

UNCLASSIFIED



DEPARTMENT OF DEFENSE CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE

Version 1, Release 4

14 January 2022

Developed by DISA for the DoD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Department of Defense, Defense Information Systems Agency, the DISA Risk Management Executive (RME), or DISA RME Cybersecurity Standards Branch of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Purpose and Audience.....	1
1.2 Authority	2
1.3 Scope and Applicability	2
1.4 SRGs/STIGs.....	5
1.5 SRG and STIG Distribution	6
1.6 Document Revisions and Update Cycle.....	6
1.6.1 Comments, Proposed Revisions, and Questions.....	6
1.7 Document Organization	6
2. BACKGROUND	8
2.1 Key Terminology	8
2.2 Cloud Computing, Cloud Service, and Cloud Deployment Models.....	8
2.3 Cloud Service Provider (CSP) and Cloud Service Offering (CSO).....	10
2.4 DoD Risk Management Framework (DoD RMF)	10
2.5 Federal Risk and Authorization Management Program (FedRAMP).....	11
2.6 FedRAMP Plus (FedRAMP+)	11
2.7 DoD Provisional Authorization.....	11
3. INFORMATION SECURITY OBJECTIVES/IMPACT LEVELS.....	14
3.1 Information Impact Levels.....	15
3.1.1 Impact Level 2: Non-Controlled Unclassified Information.....	17
3.1.2 Impact Level 4: Controlled Unclassified Information	18
3.1.3 Impact Level 5: Controlled Unclassified Information and Unclassified National Security Information (U-NSI).....	19
3.1.4 Impact Level 6: Classified Information Up to SECRET	20
4. RISK ASSESSMENT/AUTHORIZATION OF CLOUD SERVICE OFFERINGS	22
4.1 Assessment of Commercial and Non-DoD Cloud Services for Enterprise Use	23
4.1.1 Assessment of On-Premises Commercially Owned and Operated Cloud Services	28
4.1.2 DoD Component Sponsorship of a CSO for a FedRAMP Agency ATO	28
4.2 Assessment of DoD O&O Cloud Services and Enterprise Services Applications	28
4.3 Cloud Service Offering and Mission Owner Risk Management	29
4.3.1 Cloud Computing, Authorization Boundaries	29
4.3.2 Cloud Service Offering (CSO) Risk	30
4.3.3 Mission Risk	30
4.4 CSP Transition from CC SRG Version/Release to Updated CC SRG Version/Release .	32
4.5 DoD PA in Relation to RFP Response and Contract Award; DFARS Interpretation.....	33
4.6 Cloud Service vs. a Managed IT Service	34
5. SECURITY REQUIREMENTS	36

5.1	DoD Policy Regarding Security Controls	36
5.1.1	DoD Use of FedRAMP Security Controls.....	37
5.1.2	DoD FedRAMP+ Security Controls/Enhancements.....	38
5.1.3	Parameter Values for Security Controls and Enhancements	41
5.1.4	National Security Systems (NSS)	41
5.1.5	Personally Identifiable Information (PII)/Protected Health Information (PHI) in the Cloud.....	41
5.1.6	Security Controls/Enhancements To Be Optionally Addressed in the Contract/SLA	44
5.1.7	Additional Considerations and/or Requirements for L4/5 DoD PA Award	45
5.2	Legal Considerations.....	47
5.2.1	Jurisdiction/Location Requirements	47
5.2.2	Cloud Deployment Model Considerations/Separation Requirements	50
5.2.3	DoD Data Ownership and CSP Use of DoD Data.....	56
5.3	Ongoing Assessment.....	57
5.3.1	Continuous Monitoring.....	58
5.3.2	Change Control	62
5.3.3	Support for Financial Audits – SOC 1 Type II Reports.....	66
5.4	CSP Use of DoD Public Key Infrastructure (PKI).....	68
5.4.1	Identification, Authentication, and Access Control Credentials.....	70
5.4.2	Public Key (PK) Enabling	73
5.5	Policy, Guidance, Operational Constraints	74
5.5.1	SRG/STIG Compliance	74
5.6	Physical Facilities and Personnel Requirements.....	75
5.6.1	Facilities Requirements.....	75
5.6.2	CSP Personnel Requirements	75
5.7	Data Spill.....	80
5.8	Data Retrieval and Destruction for Off-Boarding from a CSO	82
5.9	Reuse and Disposal of Storage Media and Hardware.....	83
5.10	Architecture.....	83
5.10.1	Cloud Access Point (CAP).....	84
5.10.2	Network Planes	101
5.10.3	CSP Service Architecture	106
5.10.4	Internet Protocol (IP) Addressing and Domain Name Services (DNS).....	110
5.10.5	Mission Owner Requirements Using SaaS and Some PaaS (All Levels).....	115
5.10.6	Mission Owner System/Application Requirements Using IaaS/PaaS	116
5.10.7	Hybrid Cloud-Interconnections Between CSOs	121
5.11	Encryption of Data-at-Rest in Commercial Cloud Storage.....	122
5.11.1	Cryptographic Erase.....	124
5.12	Backup.....	124
5.13	DoD Contractor/DoD Component Mission Partner Use of CSOs	125
5.13.1	DoD Component Mission Partners	125
5.13.2	Non-CSP DoD Contractors and DIB Partners Use of CSOs for the Protection of Sensitive DoD Information	126
5.13.3	Non-CSP DoD Contractors Use of CSOs as a Portion of a Non-CSO Product or Service.....	127
5.14	DoD Mission Owner Test and Development in the Cloud	127

5.14.1 Workstation Connectivity to Cloud Based T&D Zones	130
5.15 Ports, Protocols, Services, Management and Cloud Based Systems/Applications	131
5.16 Mobile Code	132
5.17 Registration and Connection Approval for Cloud Based Systems/Applications	134
5.17.1 DISA Systems/Network Approval Process (SNAP)	134
5.17.2 DoD DMZ Whitelist	134
5.17.3 Select and Native Programming Data Input System- Information Technology (SNaP-IT)	135
5.18 Supply Chain Risk Management Assessment	135
5.19 Electronic Mail Protections	136
5.19.1 Electronic Mail Protections IAW TASKORD 12-0920	136
6. CYBERSPACE DEFENSE AND INCIDENT RESPONSE	138
6.1 Overview of Cyberspace Defense	138
6.2 Concept Changes for Information Impact Levels for Cloud Computing	138
6.2.1 Boundary Cyberspace Defense Actions	139
6.2.2 Mission Cyberspace Defense Actions	139
6.3 Cyberspace Defense Actions	140
6.4 Cyberspace Defense Roles and Responsibilities	141
6.5 Cyber Incident Reporting and Response	142
6.5.1 Incident Response Plans and Addendums	143
6.5.2 Information Requirements, Categories, Timelines, and Formats	144
6.5.3 Incident Reporting Mechanism	145
6.5.4 Digital Forensics in the Cloud and Support for Law Enforcement/Criminal Investigation	146
6.6 Warning, Tactical Directives, and Orders	149
6.7 Continuous Monitoring/Plans of Action and Milestones (POA&Ms)	149
6.8 Notice of Scheduled Outages	150
6.9 PKI for Cyberspace Defense Purposes	150
6.10 Vulnerability and Threat Information Sharing	150
Appendix A. References	152
Appendix B. Glossary	157
Appendix C. Roles and Responsibilities	161
Appendix D. CSP Assessment Parameter Values for PA	164
Appendix E. Privacy Overlay Comparative C/CE Tables and Value Tables	173