Defense Cloud Security Guidance Aims to Empower Military Services

Posted At : January 28, 2015 9:49 AM | Posted By : Kyra Fussell

Related Categories: Department of Defense, Information Security, Cloud Computing, Cybersecurity, General Services Administration (GSA)

Mid January 2015, Defense Department's (DOD) Defense Information Services Agency (DISA) **released guidance** for use of commercial and non-DOD cloud providers within the DOD.

Since the DISA publication is a Security Requirements Guide (SRG), it offers non-product specific requirements to mitigate risks associated with commonly encountered IT system vulnerabilities. While SRGs provide high level direction, Security Technical Implementation Guides (STIGs) offer product-specific details for validating, attaining, and maintaining compliance with the SRG requirements.

The previously published Cloud Security Model outlined 6 Information Impact Levels. Although the DOD cloud computing SRG has reduced the number to 4 impact levels, the numeric designators remain consistent with the previously published model. DOD provisional risk assessments for cloud services focus on evaluating the requirements for the impact levels at which a cloud service offering is supported by a provider. Provisional authorization is then leveraged by the mission owner in granting authority to operate (ATO) for mission systems operating in the cloud.

Defense Department Information Security Objectives/ Impact Levels

Impact Level		Description	Risk Assessment
1	Unclassified Information approved for Public release	No longer in use. This has been merged with Level 2.	
2	Non-controlled Unclassified Information	Includes data cleared for public release along with some DOD private but unclassified information (requires low level of access control)	Maybe hosted by a Cloud Service Provider (CSP) that is FedRAMP compliant at the moderate level.
3	Controlled Unclassified Information	No longer in use. This has been merged with Level 4.	
4*	Controlled Unclassified Information	Mission critical data or information that requires protection from unauthorized disclosure as established by law or policy. Designating information at this level is the responsibility of the owning organization.	Level 4 and above assessments are based on a combination of security controls in the FedRAMP Moderate baseline and DOD specific controls and requirements. Where possible, DOD will leverage documentation from the FedRAMP Secure Repository and CSP proprietary artifacts.
5	Controlled Unclassified Information	CUI requiring a higher level of protection as determined by the information owner, public law, or other government regulations. This level also supports unclassified National Security Systems (NSS).	
6	Classified Information up to SECRET	Information that is determined to be classified national security information or restricted data. This level requires a set of tailored controls (similar to level 5) and includes classified information overlay controls/control enhancements.	

Source: Department of Defense, Deltek

*With regard to information designated at Level 4, Controlled Unclassified Information (CUI) covers a number of categories including export control, privacy information, and protected health information.

The security control baseline for all levels aligns with the FedRAMP moderate baseline's definition for confidentiality and integrity. This shift from high confidentiality and high integrity intends to support the categorization of customer systems targeted to be deployed to commercial CSP facilities. The 15 December 2014 CIO memo called out FedRAMP as the minimum security baseline for all DOD cloud services and advised that defense components "may host unclassified DOD information that has been publicly released on FedRAMP approved cloud services."

The DISA cloud computing SRG covers systems up to the Secret level of classification. Services running at a classification levels above secret, including compartmented information, are governed by other policies and fall outside the scope of the guidance DISA released. General Service Administration's (GSA) Federal Risk and Authorization Management Program (FedRAMP) aims to have a cloud security baseline established for FISMA high requirements within the next six months. DISA plans to consider incorporating the FedRAMP High Baseline into its guidance once it becomes available.

Ultimately, CSPs have three paths to choose from in pursuing a DOD provisional authorization. One option is to achieve a provisional authorization through FedRAMP's Joint Authorization Board (JAB). Another option is to achieve FedRAMP Agency ATO by completing the FedRAMP compliance process as well as meeting any additional security control requirements from the authorizing agency. The third option is for a system to be comply with requirements fo DOD Self-Assessed Provisional Authorization. The concept of FedRAMP Plus (FedRAMP+) applies to situations where an agency has specific security requirements beyond the FedRAMP baseline. Within the DOD SRG, these additional security controls and requirements are necessary to meet and assure DOD's mission requirements.

Like FedRAMP's intention to allow agencies to take a greater role in steering commercial cloud authorizations, DISA's guidance will empower the military services to procure their own solutions and leverage the government's work through FedRAMP. Considering the trend toward shared service adoption, after a cloud solution is adopted by one service branch, other defense components may look to

implement FedRAMP+ solutions or DISA may evaluate that solution for potential formal shared service use.

Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about ***GovWinIQ****. Follow me on twitter* ***@FIAGovWin****.*