and SA-19 to FedRAMP + in support of SCRM • Section 5.2.3 - DoD Data Ownership and CSP Use of DoD Data (Formerly 5.5.2) RE: Refined / revised this section for clarity and to address DoD vs CSP data ownership. • Section 5.2.2.5 - Separation in Support of Law Enforcement and Criminal Investigation RE: Added separation of Federal and Non-Federal government information in support of LE/CI investigations of Federal Government employees and elected officials as well as anyone with access to Federal Government information. • Section 5.3.1 - Continuous Monitoring RE: the use of NIEM based XML for CM reporting. • Section 5.6.2 - CSP Personnel Requirements RE: stipulated implied limitations on CSP personnel WRT national affiliation. • Section 5.6.2.2 - CSP Personnel Requirements – PS-3: Background Investigations RE: modified for on vs off premises CSOs WRT facilities and personnel clearances; Added NISP references for contractors • Section 5.10.1 - Cloud Access Point (CAP) RE: better explained DoD DMZ in association w/ CAP. RE: Level 4/5 CSP/CSO infrastructure/applications and DoD Mission Owner applications being able to operate through the CAP without a dependency for any traffic needing to traverse the IAPs. • Section 5.10.4 - Internet Protocol (IP) Addressing and Domain Name Services (DNS) RE: Revised the entire section splitting DNS and IP addressing into separate sections for clarity. RE: Revised for better coverage of the topics and areas where the mission owner does not have control over IP addressing. • Section 5.18 - Supply Chain Risk Management Assessment RE: requirements for a CSP to provide a SCRM plan for review for a DoD PA; moved SC-12 and SA-19 from the SLA table to the FR+ table for Levels 4, 5, and 6 • Section 5.195.18 - Electronic Mail Protections IAW TASKORD 12-0920 RE: Email security and hygiene • Section 6.3 - Cyber Defense Roles and Responsibilities RE: Replaced Figure 10; Added Figure 11; added/updated descriptions for Figured 10 & 11 • Section 6.1 - Overview of Cyber Defense Tiers RE: added references and a note RE DRAFT DoDI 8530.01 and JP 3-12 (R) and the replacement of O-8530.1 • Section 6.4.4.2 - Incident Information Collection, Preservation, and Protection RE: Added IR-5(1) to FedRAMP+ in support of automated collection, preservation, and protection • Appendix A - References RE: Added a reference to 8320.07

Revision Date	Change Type	Description of Change
		RE: added references and a notes RE DRAFT DoDI 8530.01 and JP 3-12 (R) RE: Added references to DoD 5220.22-R; 48 CFR Subpart 4.4; FAR 52.204-2 WRT industrial security regulations as driven by public law
23 June 2015	DRAFT Version 1 Release 2	Released for public Comment
	Administrative Changes	• Many administrative corrections and changes throughout • Revised organization names IAW DISA reorganization
	Clarifications and Explanations	• Section 1 - Introduction RE: the definition of Mission Owner and the relationship to a DoD Component ; Added a definition for C/CE. • Section 1.1 - Purpose and Audience RE: Simplification of the first paragraph and to better explain the purpose bullets • Section 1.3 - Scope and Applicability RE: CSP subcontracting, SRG primary focus, internal and external IT Services per DoDI 8510.01. • Section 1.4 - Security Requirements Guides (SRGs) / Security Technical Implementation Guides (STIGs) RE: applicability to Mission Owners and CSPs. • Section 1.6 - Document Revisions and Update Cycle RE the submission of Comments, Proposed Revisions, and Questions being accepted at any time. • Section 2.1 - Cloud Computing, Cloud Service, and Cloud Deployment Models RE: Cloud service model definitions and use of private and community in the SRG. • Section 2.4 - Federal Risk and Authorization Management Program (FedRAMP) RE: the description/definition of FedRAMP and the acceptance of FedRAMP Agency ATOs • Section 2.6 - DoD Provisional Authorization RE: Definition of a DoD PA; CSP subcontracting; PA revocability; PA listing. • Section 3.1 - Security Objectives (Confidentiality, Integrity, Availability) RE: The categorization of information. • Section 3.2 - Information Impact Levels RE: Revised figure 1 • Section 3.2.2 - Level 2: Non-Controlled Unclassified Information RE: C and I level accommodated • Section 3.2.4 - Level 4: Controlled Unclassified Information RE: C and I level accommodated; noted Privacy rider • Section 3.2.5 - Level 5: Controlled Unclassified Information RE: C and I level accommodated; noted Privacy rider • Section 3.2.6 - Level 6: Classified Information up to SECRET

Revision Date	Change Type	Description of Change
		RE: C and I level accommodated; added footnotes • Section 4 - RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS RE: choosing a CSP's CSO possessing a PA and AO leveraging • Section 4.1 - Assessment of Commercial/Non-DoD Cloud Services RE: Level 2 use of FedRAMP Agency ATOs; Level 2 award of DoD PA; Level 4/5/6 DoD PAs; DoD component assessed PA and its listing on FedRAMP; "Other SCA organizations". • Section 4.2 - Assessment of DoD Cloud Services and Enterprise Services Applications RE: DoD RMF applicability vs FedRAMP • Section 4.3.3 - Mission Risk RE: MO's use of DoD PA and inheritance • Section 5 - SECURITY REQUIREMENTS RE: the categories of security requirements covered in the section • Section 5.1.1 - DoD use of FedRAMP Security Controls RE: assessment for Level 2 PAs • Section 5.1.2 - DoD FedRAMP+ Security Controls/Enhancements RE Coverage of availability; how selected; N/A in level 6 of Table 2; Also moved the overlay discussion paragraphs to new sections and referenced them; • Section 5.1.3 - Parameter Values for Security Controls and Enhancements RE: Applicability and sources of parameter values • Section 5.2.1 - Jurisdiction/Location Requirements RE: reorganized the section and sub bullets for improved clarity ;coordination with DFARS; related control; added subsections for on-premises 5.2.1.2 and Off-premises 5.2.1.1 • Section 5.2.2 - Cloud Deployment Model Considerations / Separation Requirements RE: dedicated infrastructure; Shared/Multi-tenant/public; ITAR compliant; related control • Section 5.2.2.1 - Impact Level 2 Location and Separation Requirements RE dedicated infrastructure; virtual separation • Section 5.2.2.2 - Impact Level 4 Location and Separation Requirements RE: restricting L4 to a “Government Community” w/ access by "US Persons" • Section 5.2.2.3 - Impact Level 5 Location and Separation Requirements RE dedicated infrastructure; virtual separation • Section 5.2.2.4 - Impact Level 6 Location and Separation Requirements RE dedicated infrastructure; virtual separation; restriction to On-Premises • Section 5.3 - Ongoing Assessment RE: processes and responsibilities • Section 5.3.1 - Continuous Monitoring RE: processes and responsibilities

Revision Date	Change Type	Description of Change
		• Section 5.3.2 - Change Control RE Coordination w/ FedRAMP processes; related Control; major significant change; FedRAMP and DISA assessment; Change approval flow in the figure • Section 5.3.2.2 - DoD Assessed CSOs RE: Change approval flow in the figure • Section 5.4.1.1 - Mission Owner Credentials RE explanation of the columns in the table • Section 5.4.1.2 CSP Privileged User Credentials RE: the credential types expected for use at L2/4 and L5 • Section 5.5.1 - SRG/STIG Compliance RE: applicability to CSP infrastructure; related controls • Section 5.6.2 - CSP Personnel Requirements RE: explanation personnel access to information Section 5.6.2.2 - CSP Personnel Requirements – PS-3: Background Investigations RE: CSP demonstrating investigation equivalency by using a GSA listed investigation contractor • Section 5.7 - Data Spill RE: data spill remediation methods. Section 5.10.1 - Cloud Access Point RE: definition, use, and applicability • Section 5.10.3 - CSP Service Architecture RE: Alternate approached to CND • Management Plane Connectivity RE: CSP management plane; protection of management interfaces • Section 5.10.3.1 - CSP Service Architecture - SaaS RE: STIGs; Data-at-rest and data in transit encryption; hardening/patching; user communities without CAC/PKI • Section 5.10.4 - Internet Protocol (IP) Addressing and Domain Name Services (DNS) RE:Non-.mil domain addressing; Impact Level 4/5 NIPRNet IP addresses; Impact Level 6 SIPRNet addresses; IP address assignment/management; updated to and coordinated with DoDI 8410.01 • Section 5.10.6 - Mission Owner System/Application Requirements using IaaS/PaaS • RE: Registration with the SNAP database at Level 2 in support of CND • RE: Internet Facing applications • Section 6.1 - Overview of Cyber Defense Tiers RE: explanation of tiers; adjusted for the standup of JFHQ-DoDIN • Section 6.3 - Cyber Defense Roles and Responsibilities RE: Minor clarifications of roles and responsibilities • Section 6.4 - Cyber Incident Reporting and Response

Revision Date	Change Type	Description of Change
		RE: the definitions of Cyber Incident • Section 6.4.3 - Incident Reporting Mechanism RE: DFARS reference; reporting tool modification; Level 6 commercial CSPs • Section 6.6 - Continuous Monitoring / Plans of Action and Milestones (POA&Ms) RE: Timeline for high/moderate findings • Section 6.9 - Vulnerability and Threat Information Sharing RE: DIB Collaboration • Appendix A - References RE: Additional references • Appendix C - Roles and Responsibilities RE: Cloud SCA; FedRAMP JAB; 3PAO • Appendix D- CSP Assessment Parameter Values for PA RE: explanation of the table and its use; cleanup of the table entries to reflect one set of values for CSP assessment, and adjusted/added some parameter values: ▪ Removed "Not appropriate to define" notations in the table in favor of the explanation in the appendix front matter ▪ Identified applicability to levels as appropriate for differences between FedRAMP PA for L2 and DoD PA for L4 and up. ▪ Merged FedRAMP and DoD parameters due to lack of overlap: AC-11, AT-2, AT-3, AU-2(3), PE-3, PS-6, RA-5, SA-9, SI-2 ▪ AC-2 (9) - Added a value IAW DoD best practice. ▪ AT-3 (2) - Added a value for the first parameter for clarity regarding which personnel need training on physical security controls. ▪ AU-5 - revised FedRAMP value to be applicable to all levels. ▪ CA-2 - Combined FedRAMP and DoD RMF TAG values to be applicable to all levels. ▪ IA-3 (1) - Added a value for the selection and provided supplemental guidance. ▪ IA-5(1) - Changed password minimum character change requirement due to lack of support in most commercial products. It now matches FedRAMP requirement of 1 character instead of half the minimum length. ▪ IR-4 (8) - Added "the Mission Owner's MCND, and Law Enforcement" to the first parameter value and added a value for the second parameter. ▪ IR-6 - Added "the Mission Owner's MCND, and Law Enforcement" to the second parameter value (b.). ▪ IR-6 (2) - added a value. ▪ SI-2(2) - HBSS changed to "host-based monitoring software", as HBSS is not available to commercial CSPs and DoD should not be requiring a specific software vendor (McAfee) to commercial CSPs just because DoD standardized on it. Also deleted 30-day requirement since it refers to scans in addition to HBSS - replaced with a generic "continuously" monitored requirement.

Revision Date	Change Type	Description of Change
		▪ SC-7(12) - Changed to generic HIPS requirement. DoD should not be requiring a specific software vendor (McAfee) to commercial CSPs just because DoD standardized on it. ▪ SI-4 - Added values for the first value and selection parameters in g. ▪ SI-4 (22) - Added "Alerts" and "and the Mission Owner's MCND" to the RMF TAG value for the selection parameter and its value. ▪ SI-4(23) - HBSS changed to "host-based monitoring software", as HBSS is not available to commercial CSPs and DoD should not be requiring a specific software vendor (McAfee) to commercial CSPs just because DoD standardized on it. ▪ Added Table 9 - Parameter Values for SLA controls/Enhancements Listed in Table 3 ▪ SC-18 (3) – Added a value RE: Mobile code download and execution ▪ SC-18 (3) - Added a value and corrected the existing value RE: automatic execution of mobile code
	Added Information or Expanded Guidance / Requirements	• Section 4.3.1 - Cloud Computing, Authorization Boundaries RE: Where A&A boundaries are drawn for IaaS/PaaS/SaaS; Control of hardware/software • Section 4.4.1 - CSP Transition from CC SRG Version/Release to Updated CC SRG Version/Release RE: the timeline for CSP compliance with changes in CSP requirements in CC SRG updates • Section 4.5 - DoD PA in Relation to RFP Response and Contract Award RE: Go live only after DoD PA granted • Section 5.1.4 - National Security Systems (NSS) RE: levels that can accommodate NSS • Section 5.1.4.1 - NSS Level 6 Classified Overlay Applicability RE: Requirements for additional controls on classified systems • Section 5.1.5 - CNSSI 1253 Privacy Overlay RE: Requirements for additional controls on systems with privacy data • Section 5.1.5.1 - PII/PHI at Level 2 RE: Business rolodex exemption for CUI applicability at Level 2 • Section 5.1.5.2 - Effects of the Privacy Overlay on CSPs and Mission Owners Section 5.1.5.3 - CSO Assessment of Privacy Overlay Control/Control Enhancements RE: Privacy overlay C/CE assessment for PA privacy rider • Section 5.1.5.4 - Mission System / Application Assessment of Privacy Overlay Control/Control Enhancements RE: Privacy overlay C/CE assessment for Mission Owner's ATO • Section 5.2.3 - DoD Data Ownership and CSP Use of DoD Data RE: Restrictions of CSP use of DoD data • Section 5.6.2.4 - Training Requirements RE: Applicability of DoD 8570.01-M • Section 5.7 - Data Spill

Revision Date	Change Type	Description of Change
		RE: Cryptographic erase • Section 5.8 - Data Retrieval and Destruction for Off-boarding from a CSO RE: Off-boarding; Cryptographic erase; Mission owner recovery capability • Section 5.10.1 - Cloud Access Point RE: ICAP vs. BCAP • Section 5.10.1.1 - Mission Partner Environments or Communities of Interest Network Cloud Access Points RE: CAPs for networks other than NIPRNet/SIPRNet • Section 5.10.3.3 - CSP Disaster Recovery (DR) - Continuity of Operations (COOP) RE: Mitigation of physical risk through use of multiple facilities in different locations • Section 5.10.7 - Active Directory Integration for Cloud RE: Integration of cloud-based AD with DoD infrastructure • Section 5.10.7.1 - Active Directory Federation Services (ADFS) RE: Use of ADFS to meet AD trust requirements • Section 5.10.7.2 - Active Directory DirSync (Directory Synchronization) RE: Use of AD DirSync to meet AD cloud requirements • Section 5.11 - Encryption of Data-at-Rest in Commercial Cloud Storage RE: Use of encryption at rest with DoD-controlled encryption keys • Section 5.11.1 - Cryptographic Erase RE: Use of NIST 800-88 defined CE function to sanitize data • Section 5.12 - Backup RE: Mitigation of risk through use of multiple storage services • Section 5.13 - DoD Contractor / DoD Component Mission Partner Use of CSOs RE: How DoD contractors outside the DoDIN can utilize CSOs • Section 5.14 - Mission Owner DoD Test and Development in the Cloud RE: How T&D environments can be implemented in CSOs • Section 5.15 - Ports, Protocols, Services, Management and Cloud Based Systems/Applications RE: PPSM registration and boundaries • Section 5.16 - Mobile Code RE: CSP and DoD mobile code policy • Section 5.17 - Registration and Connection Approval for Cloud Based Systems/Applications RE: Registration in DISA SNAP, DMZ Whitelist, and DoD CIO SNaP-IT • Section 6.4.4 - Digital Forensics in the Cloud RE: Challenges of and support for digital forensics in cloud environments Includes the following subsections: ▪ 6.4.4.1 - Malicious Software ▪ 6.4.4.2 - Incident Information Collection, Preservation, and Protection ▪ 6.4.4.3 - Forensics/Incident Information Chain-of-Custody

Revision Date	Change Type	Description of Change
		▪ 6.4.4.4 - Digital Forensics Support by CSP toward PA Award • Appendix E - Privacy Overlay Comparative C/CE Tables and Value Tables RE: added/modified C/CE
12 Jan. 2015	Version 1 Release 1	Initial publication