DOD CLOUD COMPUTING SRG
REVISION HISTORY

Version 1, Release 4

14 January 2022

Developed by DISA for the DoD

Version/ Release	Description of Change	Revision Date
FINAL Ver 1, Rel 4	• Addressed general readability issues during final editing that required clarification. • Made edits for grammar, style, and punctuation.	14 January 2022
DRAFT Ver 1, Rel 4	• Released for public comment. • Addressed major policy, process, cloud adoption model changes, corrections, and clarifications as follows: o Provided guidance WRT reciprocity for CSPs having a FedRAMP High PA for achieving a DoD L4/5 PA. o Updated CND/CD guidance IAW new Cyber Defense policy DoDI 8530.01 and the decision to eliminate the CD CONOPS. Additional updates will be coordinated with the DoDI 8530.01 Manual when published. o Clarified guidance and definitions for CAP, BCAP, and ICAP and expand the focus beyond NIPRNet. o Clarified guidance and definitions for On-Premises and Off-Premises, while addressing/introducing the concept of Virtually Off-Premises in a Cloud Computing construct. o Added requirements for situations where a P/SaaS CSP cannot advertise NIPR	26 February 2021
	Administrative Changes • Administrative corrections and changes throughout	
	Clarifications/Explanations/Added Information **Expanded Guidance/Requirements** ***Section 1:*** • Created Section … • Added Section … ***Section 2:*** • In section … ***Section 3:*** • Section 3.1 Security Objectives (Confidentiality, Integrity, and Availability): Removed first paragraph referencing the next section. • Section 3.2 Information Impact Levels: Clarified that ILs are associated with the DoD and not FedRAMP or the rest of the Federal Government.	

Version/ Release	Description of Change	Revision Date
	• Section 3.2.4: Added clarifying language to IL6 definition. ***Section 4:*** • Section 4.3.3 Mission Risk: Added a sentence to further explain when the ATO requirement would still apply to DoD CSP SaaS CSOs with only a PA. ***Section 5:*** • Section 5.1.1: Emphasized "full reciprocity" for Impact Level 2 with FedRAMP. • Section 5.1.5: Reorganized entire PII section for better clarity. • Section 5.1.5.1 PII/PHI at Level 2: Inserted five requirements needed for low impact/sensitivity PII to be published or collected in CSOs having a Level 2 PA. • Section 5.1.6: Highlighted this section is Optional for additional Mission Owner controls where required. Added SLA clarification to paragraph. • Section 5.2.1 Jurisdiction/Location Requirements: Added requirement for Mission Owner and/or contracting officer to review CSP Terms and Conditions. • Added Section 5.2.2.3.1 Impact Level 5 Separation in an Impact Level 4 CSO: Added eight requirements for Level 5 systems and data that are based on a subset of services offered by or in addition to a Level 4 CSO. • Section 5.2.2.3.2: Added requirements Key Management Services to protect IL5 information in and IL4 cloud as requested by the NSA. • Created Section 5.3.3 Support for Financial Audits – SOC 1 Type II Reports: Discusses the System and Organization Control (SOC 1) Type II reporting requirements for service organizations. • In Section 5.4.1.1 Mission Owner Credentials for CSP and Mission System Interfaces: Added detail explaining how Mission Owners can seek AO approval to use a DoD-compliant assertion service when necessary. • In Section 5.10.1: Updated notional	

Version/ Release	Description of Change	Revision Date
	connection drawings. • In Section 5.10.1.1.1 NIPRNet BCAP: Added the purpose of the NIPRNet BCAP. Added a note explaining how Mission Owners might seek DoD CIO approval to host applications that do not support NIPRNet based users. • In Section 5.10.1.1: Updated to reflect BCAP is applicable to level 4/5 and DMZ protections must be considered. • In Section 5.10.1.1.2 NIPRNet BCAP Meet-Me Points: Added requirements and CCIs associated with a NIPRNet BCAP Meet-Me Point / DISN PoP located in a commercial facility. • In Section 5.10.1.4 SIPRNet BCAP/ICAP: Clarified that BCAPS and ICAPS are required as they are for NIPRNet connections to CSOs. Added three key takeaways to Figure 15. • In Section 5.10.3.1: Removed reference to DMZ STIG. Added language pertaining to public internet facing and private NIPRNET facing web applications. Updated Data at Rest to allow FIPS 140-2 or 140-3. • In Section 5.10.4.1: Revised language to include public internet facing and private NIPRNET facing scenarios for routing purposes. Updated DoD NIC references. • In section 5.10.6 Mission Owner System/Application Requirements using IaaS/PaaS: Added a sentence discussing CSO API calls in relation to the configuration of virtual networks. • Created section 5.10.8 Hybrid Cloud – Interconnections between CSOs to address some of the security and architectural constraints surrounding interconnections of IL4/5 or IL6 CSOs. Added subsections as follows: ▪ 5.10.8.1 Mission Owners Applications: states auditing of traffic will be performed by the interconnected CSOs. ▪ 5.10.8.2 On/Off-premises Scenarios: states that the interconnection of IL4/5 or IL6 CSOs that are	

Version/ Release	Description of Change	Revision Date
	both on-premises and off-premises will be via the BCAP. ▪ 5.10.8.3 SaaS CSOs using "External Services": included guidelines for CSPs leveraging one or more third party "external services". • Section 5.11: Added approved KMS by the NSA as an option. • Section 5.17.2: Revised language to include public internet facing and private NIPRNET facing scenarios for DMZ Whitelist purposes. ***Section 6:*** • Replaced entire section with rewrite from CSSP working group. ***Appendices:*** • Appendix A References: … • Appendix B Glossary: … • Appendix C Table 7 Roles and Responsibilities: … • Appendix D: Updated Table 8 to reduce differences between DoD and FedRAMP level 4/5. Incorporated some high baseline values for the DoD at the moderate level.	
FINAL Ver 1, Rel 3	Released final signed document	06 March 2017
	Administrative Changes • Corrected the updated CND/CD lexicon to that defined in new Cyber Defense policy DoDI 8530.01 and JP 3-12 (R) throughout (except in the revision history). This primarily relates to the use of the terms Cybersecurity and CSSP.	
	Clarifications/Explanations/Added Information/Expanded Guidance/Requirements • Section 1: Created Section 1.1 Key Terminology to house a discussion and listing of the key terminology used in the document. Moved the definitions of the terminology to Appendix B Glossary. • Added Section 1.4.1 Applicability of CC SRG vs DoDI 8550.01 to answer questions about the permitted use of "Internet Based Capabilities" as defined in DoDI 8550.01 and whether they are subject to CC SRG requirements. • Section 2.6 DoD Provisional Authorization: Clarified that a DoD PA is a "pre-acquisition determination of risk" rather than an "acceptance of risk". Acceptance of risk is the responsibility of the	

Version/ Release	Description of Change	Revision Date
	Mission Owner's AO when awarding their ATO. • Section 3.2 Information Impact Levels: Minor revisions to Para 3 and 4 for clarity. • Section 3.2.2 Level 2: Non-Controlled Unclassified Information: Minor revisions for clarity. Added a statement regarding the CSO's customer base and connectivity for clarity. • Section 3.2.4 Level 4: Controlled Unclassified Information: Minor revisions for clarity RE mission critical data and added a note RE ITAR data and non-US-Persons. Added statements regarding the CSO's supported community, customer base, and connectivity for clarity. • Section 3.2.5 Level 5: Controlled Unclassified Information: Clarified constraints RE: determining what CUI needs the added security afforded at L5. Added statements regarding the CSO's supported community, customer base, and connectivity for clarity. • Section 3.2.6 Level 6: Classified Information up to SECRET: Added statements regarding the CSO's supported community, customer base, and connectivity for clarity. • Section 4.1 Assessment of Commercial/Non-DoD Cloud Services: Minor revisions RE: incorporating the FedRAMP High Baseline as a basis for L4/5 PAs.	