DEPARTMENT OF DEFENSE (DoD)
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE (SRG)

Version 1, Release 1

12 January 2015

Developed by the
Defense Information Systems Agency (DISA)
for the
Department of Defense (DoD)

3 INFORMATION SECURITY OBJECTIVES / IMPACT LEVELS

Cloud security information impact levels are defined by the combination of: 1) the level of information to be stored and processed in the CSP environment; and 2) the potential impact of an event that results in the loss of confidentiality, integrity or availability of DoD data, systems or networks. DoD Mission Owners categorize mission information systems in accordance with DoDI 8510.01 and CNSSI 1253 to select the impact level that most closely aligns with defined baselines.

3.1 Security Objectives (Confidentiality, Integrity, Availability)

Information Impact Levels consider the potential impact should the confidentiality or the integrity of the information be compromised.

According to Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, confidentiality is "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]. A loss of confidentiality is the unauthorized disclosure of information.

FIPS Publication 199 defines integrity as "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]. A loss of integrity is the unauthorized modification or destruction of information. It is important to note that the unauthorized destruction of information will result in the loss of availability of that information.

FIPS-199 defined three levels to designate the impact of a loss of confidentiality or a loss of integrity (refer to Table 1). The security control baseline for all Impact Levels is based on moderate confidentiality and moderate integrity. If a Mission Owner has high potential impacts, specific requirements must be included in the contract/SLA to address/mitigate this risk or deploy to DoD facilities assessed using CNSSI 1253 high baselines through the DoD RMF. In the future DISA will consider incorporating a FedRAMP High Baseline into this SRG after one becomes available.

Table 1 - Potential Impact Definitions for Security Objectives

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information	The unauthorized modification or destruction of information	The unauthorized modification or destruction of information

	could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The baseline objectives do not address the impact of availability; it is expected that the Mission Owner will assess the CSP's stated availability rating(s) during CSP selection. Any specific or additional availability requirements must be included in the contract or a service level agreement with the CSP. Mission Owners must ensure the language is specific and inclusive for their required availability. For example, if the requirement is "CSP maintenance affecting system availability must be coordinated 4 weeks in advance and only conducted between 02:00 and 04:00 EST on Sunday morning," then the contract / SLA should detail the requirement. Recommended contract / SLA availability controls are provided under the FedRAMP+ Controls/Enhancements in Section 5.1.5, *Controls/Enhancements to be Addressed in the Contract/SLA*.

CSPs will be evaluated or queried as part of the assessment process to determine the level of availability they offer to be listed in the DoD Cloud Service Catalog. This evaluation does not prevent a CSP from receiving a PA or being included in the DoD Cloud Service Catalog; it is only used to facilitate the matching of a DoD Mission Owner to one or more appropriate cloud services meeting their needs.

3.2 Information Impact Levels

The previously published Cloud Security Model defined 6 information Impact Levels. In order to simplify the selection process, the number of levels was reduced from 6 to 4. This was accomplished by integrating levels 1 (public information) and 3 (low impact Controlled Unclassified Information (CUI)) into levels 2 and 4, respectively. The numeric designators for the Impact Levels have not changed to remain consistent with previous versions of the Cloud Security Model, leaving Impact Levels 2, 4, 5, and 6. Note that a higher level can process data from a lower level.

Additionally, the security control baseline for all levels has been changed to moderate confidentiality and moderate integrity as defined by CNSSI 1253 and the FedRAMP Moderate Baseline. This modification from high confidentiality and high integrity is intended to better align with the categorization of most DoD customer systems that will be deployed to commercial CSP facilities. Mission owners with systems categorized at high confidentiality or integrity impact levels must deploy to DoD facilities assessed using CNSSI 1253 high baselines through the DoD RMF or contract for the added security. DISA will consider incorporating a FedRAMP High Baseline into this SRG after one becomes available.

The following subsections describe the impact levels, to include those used previously, and the type of information to be stored or hosted in CSOs.

3.2.1 Level 1: Unclassified Information approved for Public release

Level 1 is no longer used and has been merged with Level 2.

3.2.2 Level 2: Non-Controlled Unclassified Information

Level 2 includes all data cleared for public release, as well as some DoD private unclassified information not designated as CUI or critical mission data, but the information requires some minimal level of access control.

3.2.3 Level 3: Controlled Unclassified Information

Level 3 is no longer used and has been merged with Level 4.

3.2.4 Level 4: Controlled Unclassified Information

Level 4 accommodates CUI which is the categorical designation that refers to unclassified information that under law or policy requires protection from unauthorized disclosure as established by Executive Order 13556 (November 2010) or other mission critical data. Designating information as CUI or critical mission data to be protected at Level 4 is the responsibility of the owning organization. Determination of the appropriate impact level for a specific mission with CUI and mission data will be the responsibility of the mission AO.

CUI contains a number of categories[3], including, but not limited to the following:

- Export Control--Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. This includes dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
- Privacy Information--Refers to personal information or, in some cases, *personally identifiable information* (PII)[4] as defined in Office of Management and Budget (OMB) M-07-16[5] or *means of identification* as defined in 18 USC 1028(d)(7).
- Protected Health Information (PHI)[6] as defined in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).
- Other information requiring explicit CUI designation (i.e., For Official Use Only, Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information).

3.2.5 Level 5: Controlled Unclassified Information

Level 5 accommodates CUI that requires a higher level of protection as deemed necessary by the information owner, public law, or other government regulations. Level 5 also supports unclassified National Security Systems (NSSs) due to the inclusion of NSS specific requirements in the FedRAMP+ controls/control enhancements (C/CEs). As such, NSS must be implemented at Level 5.

[3] CUI Categories: http://www.archives.gov/cui/registry/category-list.html
[4] NIST SP800-22, Protecting PII: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
[5] OMB M-07-16: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
[6] PHI: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

3.2.6 Level 6: Classified Information up to SECRET

Level 6 accommodates information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD). At this time, only information classified as SECRET, in accordance with the applicable executive orders, is applicable to this level. Services running at higher classification levels, to include compartmented information, are governed by other policies and are beyond the scope of this document. Impact Level 6 requires a similar set of tailored controls as Level 5 and includes the CNSSI 1253 Appendix F, Attachment 5 Classified Information Overlay C/CEs.

4 RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS

The shift to cloud computing necessitates changes in the Risk Management processes. The goal is to address the security requirements and controls, relative to the criticality of DoD information in the external cloud, in a cost effective and efficient manner, while still assuring the security of DoD's core missions and networks in accordance with the DoD RMF. To support the relationship of missions to cloud capabilities, DoD has defined information Impact Levels (discussed in Section 3) that broadly align to the criticality, sensitivity of data, and missions that would operate in a cloud environment. The DoD provisional authorization (PA) risk assessment process is focused on evaluating the requirements for the impact level(s) at which a CSP's Cloud Service Offering (CSO) is capable of supporting. The resulting PA would then be leveraged by the Mission Owner's Authorization Official in granting an authorization to operate (ATO) for the mission system operating within the cloud.

4.1 Assessment of Commercial/Non-DoD Cloud Services

The 15 December 2014 DoD CIO memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services,* states "components may host Unclassified DoD information that **has been publicly released** on FedRAMP approved cloud services." The memo also states "FedRAMP will serve as the minimum security baseline for all DoD cloud services."

***Impact Level 2*:** Using the definitions outlined in section 3, Impact Level 2 information may be hosted in a CSP that is government assessed as FedRAMP compliant at the moderate level. The two acceptable government assessments include:

- JAB Provisional Authorizations – Based on a determination by the JAB that an acceptable level of risk exists for leveraging across the Federal Government. DoD is an active participant in the technical reviews of the JAB PA security assessment artifacts.
- Agency ATOs – Based on an assessment and ATO issued by a specific agency. These are assessed and authorized by a DoD agency, with the artifacts made available for leveraging by others across the Federal Government.

The decision to leverage such authorizations is subject to acceptance by the Mission Owner and the responsible Authorizing Official (AO).

Impact Level 4/5/6: Assessments for Impact Levels 4 and above is based on a combination of the security controls in the FedRAMP Moderate baseline and the DoD specific controls/requirements outlined in section 5.1.2 DoD FedRAMP+ Controls/Enhancements. Where possible, DoD leverages documentation and artifacts in the FedRAMP Secure Repository and additional CSP proprietary artifacts. FedRAMP+ requirements will be assessed by a FedRAMP certified Third Party Assessment Organization (3PAO) or an approved DoD assessor. An overall determination of risk is prepared by the DISA Cloud Security Control Assessors to support a DoD PA decision and listing in the DoD Cloud Service Catalog[7], available to DoD personnel. The DISA Authorizing Official (AO) (formerly the DISA DAA) approves DoD PAs.

There are three paths that can be followed in assessing a CSP for a DoD PA. These are:

[7] DoD Cloud Service Catalog:
https://disa.deps.mil/disa/org/atb/Cloud%20Broker/Lists/Catalog/CatalogPageView.aspx (DoD PKI required)

- **CSPs with a FedRAMP JAB PA or in the process of obtaining a JAB PA:** DoD leverages the documentation and artifacts produced as part of the FedRAMP process, supplemented with an assessment of the DoD-specific security controls and requirements not addressed by FedRAMP for Impact Levels 4 and above. CSPs having a FedRAMP JAB PA have been assessed by a certified 3PAO against the FedRAMP Moderate Baseline. For those in the process of obtaining a JAB PA, DoD promotes the use of parallel activities (FedRAMP and FedRAMP+) to minimize cost and create efficiencies in the assessment process.

- **FedRAMP Agency ATO:** CSPs having a Federal agency authorization based upon security controls assessed by a certified 3PAO can be assessed for a DoD PA provided that the authorization is accepted and listed in the FedRAMP agency authorizations. The information from the agency ATO will be supplemented with an assessment of the DoD-specific controls and requirements.

- **DoD Self-Assessed PA:** CSP is assessed by the DISA cloud assessment team, independent of FedRAMP. The CSP is minimally assessed against the FedRAMP Moderate Baseline and FedRAMP+ requirements. A DoD self-assessment is typically used for dedicated cloud service offerings supporting the DoD or a private cloud service offering by a DoD or commercial CSP. In this scenario, the CSP's assessment package will not be in the FedRAMP secure repository, since private clouds are ineligible for inclusion in the FedRAMP catalog. When a FedRAMP authorization does not exist for a commercial CSP, the DoD organization with a need for the authorization will be required to support resourcing for the full assessment, in coordination with the DISA cloud security assessment team. This assessment of both the FedRAMP, FedRAMP+ security controls, and other SRG requirements determines whether to grant a DoD PA and the appropriate impact levels.

NOTE: Any change of ownership involving a CSP, whether the primary CSP or an underlying CSP on which a CSO was built, will be reviewed by the DISA AO to assess the impacts and risks associated with the continuation of the DoD PA.

4.2 Assessment of DoD Provided Cloud Services

DoD operated CSOs (e.g., milCloud) are subject to the same requirements found in this SRG and the same security controls as commercial CSPs. However, DoD CSP programs and services must follow DoD Risk Management procedures in accordance with DoDI 8510.01. DoD enterprise service programs considered as cloud services under the SaaS model (e.g., Defense Enterprise Email (DEE), Defense Connect Online (DCO), DoD Enterprise Portal Service (DEPS)), are also subject to the DoDI 8510.01 requirements. Such programs are not subject to being assessed through the FedRAMP program and do not share DoD ATOs with the FedRAMP secure repository.

DoD is transitioning to the DoD RMF from the DoD Information Assurance Certification and Accreditation Process (DIACAP). DIACAP is based on a set of DoD specific security controls, not the NIST 800-53 security control catalog. Cloud services initiated and authorized under the

DIACAP will be assessed and authorized using the RMF in accordance with DoD transition guidance as defined in DODI 8510.01 or supplemental DoD guidance.

4.3 Cloud Service Offering and Mission Owner Risk Management

Risk management must consider both the CSO and the supported mission (i.e., the Mission Owner's system or application). Each CSO must be granted a DoD PA in order to host DoD mission systems. The PA can then be used by the Mission Owner's risk management officials as a basis of reciprocity for the controls provided by the CSP, recognizing the controls will vary based on the service model (IaaS, PaaS, SaaS) and could also vary based on requirements such as privacy or classification controls. Additionally, there are controls that are "shared controls" where both the CSO and the Mission Owner need to address a requirement. The responsible AO leverages the PA information, supplemented with an assessment of the risks within the Mission Owner's responsibility, in granting an authorization to operate.

Understanding the distinction between what's provided and addressed with the CSO versus what's addressed by the Mission Owner is critical to implementing the DoD cloud security requirements as defined in this SRG.

4.3.1 Cloud Service Offering (CSO) Risk

The DoD PA provides a risk acceptance determination for the CSO against the appropriate DoD security requirements. The DoD PA assessment process assesses CSO risk based on its supported impact level. At a level 4 and above, it's important to recognize that the DoD PA evaluation process also assesses the risk to DoD of permitting CSPs to interconnect with DoD networks.

4.3.2 Mission Risk

Overall mission risk will continue to be assessed and authorized by the Mission Owner's AO through the issuance of an ATO. Mission refers to the information system and functions for which a DoD entity acquires or uses a CSO. This may be the direct use of a SaaS CSO in performing an IT-enabled mission, or the instantiation of an IT system or application on an IaaS/PaaS CSO.

Mission Owners categorize mission systems and/or applications in accordance with (IAW) DoDI 8510.01 defined processes. Mission owners then select CSOs from the DoD Cloud Service Catalog based on their security posture and the risk tolerance of the Mission Owner. While CSOs will have been assessed and provisionally authorized for use, the Mission Owner must proceed IAW the RMF to obtain an Authority To Operate (ATO) from their assigned AO.

The Mission Owner inherits compliance from the CSO for the security controls (or portions thereof) that the CSP meets and maintains. A Mission Owner's system or application built on an IaaS or PaaS offering will be subject to meeting many of the same security controls within the system/application. Mission Owners contracting for SaaS offerings inherit the bulk of compliance with the security controls from the CSO. Inheritance will be different between CSPs operating within a service type and thus must be evaluated separately. It should also be noted that the number of controls increases with higher impact levels and additional overlay controls (e.g. privacy). Figure 1 illustrates this concept.

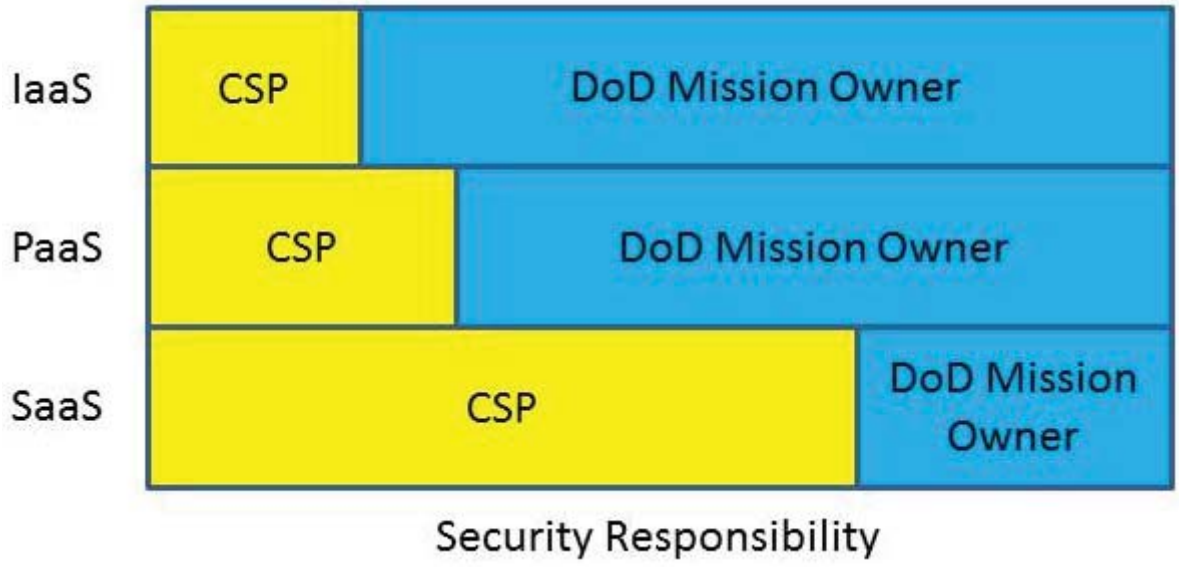

Figure 1 – Notional Division of Security Inheritance and Risk

The benefit of starting with a provisionally authorized CSO is that much of the security controls assessment work is already accomplished. Mission Owners and their AOs must still review the FedRAMP and DoD PA artifacts to understand the risks that the mission will inherit when using the selected CSO for the mission system/application. Mission owners may need to implement, or request that the CSP implement, compensating controls for any risk deemed unacceptable prior to obtaining an ATO.

4.4 CSP Transition from CSM v2.1 to SRG v1r1

FedRAMP provides a transition strategy[8] for migrating CSP assessments from the FedRAMP v1 baselines based on NIST 800-53 rev3 to the FedRAMP v2 baselines based on NIST 800-53 rev4. This strategy went into effect on June 6, 2014. The key points are as follows:

- Any new assessment starting after June 1, 2014 will immediately transition to FedRAMP v2 baselines based on NIST 800-53 rev4.
- CSPs in the process of being assessed against FedRAMP v1 baselines based on NIST 800-53 rev3 prior to June 1, 2014 will continue on this track, but must transition to the FedRAMP v2 baselines within one year of their authorization date.
- CSPs currently in continuous monitoring will have until their next annual assessment to complete the transition to FedRAMP v2 baselines.

The requirements in this SRG become effective immediately upon final publication. However, the DoD migration plan for CSP assessments will mirror the FedRAMP plan as follows:

- Any new assessment starting after the release of this Cloud Computing SRG will be assessed against these requirements.

[8] FedRAMP transition strategy: http://cloud.cio.gov/topics/fedramp-800-53-rev-4-guidance-cloud-service-providers-0

- CSPs currently in the process of being assessed against the requirements in the CSMv2.1 will continue on this track, but must transition to compliance with the Cloud Computing SRG requirements in coordination with their next FedRAMP annual assessment.
- CSPs currently in continuous monitoring under CSMv2.1 will have until their next FedRAMP annual assessment to complete the transition to compliance with the Cloud Computing SRG control requirements.

A DoD PA issued for a CSP using the CSMv2.1 and based on FedRAMP v1 remains in effect for the duration of the DoD PA, so long as compliance is achieved with the timelines described above. DoD mission systems leveraging a CSO may experience a period of time of time where risks based on FedRAMP v2 or new FedRAMP+ security controls have not yet been assessed. Mission owners and their AOs must review the controls to determine if the risk is acceptable until such time the CSP is required to comply or include the required compliance in the acquisition language.

NOTE: CSPs wishing to transition sooner than later may do so at any time.