CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NOV 0 6 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Cloud Way Forward Report Public Release

In light of current fiscal realities, the DoD CIO is examining the use of commercial cloud computing as a cost savings measure for the Department of Defense. To that end, a 45 day study was commissioned to examine the balance between risks to the Department across the wide spectrum of computing needs and the costs of traditional security measures.

The result of that study, "The DoD Cloud Way Forward," is attached for your information and use and is scheduled for public release this week. The document will be posted to the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) to share the Department's initial findings regarding the implementation and use of commercial cloud with industry.

The study introduces three new constructs to help DoD Cloud Customers identify the appropriate security for use of commercial cloud computing. A key aspect of the report is clear guidance to both Cloud Service Providers and DoD Cloud Customers describing the cradle-to-grave process they must follow in order to move DoD computing into commercial cloud infrastructure.

Finally, this study identifies key additional work items which the Department must complete to implement report recommendations and remove current barriers to the usage of commercial cloud. These items include additional technical refinement of security requirements, an update to the Department's policies that currently hinder the use of commercial cloud, and continued focus on the resolution of legal issues that constrain the use of commercial cloud. As these follow-on work items progress, the findings and conclusions will be reflected in revised policy guidance and security models for the Department.

My contact for this matter is Mr. Kevin M. Dulany, 571-372-4699, Kevin.M.Dulany.civ@mail.mil.

Terry A. Halvorsen
Acting

Attachment:
As stated

DoD Cloud Way Forward

23 July 2014
Version 1.0

Approved for Public Release

Executive Summary 3
1. Introduction 4
2. Guidance to Cloud Service Providers 6
3. Reference Architecture/Implementation 16
4. Guidance to DoD Cloud Customers 31
5. Way Ahead 41
Appendix A - Summary of Changes 44
Appendix B - References 46

Executive Summary

The Department of Defense continues to adjust its budget in response to the fiscal realities of the nation post-conflict in Iraq and Afghanistan. This report documents the results of a 45 day effort chartered by the DoD CIO to maximize the use of commercial cloud computing as a cost savings measure. Key to this effort was reexamining the balance between the risks to the Department across the wide spectrum of computing needs and the costs of our traditional security measures.

Three new constructs are introduced to help DoD Cloud Customers identify the appropriate security for the use of commercial cloud computing. First, the security levels in the Cloud Security Model have been modified to reflect the difference between National Security Systems and DoD computing systems that are not National Security Systems. Proposed changes to the Cloud Security Model reduce the number of security controls for the non-National Security Systems and change the specific categorization levels (Low, Moderate, High) for the cloud security impact levels (1-6). This lays the groundwork for collapsing the Cloud Security Model Impact Levels. Second, the concept of Mission Impact to the DoD has been created. Identifying systems that may be of high importance to the specific mission they serve, but are of low impact to the overall mission of the Department to wage war and defend the nation allows DoD Cloud Customers to choose different security profiles for those systems. Proposed change includes a reduced set of security requirements and example systems that might fall into this new category. Finally, this report proposes a new structure of security controls for the Cloud Security Model that simplifies the controls at impact levels 1 and 2 for confidentiality and integrity protection of DoD public information.

A key part of this report is clear guidance to both Cloud Service Providers and DoD Cloud Customers. This report describes the cradle-to-grave process that both a Cloud Service Provider and a DoD Cloud Customer follow in order to move DoD computing into commercial cloud infrastructure. There is separate guidance for each audience but it is written to show the relationships between the two. The descriptions cover how to identify the appropriate security controls, gain approval to operate for DoD computing, maintain and sustain the risk posture, and report risk status.

In order to provide clearer guidance on the actual connection of commercial infrastructure to DoD networks, this effort has created a detailed reference architecture and guidance. This new architectural guidance is consistent with the NIPRNet hardening efforts in DISA and the Joint Information Environment Cyber Security Architecture (formerly called the Single Security Architecture).

Finally, analysis during this effort identified key additional work items that the Department must complete to implement the recommendations contained in the report and remove current barriers to the use of commercial cloud. These items include additional technical refinement of the security requirements, updating of certain DoD policies that hinder the use of commercial cloud, and continued resolution of legal issues that constrain the use of commercial cloud.

1. Introduction

The purpose of this document is to provide clear guidance to the Cloud Service Providers and to Department of Defense (DoD) customer organizations in support of the DoD Chief Information Officer's (CIO) goal to accelerate the adoption of cloud computing within the DoD. The document is the result of a concentrated 45 day effort by the DoD CIO's office, the Defense Information Systems Agency, and the National Security Agency. Section 2 describes the complete process for Cloud Service Providers (CSPs) to become part of the ECSB Cloud Service Catalog and host DoD Cloud Customers. Section 3 contains a reference architecture with multiple views to illustrate, but not limit, how CSPs can meet DoD requirements to offer services to DoD Cloud Customers. Section 4 defines how DoD Cloud Customers can acquire cloud services, what responsibilities they accept with such services, and how cloud acquisition fits into the DoD Risk Management Framework (RMF) Authorization Process. In addition, Section 5 lists a set on continuing tasks necessary to achieve DoD's cloud computing goals.

The Defense Information Systems Agency (DISA) performs cloud brokerage functions for the DoD. As the Enterprise Cloud Service Broker (ECSB), DISA maintains an ECSB Cloud Service Catalog of approved CSPs, manages the process for CSPs to become part of the ECSB Cloud Service Catalog, and facilitates DoD Cloud Customers in acquiring cloud services.

One of the ECSB's duties is to ensure the security of DoD data in cloud service offerings. To this end, the ECSB developed a Cloud Security Model (CSM) that defines the security requirements for CSPs that wish to become part of the ECSB Cloud Service Catalog and offer services to DoD Cloud Customers [1]. The CSM is built upon the Risk Management Framework and Federal Risk and Authorization Management Program (FedRAMP) to integrate with the DoD RMF Authorization Process and Office of Management and Budget (OMB) policy regarding federal government use of cloud computing. The CSM lists requirements that address:

- Implementation of applicable FedRAMP, Committee on National Security Systems (CNSS), and DoD security controls
- Integration with DoD Information Assurance (IA) architecture, policy, guidance, and operational constraints
- Continuous monitoring
- Incident reporting

DoD missions and data vary widely by impact and sensitivity. To best accommodate the full range of DoD Cloud Customer needs, two factors need to be considered; the impact of data loss/compromise (security) and the priority of the application(s) relative to the primary mission of the DoD (Mission Impact – as explained in Section 4 below). The CSM defines multiple impact levels that enable the ECSB to match DoD Cloud Customers with cloud services that offer an appropriate level of security. The current impact levels are described below based on information type and confidentiality/integrity impacts as defined by DoD Cloud Customer and policy. Availability is handled independent of the impact levels through the Service Level Agreement between the DoD Cloud Customer and the CSP.

Level 1 Unclassified publicly releasable information e.g., recruiting websites.

Level 2 Unclassified publicly releasable information, with access controls e.g., library systems.

Level 3 Non-National Security System (non-NSS) Controlled Unclassified Information (CUI) – Low confidentiality impact, Moderate integrity impact e.g., training systems.

Level 4 Non-NSS CUI – Moderate confidentiality impact, Moderate integrity impact e.g., HR systems.

Level 5 NSS CUI – Moderate confidentiality impact, Moderate integrity impact e.g., email systems.

Level 6 Classified information up to and including SECRET – Moderate confidentiality impact, Moderate integrity impact e.g., C2 systems.

There are many combinations of information types and impact for both confidentiality and integrity. The ECSB has defined the six impact levels based on the expectation that DoD Cloud Customer’s missions will use predefined impact levels as foundation for the tailored set of requirements, and that CSP implementation for all six impact levels have varying costs associated with implementing their systems at each of these levels. DoD Cloud Customers are expected to use the impact level that best guards against the highest impact concern for their mission, data, and application. DoD Cloud Customers should use these levels as the basis for their requirements, and tailor them as necessary for the data and importance of their mission. For example, if a mission has high confidentiality and/or high integrity impact, additional controls will have to be added over the CSM impact levels. The work performed during this effort lays the groundwork for collapsing some of the levels.

This paper proposes reductions to the number of security controls required by version 2.1 of the CSM to reflect a new balance of risk and cost at all impact levels. Delineating specific impact levels for Non-National Security System (non-NSS) and National Security System (NSS) missions is also recommended. The concept of Mission Impact to the DoD is introduced and used to recommend a lesser set of requirements for certain missions. In addition, a consolidation of the technical architectures is recommended to better support the different impact levels. These actions support the goal to accelerate deployments of missions at all impact levels to cloud services in the near term.

There are multiple service and deployment models that are cited in this document and the CSM. A key distinction is made between clouds that are dedicated to the DoD and the federal government, and those that are shared with other non-federal government tenants. The terms ‘dedicated infrastructure’ and ‘community cloud’ refer to cloud infrastructures that are provisioned for the exclusive use of the DoD and US federal government. The terms ‘shared infrastructure’, ‘public cloud’, and ‘multi-tenancy’ refer to cloud infrastructures that may be shared with non-DoD and non-US federal government tenants and depend on logical controls to maintain separation between tenants. On or off ‘premises’ refers to whether or not cloud infrastructure exists in a DoD facility. Even when off-premises solutions are used, all data stored and processed for the DoD must reside in a facility under the legal jurisdiction of the United States.

Infrastructure as a Service (IaaS) is a particular focus in this document since the DoD considers it to be foundational to higher level service models that that follow (e.g., Platform as a Service (PaaS), and Software as a Service (SaaS)). Preceding any consideration of using a higher level service, it must be determined that the underlying infrastructure meets DoD requirements.

2. Guidance to Cloud Service Providers (CSPs)

This section describes the complete process for Cloud Service Providers (CSPs) to become authorized to host computing services for DoD Cloud Customers. The subsections that follow lay out the end-to-end workflow to provide CSPs a guide to the activities necessary to open contracting negotiations with DoD Cloud Customers, to participate in the Enterprise Cloud Service Broker (ECSB) Cloud Service Catalog [2], become selected to provide cloud services, and to satisfy periodic security posture re-evaluations to remain in the catalog.

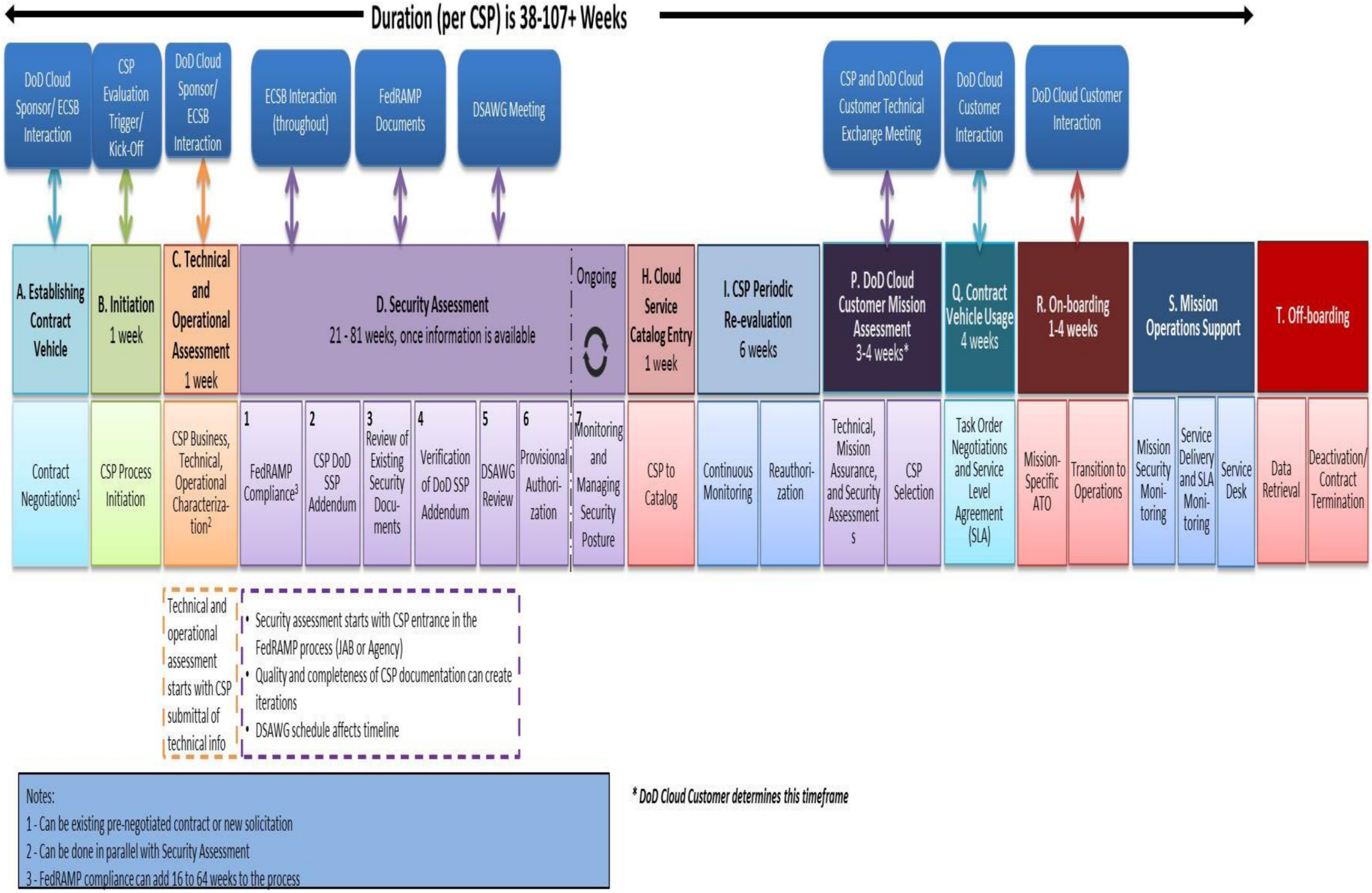
The ECSB Cloud Service Catalog provides information about DoD-approved CSPs so that mission requirements from DoD Cloud Customers can be matched to approved computing "containers" hosted by the CSPs. The "container" refers to the ECSB-approved cloud service offered by a CSP, and it encompasses all DoD customer systems and data that reside in that cloud service. The DoD Provisional Authorization (PA) of this container certifies appropriate DoD security requirements, as defined in the CSM, have been and will continue to be met for the container only, and not for the overall mission for which the container will be employed. Since the ECSB certification and DoD PA process determines container risk only, the overall mission risk will continue to be assessed and authorized by the mission owner's Authorizing Official (AO) through the current DoD risk management process (see Blocks P-R in Section 2.1 below).

The mission owner is the "DoD Cloud Customer" for a CSP. Items such as computation, data storage, and web portal hosting are examples of cloud services the CSP will be contracted to host for the DoD Cloud Customer. The CSP is expected to work with the DoD Cloud Customer to document mission-specific requirements such as minimum levels of system availability, and to provide access for physical and cybersecurity evaluations so the DoD Cloud Customer retains Authority To Operate (ATO) for that mission.

The Department will perform a technical and cybersecurity evaluations of all candidate Cloud Service Providers to provide PA for each container. The technical evaluation is to ensure providers can meet requirements to support a broad array of DoD missions. The cybersecurity evaluation is based on FedRAMP compliance, with additional security requirements for DoD systems for the protection of sensitive mission and personal data (see Figure 3).

2.1. Cloud Service Provider (CSP) Workflow

Figure 1 provides a high-level view of the processes a CSP must satisfy to successfully complete container evaluation, DoD Provisional Authorization (PA), the DoD Cloud Customer ATO, on-boarding and service operations when supporting DoD missions. Timelines shown are notional and dependent on the security status of the CSP, and cloud readiness of the DoD mission.


Duration (per CSP) is 38-107+ Weeks
DoD Cloud Sponsor/ ECSB Interaction
CSP Evaluation Trigger/ Kick-Off
DoD Cloud Sponsor/ ECSB Interaction
ECSB Interaction (throughout)
FedRAMP Documents
DSAWG Meeting
CSP and DoD Cloud Customer Technical Exchange Meeting
DoD Cloud Customer Interaction
DoD Cloud Customer Interaction
A. Establishing Contract Vehicle
B. Initiation 1 week
C. Technical and Operational Assessment 1 week
D. Security Assessment 21 - 81 weeks, once information is available
Ongoing
H. Cloud Service Catalog Entry 1 week
I. CSP Periodic Re-evaluation 6 weeks
P. DoD Cloud Customer Mission Assessment 3-4 weeks*
Q. Contract Vehicle Usage 4 weeks
R. On-boarding 1-4 weeks
S. Mission Operations Support
T. Off-boarding
Contract Negotiations¹
CSP Process Initiation
CSP Business, Technical, Operational Characteriza-tion²
1 FedRAMP Compliance³
2 CSP DoD SSP Addendum
3 Review of Existing Security Docu-ments
4 Verification of DoD SSP Addendum
5 DSAWG Review
6 Provisional Authori-zation
7 Monitoring and Managing Security Posture
CSP to Catalog
Continuous Monitoring
Reauthori-zation
Technical, Mission Assurance, and Security Assessment s
CSP Selection
Task Order Negotiations and Service Level Agreement (SLA)
Mission-Specific ATO
Transition to Operations
Mission Security Moni-toring
Service Delivery and SLA Moni-toring
Service Desk
Data Retrieval
Deactivation/ Contract Termination

Technical and operational assessment starts with CSP submittal of technical info

- Security assessment starts with CSP entrance in the FedRAMP process (JAB or Agency)
- Quality and completeness of CSP documentation can create iterations
- DSAWG schedule affects timeline

Notes:
1 - Can be existing pre-negotiated contract or new solicitation
2 - Can be done in parallel with Security Assessment
3 - FedRAMP compliance can add 16 to 64 weeks to the process

** DoD Cloud Customer determines this timeframe*

Figure 1: Cloud Service Provider (CSP) Workflow

Block A: A DoD contract is required for CSPs to begin the process of becoming part of the ECSB Cloud Service Catalog [2] and offering services to DoD Cloud Customers. The DoD Cloud Sponsor is responsible for initiating the acquisition process to provide a new contract for the CSP. Alternatively, the DoD Cloud Sponsor may also negotiate an agreement with another DoD or US federal government entity to utilize an existing contract with the CSP. CSPs may initiate the process by responding to published DoD needs found via the Federal Business Opportunities webpage [3]. A detailed acquisition plan for CSPs new to the ECSB Cloud Service Catalog is forthcoming and discussed in Section 5.18.

Block B: A DoD Cloud Sponsor or DoD Cloud Customer can initiate the CSP evaluation once suitable contracts/agreements have been reached between the ECSB, the DoD Cloud Sponsor, and the CSP. Information needs are communicated to the CSP to enable the DoD to perform CSP assessments described in Block C.

Block C: The ECSB will evaluate business, technical, operations, and service information provided by the CSP to characterize those aspects of the cloud services offered. This information forms the initial basis for a CSP's entry in the ECSB Cloud Service Catalog. The CSP is asked to provide the following information, where appropriate:

- *Overview attributes:* Business, Contact, Service Name, Facilities, Billing, Accreditation/Certification, and Third Party Audit Information
- *Technical and Operations attributes:* Availability, Help Desk Availability, Monitoring, Notification, and Reporting, System/Service Changes, Non-Production Environments, Transparency, User Control, On-Boarding, Off-Boarding, Disaster/Problem Recovery, Compliance
- *Service Models:* IaaS, PaaS, and SaaS

Block D: This block illustrates the two major steps in the DoD security assessment process for the CSP container. The first covers FedRAMP requirements, and the second covers any DoD-specific security requirements relevant to the CSM level for which the container will be approved. CSPs must successfully complete the FedRAMP assessment process, either through a JAB Provisional Authorization or Agency ATO. The JAB PA can be attained via a third party assessment organization (3PAO), an entity that will confirm that FedRAMP Security Baseline requirements are satisfied, then submit a report to be approved by the JAB. Alternately, a Federal Agency can execute the FISMA process via the agency FSO, where the FISMA accreditation is accepted in place of the FedRAMP JAB PA, and the mission is provided an ATO from that agency's AO.

The CSP will need to comply with additional DoD requirements documented in the DoD Addendum to the FedRAMP System Security Plan (SSP). The Addendum will contain additional DoD requirements based on the Service Model (IaaS, PaaS, or SaaS) and the impact level (CSM Levels 1-6) of data being hosted. Accommodations are made on a case-by-case basis for CSPs whose cloud services are limited to only DoD tenants.

- To the extent possible, existing FedRAMP, DIACAP and industry standard security artifacts and certifications will be leveraged through reciprocity.
- Verification of the CSPs compliance with DoD's security requirements, in accordance with the Cloud Security Model.
- Before making the authorization decision, the DISA Authorizing Official (AO) coordinates a review with the Defense Information Assurance Security Accreditation Working Group (DSAWG). The DISA AO has responsibility for granting DoD Provisional Authorization for operations within a CSP's container(s) including use, conditions, limitations and follow-on actions for the CSP.

- The ECSB does follow-on coordination with the CSP and FedRAMP Program Management Office (PMO) in maintaining the CSP's security posture. See Section 2.2.1 below for more details related to ongoing assessment and authorization.

Block H: The ECSB will enter information about the CSP's services in the Enterprise Cloud Service Provider (ECSB) Cloud Service Catalog based on data collected in Block B above, and refined through subsequent interactions with the CSP.

Block I: This block shows the CSP's responsibility for continuous monitoring of their cloud service offering. The CSP is expected to detect changes in the security posture of the system through this monitoring, and alert DoD Cloud Customers of any such changes. The CSP will provide reports to the DoD Cloud Customer, the ECSB, and to a Computer Network Defense Service Provider (CNDSP) Tier II to support DoD cybersecurity operations.

Periodically the ECSB Security Assessment team will formally re-evaluate the CSP in accordance with the security model. CSPs will self-attest that it continues to meet all requirements.

Block P: Once the CSP has DoD Provisional Authorization for a container, that information is entered into the ECSB Cloud Service Catalog. The entry of the CSP into the ECSB Cloud Service Catalog indicates to DoD Cloud Customers that they may leverage ECSB security assessments for the computing infrastructure within that CSP container, "inheriting" those accreditations for the purposes of any necessary follow-on ATO assessments specific to that customer's hosted mission data/services.

The DoD Cloud Customer will discuss detailed mission requirements with a candidate Cloud Service Providers from the ECSB Cloud Service Catalog to understand the details of the service the CSP offers and how that service could support mission requirements, and at what cost. Performance parameters may include:

- Usage or budget quota
- Configuration options (e.g., operating system, storage min/max)
- Response time for scaling service up or down
- Identity management and access control
- Data handling
- Availability
- Other

The DoD Cloud Customer will identify the CSP chosen to support their Cloud Service Request and notify the ECSB. At this point, the CSP will be notified by the ECSB that they are being requested to provide services to that DoD Cloud Customer.

Block Q: CSPs will enter into a contractual relationship with the DoD Cloud Customers to provide cloud services. The CSP and DoD Cloud Customer will negotiate the appropriate terms of service in compliance with DoD cloud contracting guidelines, and enter into service level agreements to further define service delivery and operating parameters for the cloud service. This contracting documentation is the place where mission-specific performance parameters and requirements such as system availability and CNDSP reporting mechanisms/timelines can be captured.

Block R: On-boarding activities occur after the contractual relationship between the CSP and the DoD Cloud Customer is in place. The DoD Cloud Customer is responsible for working with the CSP to get detailed information about how service is delivered, and document the parameters used to measure service performance in support of achieving an ATO. The DoD Cloud Customer's AO grants authority to operate based on requirements from the DoD Cloud Customer's Cloud Service Request. The DoD Cloud Customer remains responsible for the risk posture of the system, but the CSP is required to undergo periodic re-evaluation of its security posture to ensure the container remains fit to support DoD missions (upkeep of the container PA or ATO), as well as remain accredited to host the DoD Cloud Customer's data (upkeep the mission-specific ATO).

Once the CSP and the DoD Cloud Customer have documented service delivery parameters, and the DoD Cloud Customer achieves ATO for their mission data/service, operations may begin. The DoD Cloud Customer and CSP will work together to establish operational capability. The ECSB Service Operations Team may assist as necessary. Steps will vary depending on the nature of the cloud service, but may include:

- Establish connectivity
- Migrate data and/or applications to the CSP
- Identify users and manage user access
- Identify user access devices and manage user access devices
- Test
- Monitor and report results
- Confirm readiness to operate (Operational Readiness Review)
- Service activation
- Off-board service (transition out of operation; deactivation)

Block S: The CSP will continuously monitor their cloud service offering to detect changes in the security posture of the system, and will provide reports to the DoD Cloud Customer and to the ECSB. The ECSB may provide security analysis information to the DoD Cloud Customer. For some systems, the DoD Cloud Customer will also monitor for security issues. This effort may utilize information provided by the CSP and the ECSB, but may also involve information collected independently by the DoD Cloud Customer. Each of these monitoring cases may lead to updated security requirements that will need to be satisfied to maintain either the container PA (or ATO), and that customer's mission ATO.

The CSP will collect and provide metrics related to performance and operations that can be used to assess performance relative to a particular service level agreement. The ECSB will monitor health and status, performance and operational metrics. Periodically the ECSB will ask the DoD Cloud Customer to rate the service they are receiving from the CSP.

In general the service desk function is a shared function between operational organizations from the CSP, the DoD Cloud Customer, and the ECSB. Depending on the type of service being acquired from the CSP and the impact level of the mission, the DoD Cloud Customer may be able to choose from different levels (or tiers) of service desk support.

Block T: DoD Missions will continue to operate within a CSP container until contract termination, or until shutdown of service occurs that results from changes at the CSP. DoD Cloud Customers are responsible for the off boarding of the DoD mission(s) affected, to include retrieval/recovery of all mission data. However, the CSP hosting DoD missions are responsible for making the data associated with that mission available to the DoD within timeframes captured in the contract documents defining the service, and in a format defined by the DoD Cloud Customer. Successful off-boarding requires the CSP to satisfy all data sanitization requirements and, when necessary, hardware sanitization or destruction requirements called for by contractual and security documentation for the DoD Cloud Customer's mission.

2.2. Information Important to the CSP Process

This section contains more detailed information on some of the important items mentioned in Figure 1 and the block descriptions above.

2.2.1. Authorizations and Monitoring

2.2.1.1. FedRAMP Assessment

OMB policy requires Federal departments and agencies to comply with FedRAMP guidelines and share Agency ATO documentation with the FedRAMP Secure Repository. DoD will follow this guidance for commercial cloud services. Both commercial cloud services sponsored by DoD, and DoD-owned and operated cloud services must follow OMB policy and submit artifacts to the FedRAMP Secure Repository documenting a FedRAMP Joint Authorization Board (JAB) PA or a Federal Agency ATO. The DoD will honor a Federal Agency ATO in place of a JAB PA (i.e. "reciprocity" of the two authorizations) for DoD cloud services during the RMF Authorization Process provided the documentation resides in the FedRAMP Secure Repository.

2.2.1.2. DISA Field Security Operations (FSO) Assessment

The ECSB FSO will leverage FedRAMP PAs and Federal Agency ATO packages residing in the FedRAMP Secure Repository and assess CSPs for only the additional NIST SP 800-53 controls and control enhancements as required by the ECSB CSM to arrive at a DoD ECSB PA. DoD Information Systems (ISs) are subject to CNSSI-1253, so these additional controls and enhancements depend on the ECSB information impact level for which the container is being accredited. FSO will coordinate with the CSP and their 3PAO to complete the DoD assessments.

2.2.1.3. Continuous Monitoring and Ongoing Assessments

The ECSB requires an ongoing assessment and authorization capability for CSPs providing services to the DoD. This capability, specific to DoD, is built upon the foundation of the FedRAMP continuous monitoring strategy, as described in the FedRAMP CONOPS and Continuous Monitoring Strategy Guide [4].

The DoD will review artifacts provided through the FedRAMP continuous monitoring process, in addition to evidence resulting from the implementation of any DoD-specific controls required beyond the FedRAMP requirements on a continuous, ongoing basis. That information will be used in support of the annual re-authorization of each service.

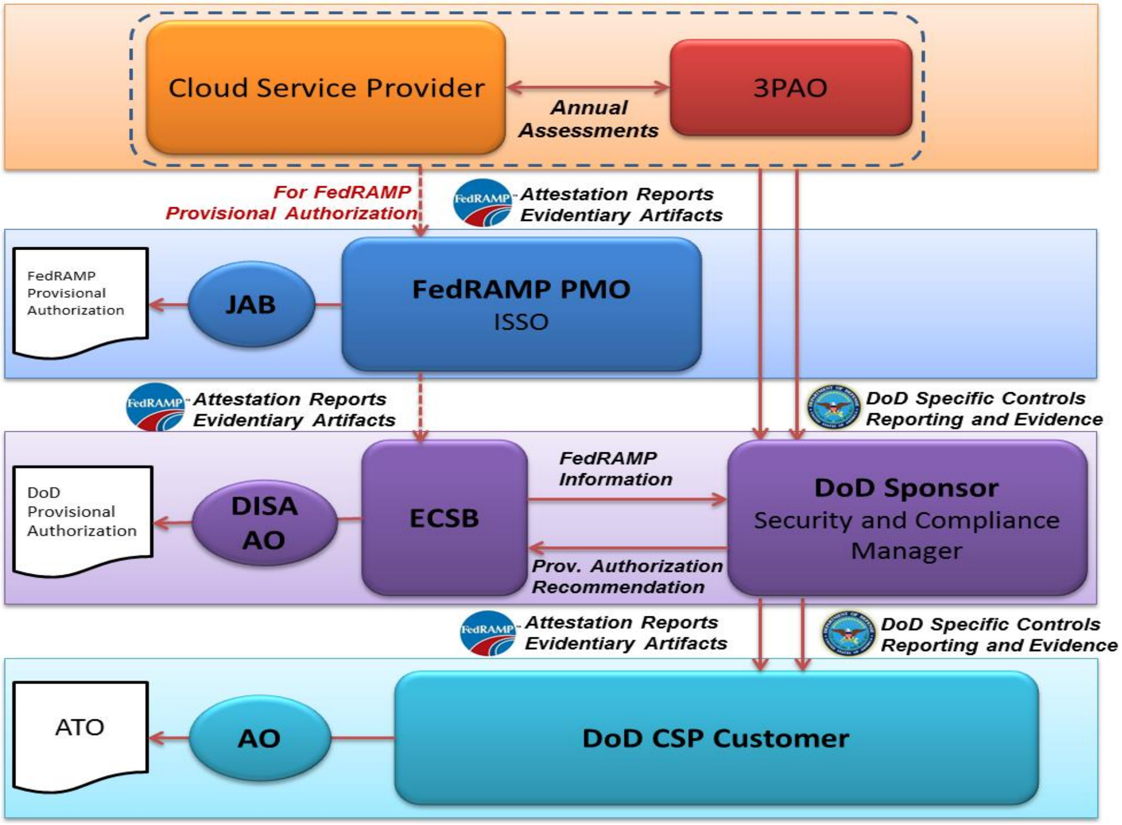

Cloud Service Provider
Annual Assessments
3PAO
For FedRAMP Provisional Authorization
Attestation Reports Evidentiary Artifacts
FedRAMP Provisional Authorization
JAB
FedRAMP PMO
ISSO
Attestation Reports Evidentiary Artifacts
DoD Specific Controls Reporting and Evidence
DoD Provisional Authorization
DISA AO
ECSB
FedRAMP Information
Prov. Authorization Recommendation
DoD Sponsor
Security and Compliance Manager
Attestation Reports Evidentiary Artifacts
DoD Specific Controls Reporting and Evidence
ATO
AO
DoD CSP Customer

Figure 2: DoD Ongoing Assessment and Authorization

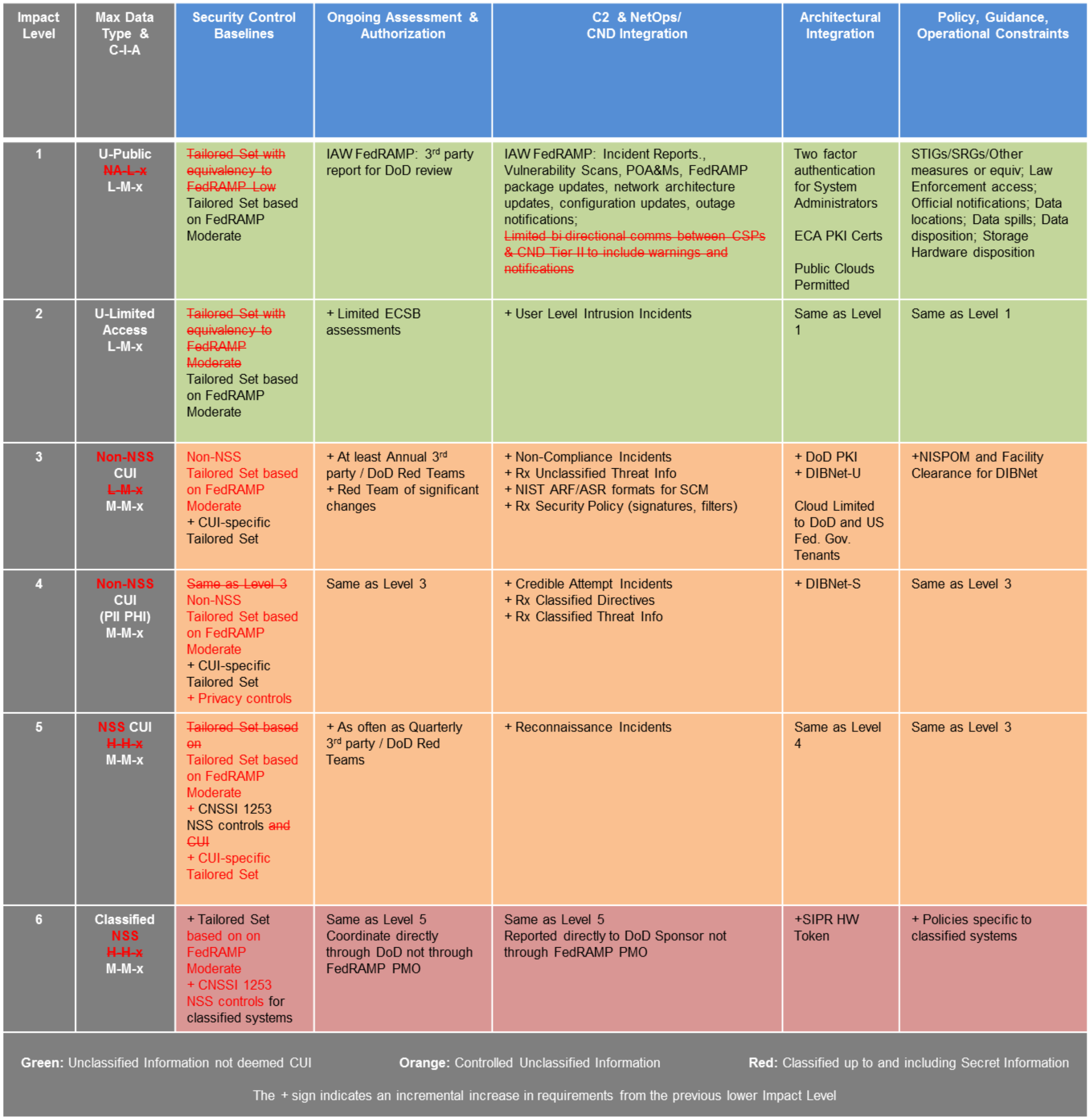
2.2.2.DoD Separation

CSP systems that contain DoD data must provide appropriate separation between CSP resources to ensure adequate security in accordance with the Multi-Tenants Cloud Hosting Location Matrix located in Section 3, Figure 5. The reference architecture views described in Section 3 illustrate separation requirement differences based on impact levels, location of the CSP container, and the way the container computing and networking infrastructure is designed. As highlighted in Section 5.12, work is under way to update hosting separation requirements.

2.2.3.Security Controls

The ECSB Cloud Security Model is based on the Risk Management Framework. Like FedRAMP, the ECSB utilizes baselines selected from the SP800-53 library of security controls. Unlike those in FedRAMP, some DoD systems are National Security Systems (NSS) and thus are subject to control baselines specified by CNSSI-1253. Impact Level 6 systems are also subject to the CNSSI-1253 Classified Information Overlay. Non-NSS systems may also have requirements that exceed the FedRAMP baseline. Consistent with these constraints, Figure 3 shows each CSM Impact Level and the associated set of security controls required by the ECSB that must be implemented in addition to those required by FedRAMP.

CSPs may offer equivalent controls, as appropriate, for consideration. CSP measures that provide similar risk mitigation as a required control, or negate the risk the control is intended to mitigate, can be considered an equivalency. Any potential equivalency is evaluated during CSP assessments, and final risk decisions for equivalencies are made by the DISA AO as part of the Provisional Authorization process.



Impact Level	Max Data Type & C-I-A	Security Control Baselines	Ongoing Assessment & Authorization	C2 & NetOps/ CND Integration	Architectural Integration	Policy, Guidance, Operational Constraints
1	U-Public ~~NA-L-x~~ L-M-x	~~Tailored Set with equivalency to FedRAMP Low~~ Tailored Set based on FedRAMP Moderate	IAW FedRAMP: 3rd party report for DoD review	IAW FedRAMP: Incident Reports., Vulnerability Scans, POA&Ms, FedRAMP package updates, network architecture updates, configuration updates, outage notifications; ~~Limited bi-directional comms between CSPs & CND Tier II to include warnings and notifications~~	Two factor authentication for System Administrators ECA PKI Certs Public Clouds Permitted	STIGs/SRGs/Other measures or equiv; Law Enforcement access; Official notifications; Data locations; Data spills; Data disposition; Storage Hardware disposition
2	U-Limited Access L-M-x	~~Tailored Set with equivalency to FedRAMP Moderate~~ Tailored Set based on FedRAMP Moderate	+ Limited ECSB assessments	+ User Level Intrusion Incidents	Same as Level 1	Same as Level 1
3	Non-NSS CUI ~~L-M-x~~ M-M-x	Non-NSS Tailored Set based on FedRAMP Moderate + CUI-specific Tailored Set	+ At least Annual 3rd party / DoD Red Teams + Red Team of significant changes	+ Non-Compliance Incidents + Rx Unclassified Threat Info + NIST ARF/ASR formats for SCM + Rx Security Policy (signatures, filters)	+ DoD PKI + DIBNet-U Cloud Limited to DoD and US Fed. Gov. Tenants	+NISPOM and Facility Clearance for DIBNet
4	Non-NSS CUI (PII PHI) M-M-x	~~Same as Level 3~~ Non-NSS Tailored Set based on FedRAMP Moderate + CUI-specific Tailored Set + Privacy controls	Same as Level 3	+ Credible Attempt Incidents + Rx Classified Directives + Rx Classified Threat Info	+ DIBNet-S	Same as Level 3
5	NSS CUI ~~H-H-x~~ M-M-x	~~Tailored Set based on~~ Tailored Set based on FedRAMP Moderate + CNSSI 1253 NSS controls ~~and CUI~~ + CUI-specific Tailored Set	+ As often as Quarterly 3rd party / DoD Red Teams	+ Reconnaissance Incidents	Same as Level 4	Same as Level 3
6	Classified NSS ~~H-H-x~~ M-M-x	+ Tailored Set based on on FedRAMP Moderate + CNSSI 1253 NSS controls for classified systems	Same as Level 5 Coordinate directly through DoD not through FedRAMP PMO	Same as Level 5 Reported directly to DoD Sponsor not through FedRAMP PMO	+SIPR HW Token	+ Policies specific to classified systems

Green: Unclassified Information not deemed CUI **Orange:** Controlled Unclassified Information **Red:** Classified up to and including Secret Information

The + sign indicates an incremental increase in requirements from the previous lower Impact Level

Figure 3: ECSB Cloud Security Model

2.2.4. Defense Industrial Base Cybersecurity and Information Assurance (DIB CS/IA)

The Defense Industrial Base Cybersecurity and Information Assurance (DIB CS/IA) Program was created to enhance and supplement participants' capabilities to safeguard DoD information that resides on or transits participants' networks. Participation in DIB CS/IA is mandatory for CSPs in the ECSB Cloud Service Catalog at Impact Levels 3-6. Participation in the program enables CSPs to access DIBNet, the network used to share threat information and CYBERCOM notifications with CSPs, as well as report incidents to CNDSP Tier II. DIB CS/IA participation requires CSPs to sign an NDA to protect shared threat information [5].

2.2.5.Public Key Infrastructure (PKI)

Whenever a CSP is hosting DoD data at Impact Levels 2-6, the CSP is responsible for authentication of entities attempting to access a hosted DoD information system. For Impact Level 2, authentication methods other than DoD PKI may be used as defined in DoDI 8520.03. The CSP will use either DoD-issued PKI (i.e. CAC, ALT), or other PKIs approved for use within DoD in accordance with DoDI 8520.02 (e.g. ECA, PIV, PIV-I) for Impact Levels 3-5, and enforce the use of a hardware token for the authentication of end users when required by DoDI 8520.03 [6]. The CSP will use the "DoD SIPRNET Hardware Token" or "Federal Agency Classified token (sometimes called the Common Service Provider token)" for Impact Level 6.

CSPs must make use of DoD OCSP or CRL resources for checking revocation of DoD certificates, DoD Certificate Authorities, and follow DoD instructions and industry best practices for the management and protection of cryptographic keys. DoD-approved PKI credentials may be used to identify applications and services contracted by the DoD, and authenticate CSP personnel and CSP owned assets to DoD systems.

2.2.6.CYBERCOM Warnings, Orders, and Directives

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CNDSP Tier II, as required by FedRAMP Security Control Baseline. These notifications may be generated by CNDSP Tier I or II and may include guidance for countermeasures to be taken by CSPs.

2.2.7.Security Technical Implementation Guides (STIGs)

The Security Technical Implementation Guides (STIGs) are the configuration standards for DoD IA and IA-enabled devices/systems. The STIGs contain technical guidance to “lock down” information systems/software that might otherwise be vulnerable to a malicious computer attack. Additional information regarding STIGs is found at http://iase.disa.mil/stigs/index.html. CSPs must utilize STIGs/Security Requirement Guides (SRGs) in their hardware and software configurations. STIGs/SRGs may fulfill the baseline configuration requirement contained in the Security Control Baseline. STIGs are applicable only if the CSP utilizes the product the STIG addresses or the technology a SRG addresses. However, the baseline configuration control applies whether or not a STIG/SRG is available.

2.2.8.Data Spills

DoD users frequently handle data at different classification levels. When data of a certain level of sensitivity is improperly placed on a system not authorized for that classification level, it is referred to as a data spill. These incidents require a response to remove the contaminated data and ensure it cannot be recovered. CSPs must be able to execute data spill responses as determined by the DoD.

2.2.9.Data Interoperability and Portability

Upon request by a DoD Cloud Customer, the CSP shall make all DoD Cloud Customer data available for electronic transfer out of the CSP environment within 60 days from the date of request. Each DoD Cloud Customer may also request different means of data transfer (for example, as called out in the SLA), at its discretion. If an Impact Level 3-5 CSP plans to reuse storage hardware with DoD data at a different sensitivity level, after requested data is successfully transferred from the CSP to DoD, the CSP shall “Purge” all instances of such data from its systems, in accordance with NIST 800-88 and the FedRAMP Security Control Baseline. For Impact Level 6, CSPs cannot reuse nonvolatile storage hardware at a lower level of sensitivity.

CSPs will ensure that no residual DoD data exists on all storage devices that are disposed of, reused in an environment not governed by the agreement between the CSP and DoD, or transferred to a third party, as required by the Security Control Baseline.

Impact Level 1-5 CSPs will ensure this by, at minimum, “Purging” all data on devices prior to disposal, reuse, or transfer, in accordance with NIST 800-88. Devices that are unable to be cleared or purged must be physically destroyed, as defined in NIST 800-88. When there is any doubt to the success of the clearing or purging process, the storage device must be destroyed in accordance with NIST 800-88.

Impact Level 6 CSPs will ensure no residual data exists by sanitizing all media in accordance with NSA/CSS 9-12 Storage Device Declassification Manual.

2.2.10. Personnel Requirements

Impact Level 1-5 CSPs will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the DoD in compliance with HSPD -12, and at a minimum, a NACI investigation and be a US person as defined in Executive Order 12333.

Impact Level 6 CSPs will require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass a National Agency Check with Local Agency Checks and Credit Check (NACLC), and at a minimum, will hold an active DoD SECRET clearance.

All employees of the CSP who have access to government data must sign a non-disclosure agreement.

2.2.11. Facility and National Industrial Security Program Requirements

All CSPs have to meet the facility requirements contained in their respective impact level security control baselines. Impact Level 3-6 CSPs have to meet additional requirements in order to host DIBNet and DoDIN connection equipment. This includes setting up a National Industrial Security Program and obtaining a Facility Clearance, as described in DoD 5220.22M.

2.2.12. Legal Requirements

There are numerous legal requirements associated with storing and processing DoD data. These requirements include DoD and law enforcement access to data, geographic limitations, personnel requirements, and operational constraints. These requirements are detailed in the Cloud Security Model, and are reflected in Figure 3.

For Levels 1-2, systems that hold non-CUI data can be hosted on public, virtually separated environments. CSPs are required to follow FedRAMP requirements as well as to assist law enforcement (LE) in the event of investigation. Contract language needs to clearly explain these activities, including notification clauses and forensics requirements.

For Levels 3-5, systems must maintain separation between tenants of a cloud system as described in Figure 5, the Multi-Tenant Cloud Hosting Location Matrix found in Section 3. In general, this means that virtually separating tenants is allowed if all tenants are Federal government Cloud Customers. Otherwise, the DoD will require the cloud infrastructure to be physically separated from non-DoD/Federal Government tenants until changes recommended as part of the way ahead in Section 5.12 are enacted.

For Level 6, all tenants must DoD entities. Any contain hosting Level 6 data must be physically separate from containers hosting data/services operating at something other than Level 6 as documented in security requirements and STIGs for those systems.

2.2.13. Change Control

The DoD will review all significant changes planned by a CSP. A significant change is defined by FedRAMP and is a change to the scope of an approved PA or an impact to the authorization boundary. A CSP that wants to make a change to their service container must do by submitting a request to the FedRAMP Program Management Office (PMO) via the FedRAMP web page, following the process outlined in the FedRAMP guidelines [7].

3. Reference Architecture/Implementation

Reference architectures are provided to show the connection requirements between a CSP and the DoD. These architectures show the needs for both the DoD and a CSP as part of the connection.

3.1. Purpose

The DoD definition of a reference architecture is: "an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions".

Reference architecture:

- Serves as a reference foundation for architectures and solutions and may also be used for comparison and alignment purposes
- Provides common language for the various stakeholders
- Provides consistency of implementation of technology to solve problems
- Supports the validation of solutions against proven Reference Architecture
- Encourages adherence to common standards, specifications, and patterns

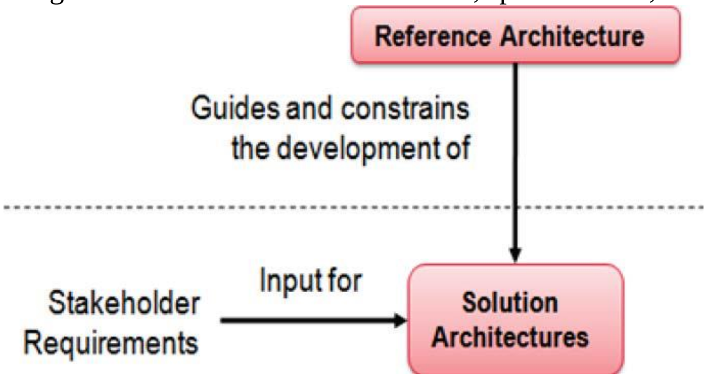


Figure 4: Architecture Context

In order to meet requirements under the Clinger-Cohen Act, Enterprise Architecture enables the Department of Defense to meet criteria such as:

- Focusing information resource planning to support their strategic missions;
- Implementing a capital planning and investment control process that links to budget formulation and execution; and
- Rethinking and restructuring the way they do their work before investing in information systems.

A reference architecture provides a template, often based on the generalization of a set of solutions. These solutions may have been generalized and structured for the depiction of one or more architecture structures based on the harvesting of a set of patterns that have been observed in a number of successful implementations. Further it shows how to compose these parts together into a solution.

Adopting a reference architecture within an organization accelerates delivery through the re-use of an effective solution and provides a basis for governance to ensure the consistency and applicability of technology use within an organization.

3.2. Technical

For the purpose of this document, the architecture is intended to describe the connection architecture and logical placement of security and infrastructure in order to guide development of implementation level design.

3.2.1. Network Planes

A plane, in a networking context, is one of three integral components of the JIE network architecture. These three elements -- the data synchronization/control plane, the user plane and the management plane – can be thought of as different areas of operations. Each plane carries a different type of traffic and is conceptually an overlay network.

The user plane (also known as the forwarding plane, carrier plane or bearer plane) carries the network user traffic. The data sync/control plane carries signaling traffic and data replication between servers/data centers. Control packets originate from or are destined for a router. The management plane carries administrative traffic.

3.2.2. User and Data Plane Connectivity

There are multiple methods of connectivity that are depicted in the architecture.

1) DoD, on-premises connectivity will use existing infrastructure (Government owned) for its user and data planes. Connections will be assessed and authorized the same as any other internal connection.
2) Non-DoD, on-premises service will use government network infrastructure within government boundaries (i.e. NIPRNET) and commercial infrastructure beyond government boundaries (i.e. Internet). Where applicable the infrastructure will use Type 1 encryption or commercial equivalent (CSfC Suite B). Connections will be assessed and authorized the same as any other internal connection on the internal side of the boundary. Connections will be assessed and authorized using the same external connection requirements as any other Internet-facing connection.
3) Non-DoD, extended on-premises (i.e. DISN extension to commercial facility) will use government network infrastructure within government boundaries (i.e. NIPRNET) and commercial infrastructure beyond government boundaries (i.e. Internet). The DISN extension to a commercial facility can be accomplished with an Multiprotocol Label Switching (MPLS) router and optical switch (referred to as a Service Delivery Node). Where applicable the infrastructure will use Type 1 encryption or commercial equivalent (CSfC Suite B). Connections will be assessed and authorized the same as any other internal connection on the internal side of the boundary. Connections will be assessed and authorized using the same external connection requirements as any other Internet-facing connection.
4) Non-DoD, off-premises connectivity will leverage commercial infrastructure but may be augmented with Government Furnished Equipment (GFE) encryption devices. Connections will be assessed and authorized using the same external connection requirements as any other Internet-facing connection.

3.2.3. Management Plane Connectivity

There are multiple methods of connectivity that are depicted in the architecture.

1) Government, on-premises connectivity will utilize existing infrastructure such as the JIE Management Network. No service provider security stack is required.

2) Non-DoD, on-premises service can leverage their existing infrastructure when protected by a DoD security stack and service provider security stack. An encrypted, tunneled connection to the service provider's infrastructure is also allowed.
3) Non-DoD, off-premises can leverage an encrypted, tunneled connection to the service provider's infrastructure that resides on-premises.

3.2.4.Additional Technical Requirements

The DoD uses several robust security stacks to protect and secure the data and network. Commercial entities offering services to DoD must use security stacks (capabilities) equivalent to that of DoD to ensure DoD data is protected.

In order to secure data/network but enable cloud infrastructure to exist and be operated "off-premises", DoD may provide equipment such as encryption devices. The GOTS equipment must be protected from network attack as well as physical security compromise (i.e. theft, tamper, etc.). The DoD will approve the connection mechanisms and placement for Government provided equipment.

3.2.4.1. Computer Network Defense (CND) and Incident Response

Computer Network Defense (CND) addresses the protection of networks, detection of threats, and response to incidents. Cyber Situational Awareness improves the quality and timeliness of collaborative decision-making regarding the employment, protection, and defense of DoD systems and data. Maintaining CND and Cyber Situational Awareness are key challenges to DoD adoption of cloud services.

All CSPs in the ECSB Cloud Service Catalog will be required to be supported by a DoD Computer Network Defense Service Provider (CNDSP) Tier II entity that is dedicated to CSP Operations. The CNDSP Tier II CSP Operations entity will be the DoD Point of Contact (POC) to whom the CSP will report incidents affecting the security posture of the cloud service(s). The CSP will coordinate its response to such incidents with the CNDSP Tier II CSP Operations entity.

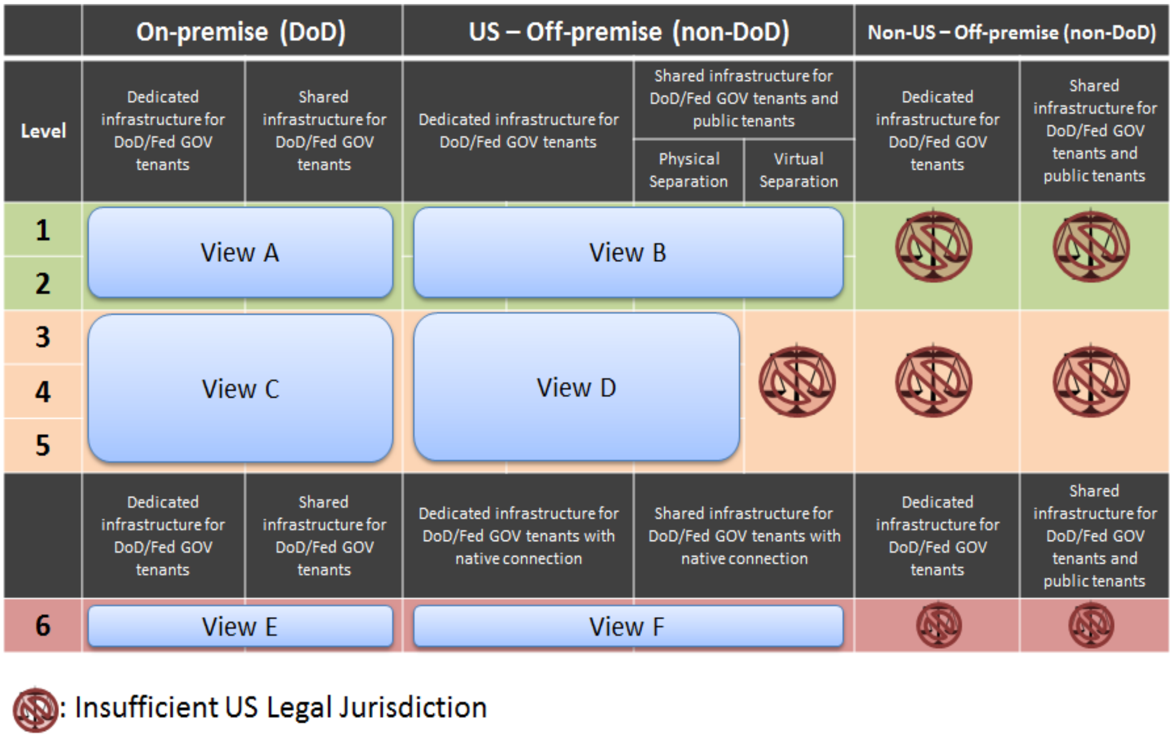
Cloud Service Providers report incidents based on the current and potential impact of the incident or event on the confidentiality, availability, and integrity of organizational operations, organizational assets, or individuals. Incident categories and required reporting timelines from the CSP to CNDSP Tier II are defined in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Appendix A to Enclosure C – Reporting Timelines. Any specification of timelines or deviations must be captured in SLAs and contractual language. CSPs will submit reports using the most protected means available for the affected information system. CSPs will use unclassified reporting mechanisms, such as the DoD Information Network (DoDIN), Defense Industrial Base Network (DIBNet), or non-secure phone/fax only for incidents on unclassified information systems in accordance with CJCSM 6510.01B, Enclosure C, Section 4 and Table C-1. When classified incident reporting is appropriate and directed, CSPs will use SIPRNet, DIBNet-S, or secure phone/fax to report and coordinate incidents as specified.

As described in the Cloud Security Model, a CSP will provide data, including meta data, and web matrix monitoring for law enforcement purposes immediately upon request.

3.2.4.2. Vulnerability Reporting

FedRAMP requires periodic vulnerability scans of CSP systems as part of the Continuous Monitoring Process and in accordance with the FedRAMP Security Control Baseline (SP 800-53 RA-5 and CA-7). Results for these scans must be reported to CNDSP Tier II in CSV, XML, or other approved electronic format. CNDSP Tier II will work with CSPs with regards to the vulnerability scan process and assisting with corrective actions.

3.2.5. Architecture



	On-premise (DoD)		US – Off-premise (non-DoD)			Non-US – Off-premise (non-DoD)	
Level	Dedicated infrastructure for DoD/Fed GOV tenants	Shared infrastructure for DoD/Fed GOV tenants	Dedicated infrastructure for DoD/Fed GOV tenants	Shared infrastructure for DoD/Fed GOV tenants and public tenants		Dedicated infrastructure for DoD/Fed GOV tenants	Shared infrastructure for DoD/Fed GOV tenants and public tenants
				Physical Separation	Virtual Separation		
1 2	View A		View B			⊘	⊘
3 4 5	View C		View D		⊘	⊘	⊘
	Dedicated infrastructure for DoD/Fed GOV tenants	Shared infrastructure for DoD/Fed GOV tenants	Dedicated infrastructure for DoD/Fed GOV tenants with native connection	Shared infrastructure for DoD/Fed GOV tenants with native connection		Dedicated infrastructure for DoD/Fed GOV tenants	Shared infrastructure for DoD/Fed GOV tenants and public tenants
6	View E		View F			⊘	⊘

⊘: Insufficient US Legal Jurisdiction

Figure 5: Multi-Tenant Cloud Hosting Location Matrix

To account for data impact levels and connection/configuration type, the Figure 5 matrix depicts the structure and the table below describes important concepts. This document contains high level abstractions of architecture artifacts produced according to DoDAF 2.0.2 standards. Connection arrangement describes the logical and physical arrangement of systems which enable the DoD environment to be connected to Commercial Systems. These arrangements vary from commercial equipment residing in Government facilities/infrastructure to residing in commercial space. Two additional views (not described in the hosting matrix) are included to provide examples of mixed configurations aggregated into a single operating environment. Additional detail is provided by the Joint Information Environment Cyber Security Reference Architecture V3 at the For Official Use Only level.

View	Type/ Context	Salient Data Points
OV-2	Operational	• CSP reports security event data down to EOC • GEOC/EOC sends direction up to CSP
SV-1	System	• Non-DoD entities are connected through EPP (IAP/MPGW/CDCGW)
SV-2 View A	System	• Fed/DoD Cloud Customers will use dedicated infrastructure • Fed/DoD Cloud Customers can be physically or virtually separated from each other (i.e. Government Community Cloud) • Level 1-2 Data is accessed from the Internet, through the EPP
SV-2 View B	System	• Fed/DoD Cloud Customers in CSP can use dedicated or shared infrastructure • Fed/DoD Cloud Customers can be physically or virtually separated from each other and non-Fed/DoD Cloud Customers • Level 1-2 Data is accessed through the Internet (no encryption)
SV-2 View C	System	• Fed/DoD Cloud Customers will use dedicated infrastructure • Fed/DoD Cloud Customers can be physically or virtually separated from each other (i.e. Government Community Cloud) • Level 3-5 Data is accessed from the Internet, through the EPP, data transmissions are encrypted (TLS, SSL, etc.) • Will use Suite B • Devices will be NIAP compliant
SV-2 View D	System	• Fed/DoD Cloud Customers in CSP will use dedicated infrastructure • Fed/DoD Cloud Customers can be physically or virtually separated from each other (i.e. Government Community Cloud) • Fed/DoD Cloud Customers must be physically separated from non-Fed/DoD Cloud Customers • Level 3-5 Data is accessed from the Internet, through the EPP, and then to the CSP, data transmissions are encrypted (TLS, SSL, etc.) • Will use Suite B • Devices will be NIAP compliant
SV-2 View E	System	• Fed/DoD Cloud Customers will use dedicated infrastructure • Fed/DoD Cloud Customers can be physically or virtually separated from each other (i.e. Government Community Cloud) • Level 6 Data is accessed from the classified fabric (SIPRNet), through the EPP or other security boundary, data transmissions are bulk encrypted (Type 1 or CSfC)
SV-2 View F	System	• Fed/DoD Cloud Customers in CSP will use dedicated infrastructure • Fed/DoD Cloud Customers can be physically or virtually separated from each other (i.e. Government Community Cloud) • Level 6 Data is accessed from the classified fabric (SIPRNet), through the EPP or other JIE security boundary, data transmissions are bulk encrypted (Type 1 or CSfC)

Table 1: Architecture View Salient Details

3.2.6. Cloud/Virtual Layer Security Model

Figure 6 below depicts the capabilities that are included in the DoD Cybersecurity Reference Architecture (CS RA) as available, planned, or new requirement. Protection for the cloud is primarily achieved at OSI layers 1 and 7, but modern tools and techniques have extended capabilities into layers 2-6 and will continue to expand as technology develops.

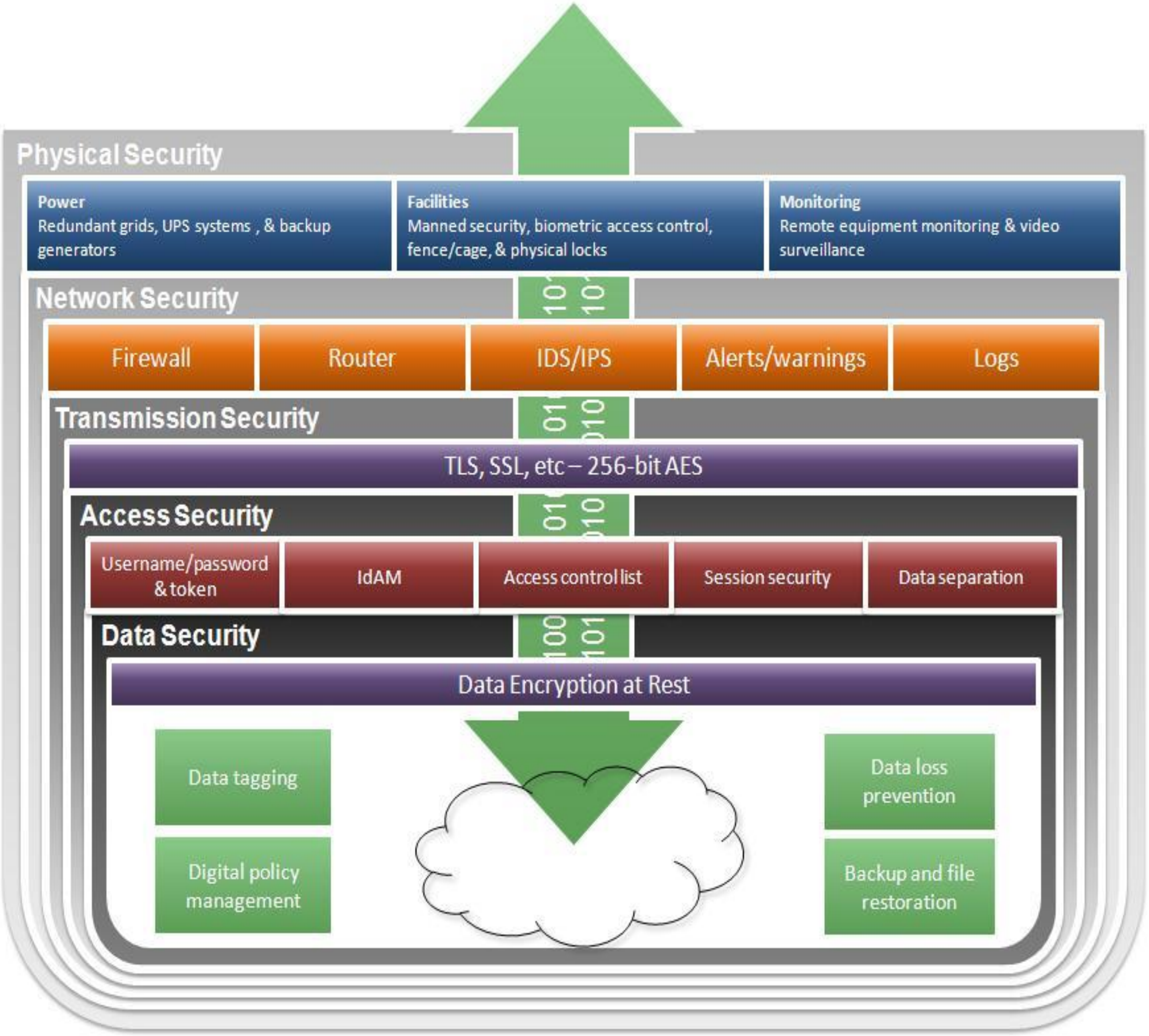

Physical Security
Power
Redundant grids, UPS systems , & backup generators
Facilities
Manned security, biometric access control, fence/cage, & physical locks
Monitoring
Remote equipment monitoring & video surveillance
Network Security
Firewall
Router
IDS/IPS
Alerts/warnings
Logs
Transmission Security
TLS, SSL, etc – 256-bit AES
Access Security
Username/password & token
IdAM
Access control list
Session security
Data separation
Data Security
Data Encryption at Rest
Data tagging
Digital policy management
Data loss prevention
Backup and file restoration

Figure 6: Cloud/Virtual Layer Security Model

Approved for Public Release

3.2.7. Operational View 2 – Operational Entity Context

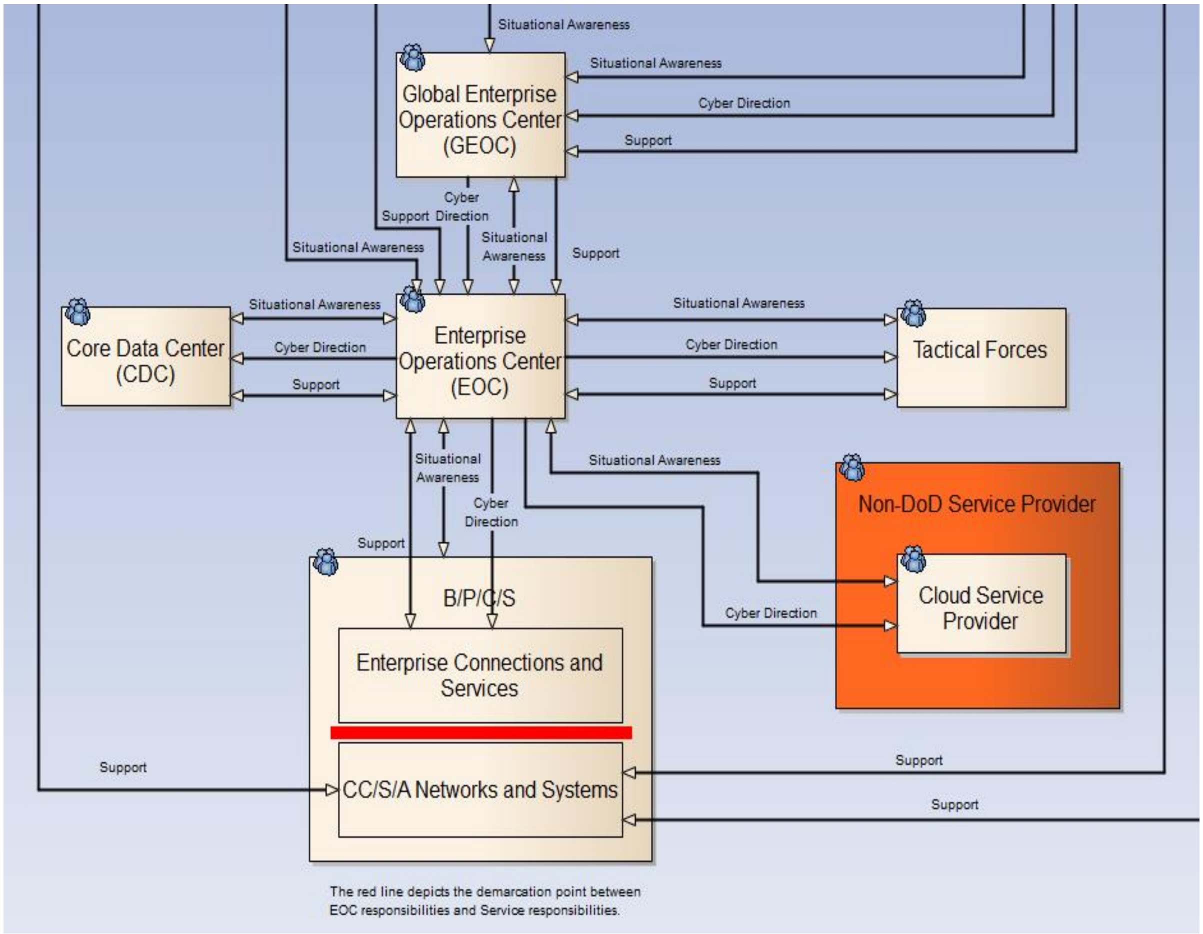


Figure 7: Operational Entity Context

Approved for Public Release

3.2.8. System View 2, View A - On-premises (DoD) Physical & Virtual separation between DoD/Fed GOV tenants

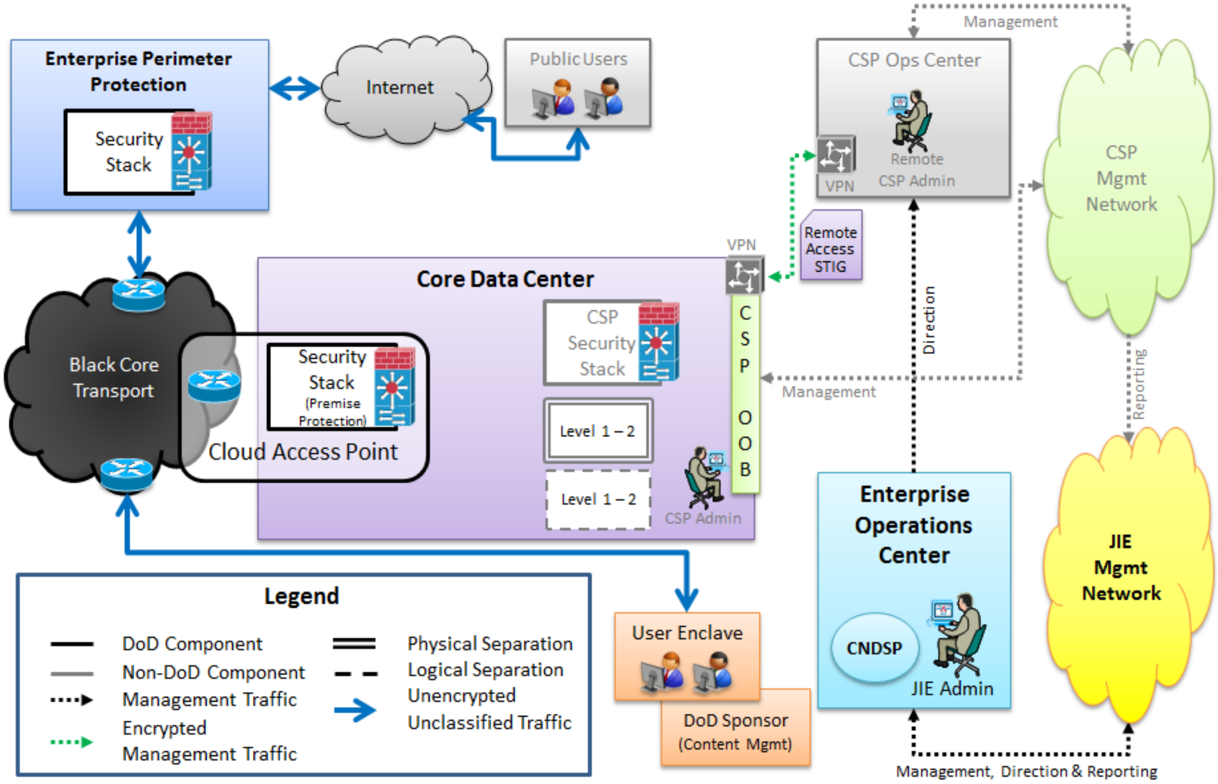


Figure 8: On-premises (DoD) Physical & Virtual separation between DoD/Fed GOV tenants

3.2.9. System View 2, View B - US Off-premises (non-DoD) Physical & Virtual separation between DoD/Fed GOV tenants

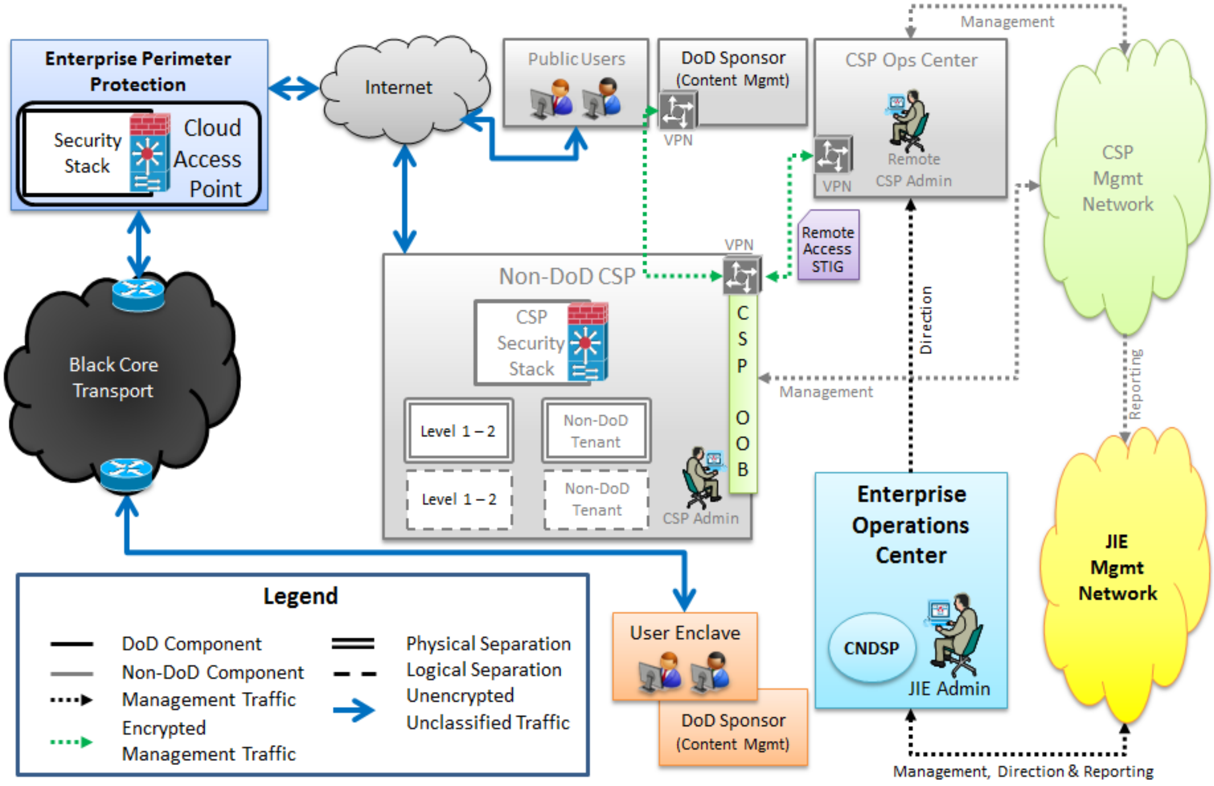


Figure 9: US Off-premises (non-DoD) Physical & Virtual separation between DoD/Fed GOV tenants

3.2.10. System View 2, View C – On-premises (DoD) Physical & Virtual separation between DoD/Fed GOV tenants

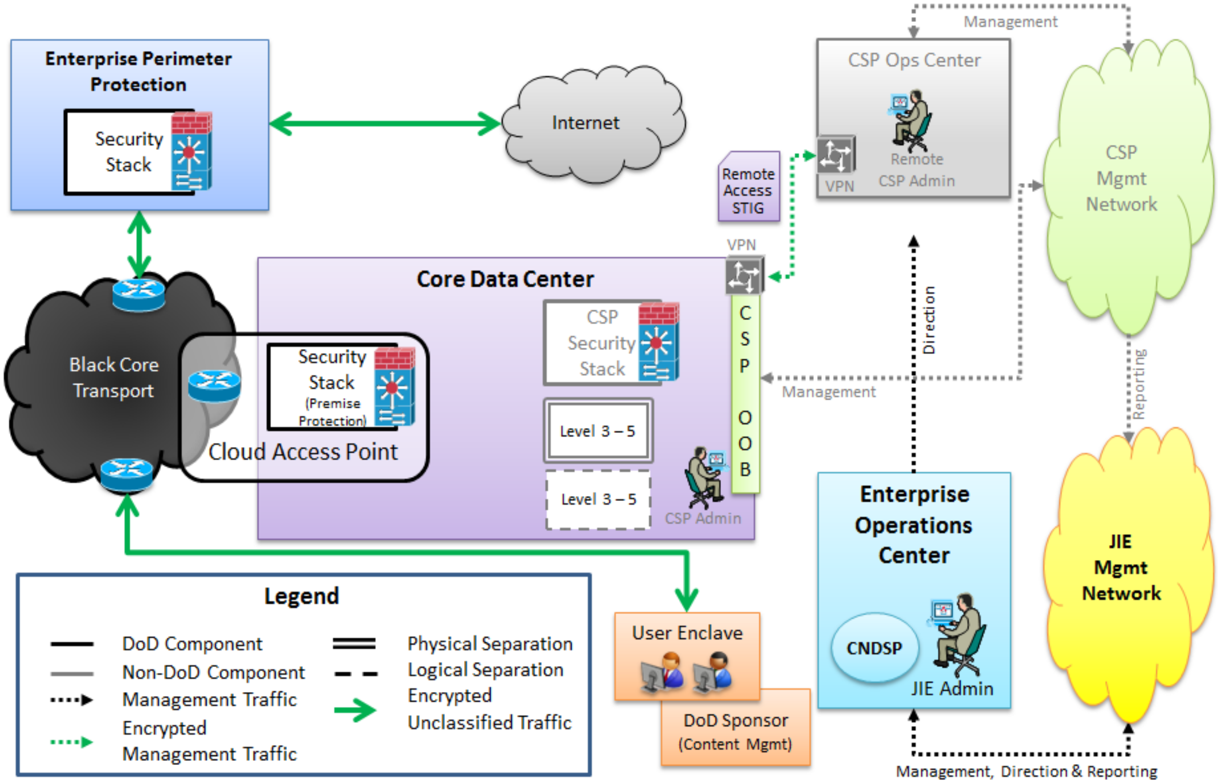


Figure 10: On-premises (DoD) Physical & Virtual separation between DoD/Fed GOV tenants

3.2.11. System View 2, View D – US Off-premises (non-DoD) Physical & Virtual separation between DoD/Fed GOV tenants

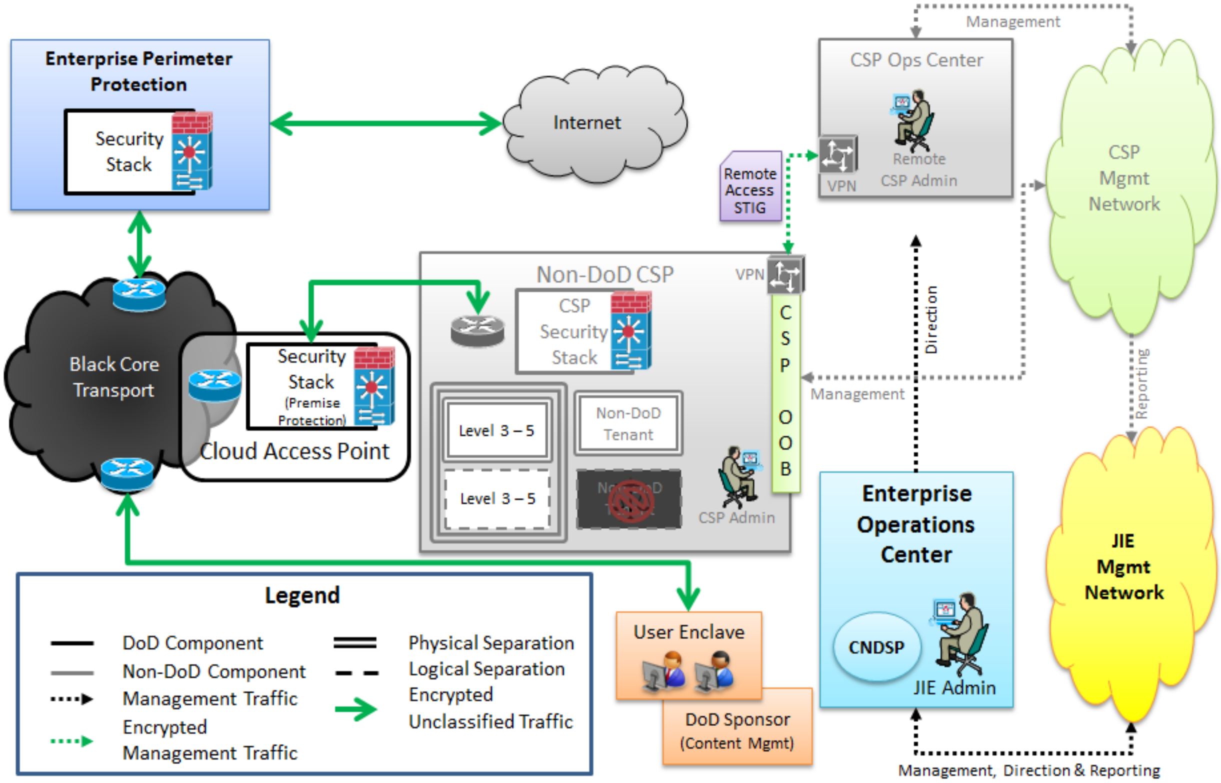


Figure 11: US Off-premises (non-DoD) Physical & Virtual separation between DoD/Fed GOV tenants

Approved for Public Release

3.2.12. System View 2, View E – On-premises (DoD) Physical & Virtual separation between DoD/Fed GOV tenants

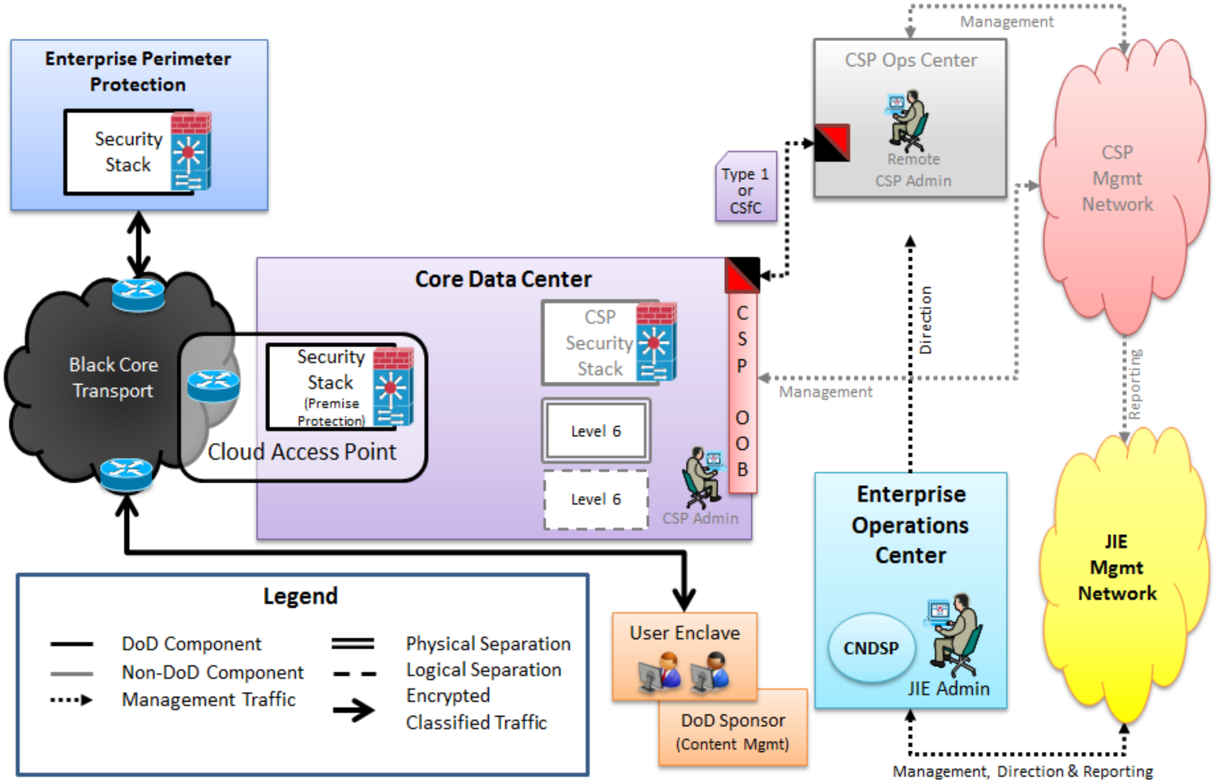


Figure 12: On-premises (DoD) Physical & Virtual separation between DoD/Fed GOV tenants

3.2.13. System View 2, View F – US Off-premises (non-DoD) Physical & Virtual separation between DoD/Fed GOV tenants

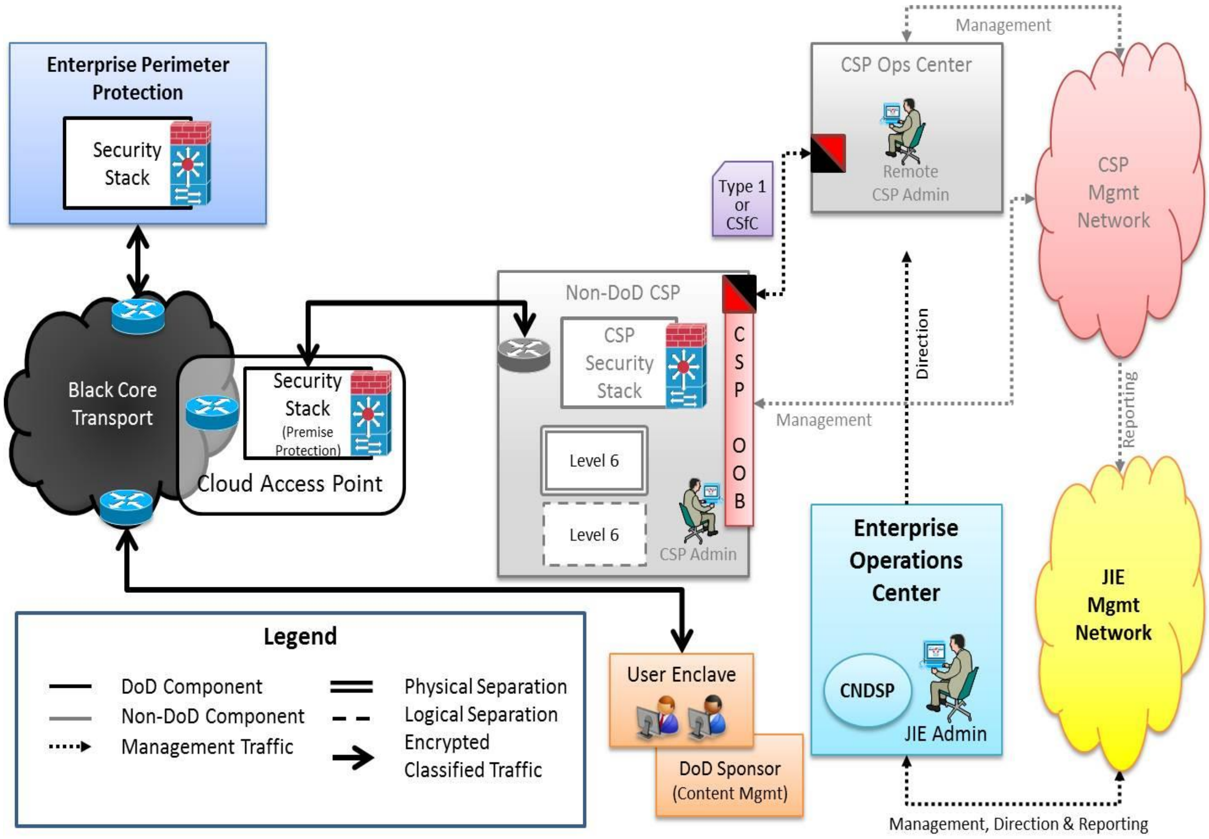


Figure 13: US Off-premises (non-DoD) Physical & Virtual separation between DoD/Fed GOV tenants

3.2.14. System View 2, Alternative Management Scenario 1 – Physical & Virtual separation between DoD/Fed GOV tenants; On-premises (DoD), 3-5 & 6 Off-premises (non-DoD), 1-2

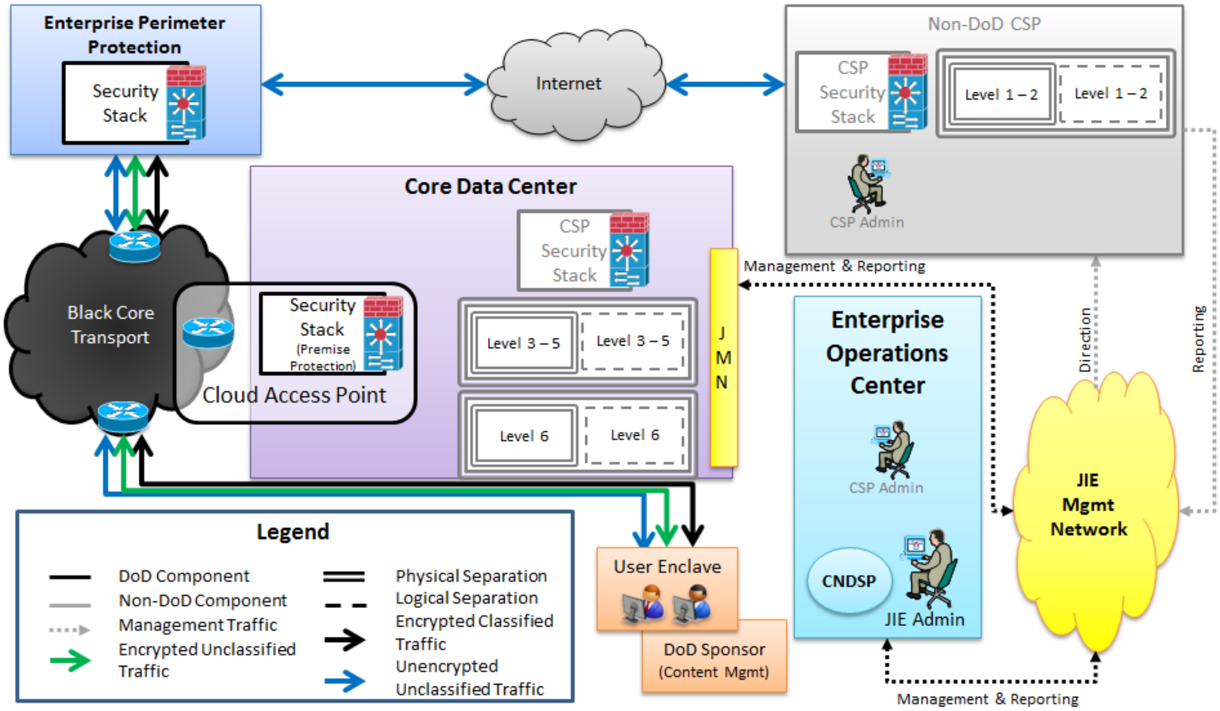


Figure 14: Physical & Virtual separation between DoD/Fed GOV tenants; On-premises (DoD), 3-5 & 6 Off-premises (non-DoD), 1-2

3.2.15. System View 2, Alternative Management Scenario 2 - Physical & Virtual separation between DoD/Fed GOV tenants: On-premises (DoD), 3-5 & 6; Off-premises (non-DoD), 1-2 & 3-5

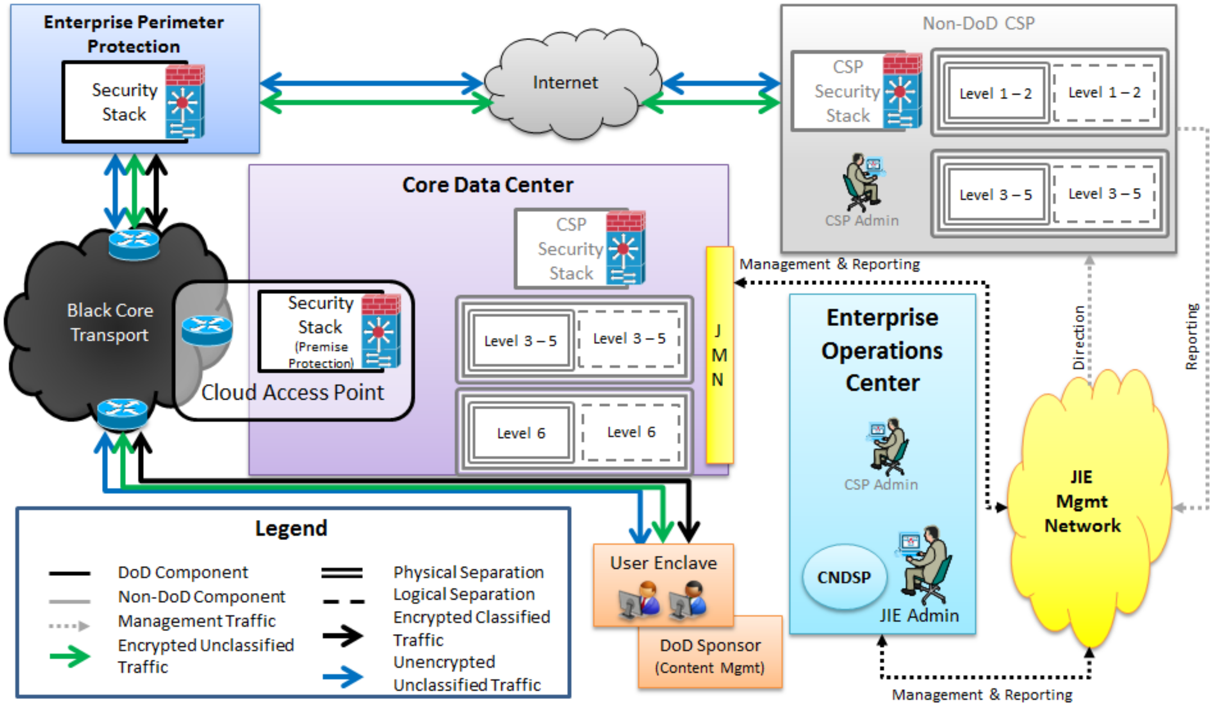


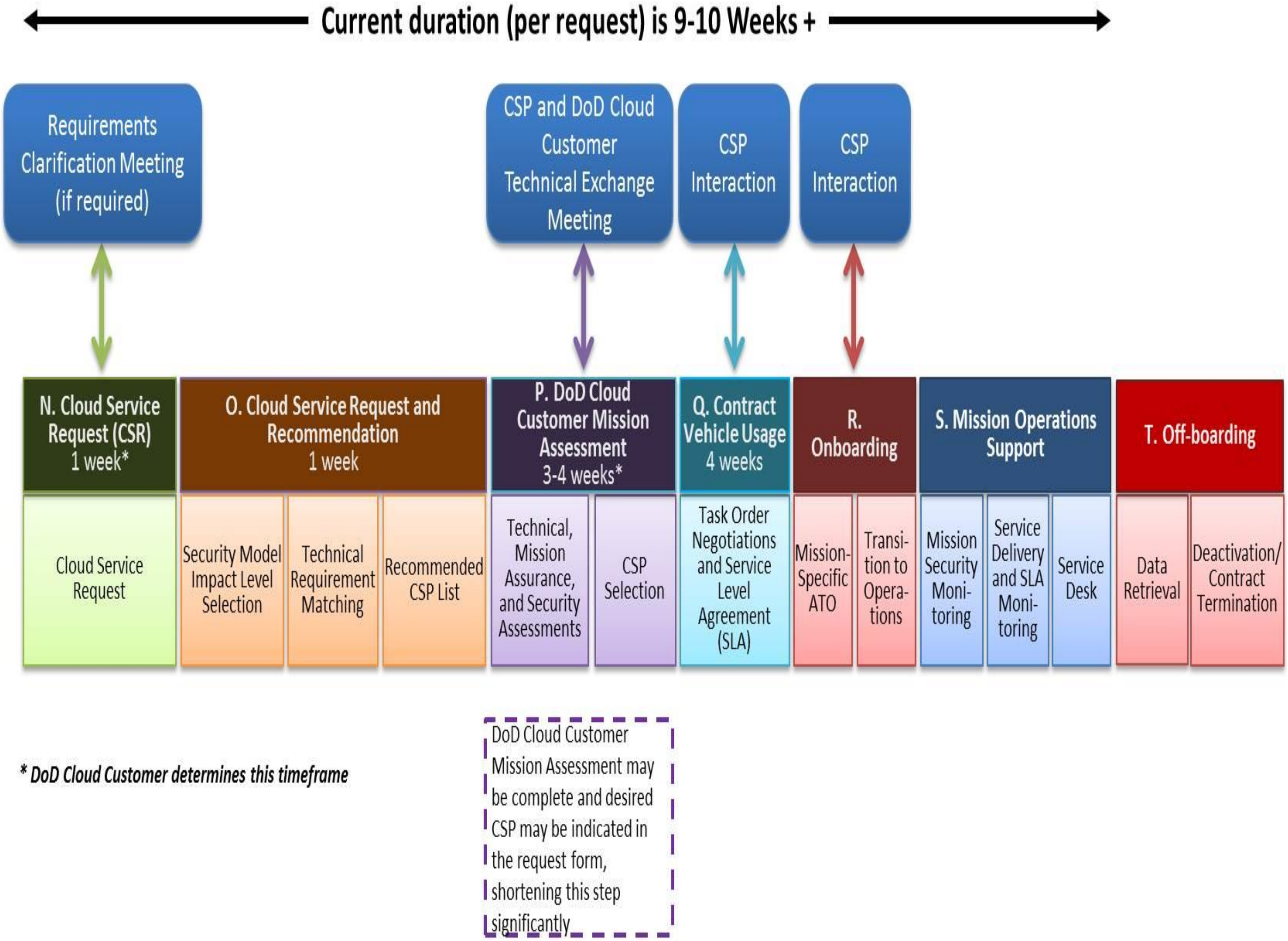
Figure 15: Physical & Virtual separation between DoD/Fed GOV tenants: On-premises (DoD), 3-5 & 6; Off-premises (non-DoD), 1-2 & 3-5

Approved for Public Release

4. Guidance to DoD Cloud Customer

4.1. DoD Cloud Customer Workflow

Figure 16 provides a high-level view of the workflow and processes for technical, mission security requirements, selection, on-boarding and mission operation support for CSPs supporting missions. Timelines shown are notional and dependent on the security status of the CSP and cloud readiness of the DoD mission. Additional detailed information for specific workflow steps and processes can be found in the ECSB Process Guide [8].



Current duration (per request) is 9-10 Weeks +

Requirements Clarification Meeting (if required)

CSP and DoD Cloud Customer Technical Exchange Meeting

CSP Interaction

CSP Interaction

N. Cloud Service Request (CSR) 1 week*
- Cloud Service Request

O. Cloud Service Request and Recommendation 1 week
- Security Model Impact Level Selection
- Technical Requirement Matching
- Recommended CSP List

P. DoD Cloud Customer Mission Assessment 3-4 weeks*
- Technical, Mission Assurance, and Security Assessments
- CSP Selection

Q. Contract Vehicle Usage 4 weeks
- Task Order Negotiations and Service Level Agreement (SLA)

R. Onboarding
- Mission-Specific ATO
- Transition to Operations

S. Mission Operations Support
- Mission Security Monitoring
- Service Delivery and SLA Monitoring
- Service Desk

T. Off-boarding
- Data Retrieval
- Deactivation/ Contract Termination

** DoD Cloud Customer determines this timeframe*

DoD Cloud Customer Mission Assessment may be complete and desired CSP may be indicated in the request form, shortening this step significantly

Figure 16: DoD Cloud Customer Workflow

Block N: DoD Cloud Customers must submit a Cloud Service Request (CSR) and work with the ECSB team as needed to clarify the request. CSRs are submitted through the DISA Cloud Service Request web form [9]. In accordance with the DoD Risk Management Framework [10], DoD Cloud Customers, with support from their Authorizing Official (AO), will categorize their systems in accordance with CNSSI 1253. This categorization produces impacts (Low, Moderate, or High) resulting from loss of confidentiality, integrity, and availability if a security breach occurs. This information is used to map the DoD Cloud Customer's requirements to an appropriate CSM Level.

Block O: The ECSB will review the DoD Cloud Customer's Cloud Service Request to assess the security and technical aspects of the request, and make recommendations about which CSPs meet the requirements.

The ECSB recommends an impact level that best fits the mission. Recommendations are based on:

- Type of data
- Adverse impact of unauthorized disclosure, modification, or destruction of data/application
- Mission Impact

The ECSB will analyze the technical requirements specified in the Cloud Service Request. Initially, the analysis process is manual; eventually, an online tool will support this process.

The ECSB will prepare a list of the candidate Cloud Service Providers that satisfy the DoD Cloud Customer's requirements.

If a DoD Cloud Customer is unable to find a cloud service that meets its needs from the list of candidates provided by the ECSB, the DoD Cloud Customer can either sponsor a new container for admission into the ECSB Cloud Service Catalog or apply for a waiver to use a cloud service outside the ECSB Cloud Service Catalog. The waiver process is discussed in Section 4.3. DoD Cloud Customers who receive a waiver will inform the ECSB of their final CSP selection so that the ECSB can track overall DoD use of cloud services. To sponsor a new container, the DoD Cloud Customer must submit a CSR that indicates it wishes to sponsor a specific cloud service for inclusion in the ECSB Cloud Service Catalog. The DoD Cloud Customer must agree to fulfill responsibilities as a DoD Cloud Sponsor, including providing a contracting vehicle for the new cloud service. The new CSP would then begin the process outlined in Figure 1.

Block P: The DoD Cloud Customer will review the ECSB's recommendations and evaluate the candidate CSPs. DoD Cloud Customers will leverage ECSB security assessments and focus on mission-specific risk determination. The DoD Cloud Customer remains responsible for the risk posture of the system. The CSP is required to undergo periodic re-evaluation of its security posture to continue to support DoD missions. DoD Cloud Customer's AOs are responsible for granting mission ATO for each mission system utilizing an authorized container.

The DoD Cloud Customer will clarify capacity requirements and service design through performance parameters in preparation for defining the configuration(s) of the services to be provided and for developing a service level agreement. The DoD Cloud Customer may discuss detailed mission requirements with one or more candidate Cloud Service Providers from the CSP List to understand the details of the service the CSP offers and how that service could support mission requirements, and at what cost. Performance parameters may include:

- Usage or budget quota
- Configuration options (e.g., operating system, storage min/max)
- Response time for scaling service up or down
- Identity management and access control
- Data handling
- Availability

- Other

The DoD Cloud Customer will identify the CSP chosen to support their Cloud Service Request and notify the ECSB.

Block Q: The DoD Cloud Customer, utilizing the existing contract with the CSP, negotiates a task order to provide services. The DoD Cloud Customer establishes the mission- specific SLA directly with the CSP. Situational awareness, continuous monitoring reporting, incident handling, and service help desk responsibilities depend upon the type of service, the entity serving as CSP, and the Mission Impact levels (1-6). These responsibilities are reflected in the Service Level Agreement.

Block R: The DoD Cloud Customer and CSP will work together to establish operational capability. The ECSB Service Operations Team may assist as necessary. Steps will vary depending on the nature of the cloud service, but may include:

- Establish connectivity
- Migrate data and/or applications to the CSP
- Identify users and manage user access
- Identify user access devices and manage user access devices
- Test
- Monitor and report results
- Confirm readiness to operate (Operational Readiness Review)
- Service activation
- Off-board service (transition out of operation; deactivation)

Block S: The DoD Cloud customer and the CSP will support mission operations. The CSP will continuously monitor their cloud service offering to detect changes in the security posture of the system. The CSP will provide reports to the DoD Cloud Customer and to the ECSB. The ECSB may provide security analysis information to the DoD Cloud Customer. For some systems, the DoD Cloud Customer will also monitor for security issues. This effort may utilize information provided by the CSP and the ECSB but may also involve information collected independently by the DoD Cloud Customer.

The CSP will collect and provide metrics related to performance and operations that can be used to assess performance relative to a particular service level agreement. The ECSB will monitor health and status, performance and operational metrics. Periodically the ECSB will ask the DoD Cloud Customer to rate the service they are receiving from the CSP.

In general the service desk function is a shared function between operational organizations from the CSP, the DoD Cloud Customer, and the ECSB. Depending on the type of service being acquired from the CSP and the impact level of the mission, the DoD Cloud Customer may be able to choose from different levels (or tiers) of service desk support.

Block T: DoD Missions will continue to operate within a CSP container until contract termination or shutdown of a service by the CSP. DoD Cloud Customers are responsible for the off boarding of the DoD mission(s) affected, to include retrieval/recovery of all mission data. A DoD Cloud Customer who is using the service that is being deactivated may want to shift to a different CSP. Activities to accomplish that will involve a subset of the DoD Cloud Customer Process.

4.2. System Categorization Process

The CSM impact levels were developed to integrate with the DoD RMF Authorization Process that all DoD entities must follow. As part of Step 1 of this process, DoD Cloud Customers must categorize their missions. Categorization incorporates aspects of both the information system and data in determining low, moderate, or high values for confidentiality, integrity, and availability. The assigned confidentiality and integrity values for a mission inform the process DoD Cloud Customers use to find a corresponding impact level. In addition to confidentiality and integrity levels, each impact level also has a set of associated data and mission types. Data and mission characteristics for each impact level are as follows:

Level 1: Public information or data. Non-NSS only.

Level 2: All FOIA releasable data, information open to the public even if it requires a login, low risk, non-sensitive PII (name, business or personal address, phone, and email). Non-NSS only.

Level 3: Non-Appropriated Fund (NAF) data that does not include health or legal data, and educational systems that fall under The Family Educational Rights and Privacy Act (FERPA), contracting data that does not contain Trade Secrets Act information. Non-NSS only.

Level 4: Moderate level PII (social security numbers, alien ID and other immigration documents, passport numbers, driver's license numbers, VIN numbers, and license plates), Trade Secrets Act data, and sensitive PII (medical/HIPAA, personnel, legal, law enforcement, and biometric data). Non-NSS only.

Level 5: Mission essential, critical infrastructure (military or civilian), deployment and troop movement, ITAR data, unclassified nuclear data. NSS.

Level 6: Classified, up to and including SECRET. NSS.

4.2.1.Mission Impact

In addition to the characterization of data within the 6 levels of the cloud security model, the impact of a particular mission or business function on the overall mission of the Department is another factor that can influence the risk management process.

The overall mission of the Department of Defense is to provide the military forces needed to deter war and to protect the security of our country. The following Mission Impacts are defined relative to the DoD's overall mission.

Mission Impact - High
A compromised mission is expected to have a high impact on DoD's overall mission to deter war and protect the security of our country e.g., DoD missions and operations continue under any cyber situation or condition.

Mission Impact - Moderate
A compromised mission is expected to have a moderate impact on DoD's overall mission to deter war and protect the security of our country.

Mission Impact - Low
A compromised mission is expected to have a low impact on DoD's overall mission to deter war and protect the security of our country.

Figure 17 below presents a notional example of mapping systems to a matrix that incorporates both the CSM data impact levels and the DoD Mission Impact attribute.

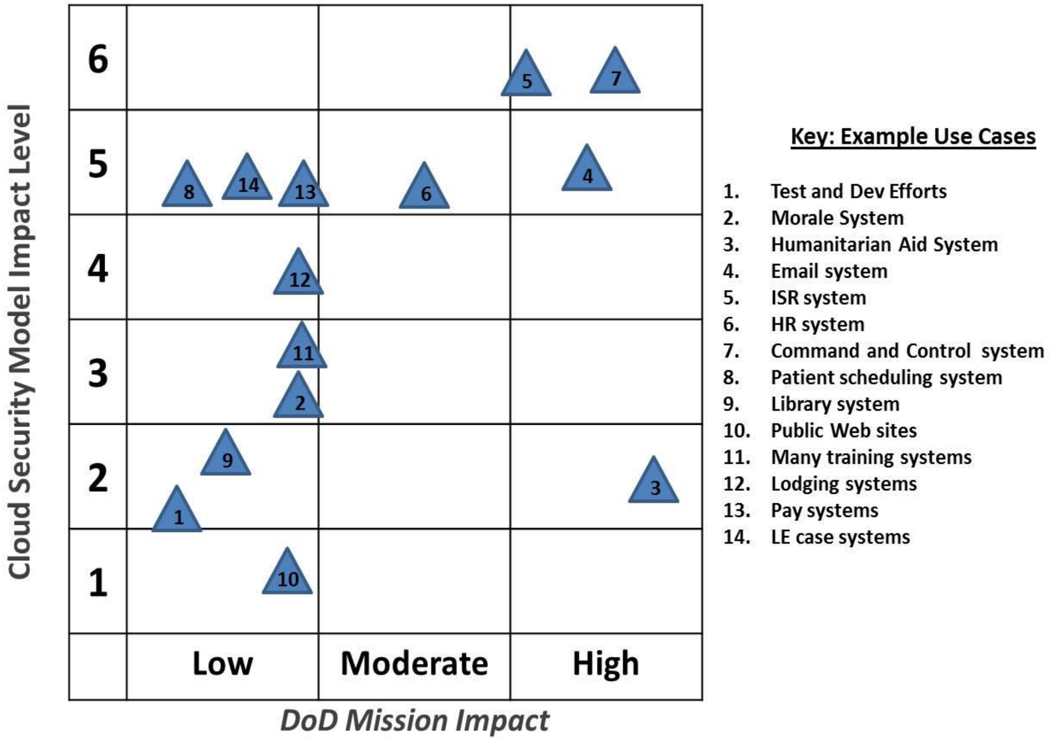


Figure 17: Notional Mapping of System to CSM Impact Levels

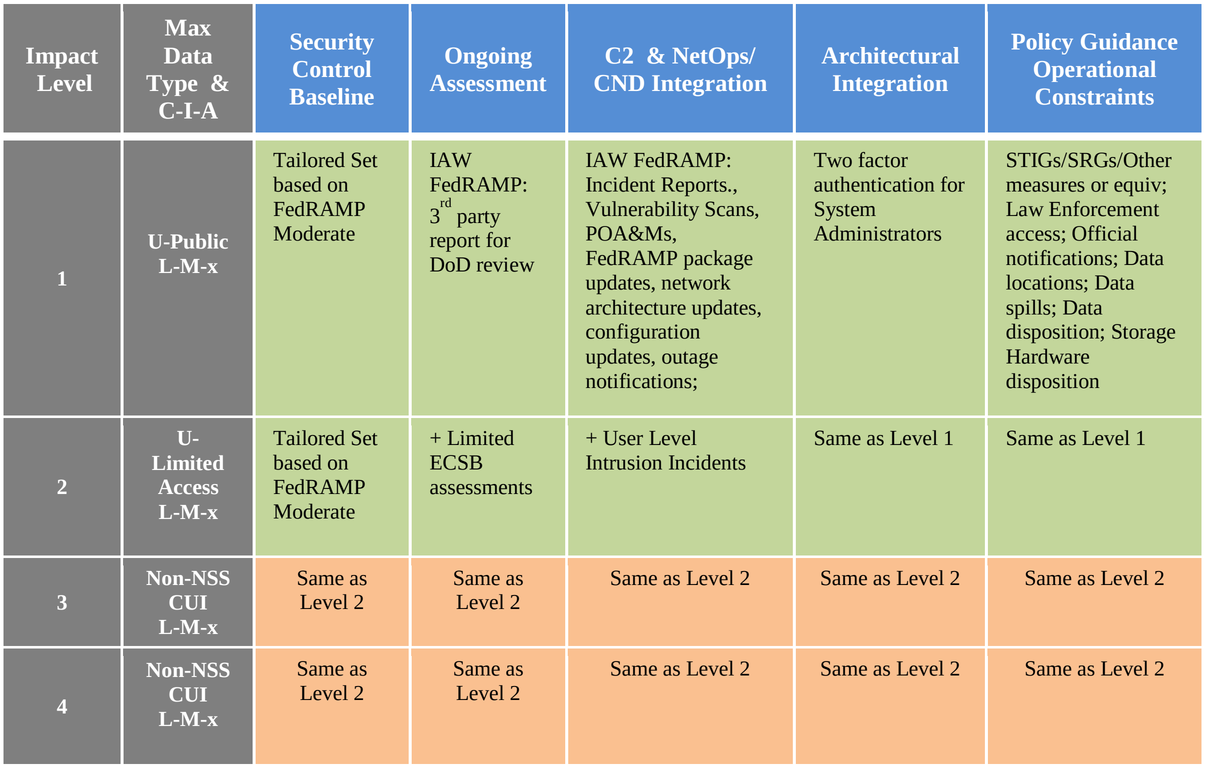
4.2.2.Reduced Requirements for Low-Impact Systems

In performing a system categorization IAW the DoD Risk Management Framework [10], the DoD Cloud Customer and AO identify the potential impact (Low, Moderate, or High) to their mission that would result from loss of confidentiality, integrity, and availability if a security breach occurs. However their individual mission or business process exists within the broader context of the overall DoD mission to deter war and protect national security.

While a particular system or set of data may be of moderate or high impact to the particular organization, their overall mission may be of low-impact to the Department's ability to deter war and protect the security of our country. For example, a student registrar system may be high impact with respect to the DoD Education Activity's ability to provide K-12 education; but K-12 education may be of low-impact to the Department's ability to deter war and protect national security.

The DoD Cloud Customer should work with its AO to determine if its particular mission qualifies for the reduced set of cybersecurity requirements specified for missions that have a low-impact on the overall DoD mission. The AO is responsible for the designation of these reduced Cyber Security requirement and associated increased Cyber Security.

The reduced set of cybersecurity requirements are identified in Figure 18, below. Note: Impact Level 5 (NSS) and 6 (Classified) are not applicable to Low-Impact systems and are not included in Figure 18.



Impact Level	Max Data Type & C-I-A	Security Control Baseline	Ongoing Assessment	C2 & NetOps/ CND Integration	Architectural Integration	Policy Guidance Operational Constraints
1	U-Public L-M-x	Tailored Set based on FedRAMP Moderate	IAW FedRAMP: 3rd party report for DoD review	IAW FedRAMP: Incident Reports., Vulnerability Scans, POA&Ms, FedRAMP package updates, network architecture updates, configuration updates, outage notifications;	Two factor authentication for System Administrators	STIGs/SRGs/Other measures or equiv; Law Enforcement access; Official notifications; Data locations; Data spills; Data disposition; Storage Hardware disposition
2	U-Limited Access L-M-x	Tailored Set based on FedRAMP Moderate	+ Limited ECSB assessments	+ User Level Intrusion Incidents	Same as Level 1	Same as Level 1
3	Non-NSS CUI L-M-x	Same as Level 2	Same as Level 2	Same as Level 2	Same as Level 2	Same as Level 2
4	Non-NSS CUI L-M-x	Same as Level 2	Same as Level 2	Same as Level 2	Same as Level 2	Same as Level 2

Figure 18: Cloud Security Requirements for Low-Impact Missions

4.3. Exceptions to Policy (Waiver) Process

If a DoD Mission has an urgent requirement that cannot be met by a DoD provisionally authorized cloud service offered in the ECSB Cloud Service Catalog, or has a compelling requirement for a new externally-provided cloud service for which it is impractical to obtain a PA, the DoD Cloud Customer must apply for a GIG Waiver using the GIG Waiver Process. A GIG Waiver is also required if the DoD Cloud Customer wants to use an approved cloud service at an Impact Level for which it has not been approved. This process may be utilized, for example, by a mission that needs to deploy low-sensitivity CUI to an Impact Level 2 service. The GIG Waiver Process steps follow:

a. Submit a GIG Waiver request through the appropriate DoD Component GIG Waiver representative, coordinated via the Broker, for an externally-provided cloud service in accordance with the GIG Waiver Process [11] for DSAWG and DISA Designated AO review.

b. The GIG Waiver Panel will hear arguments for and against granting a waiver, including assessments from the DISA Designated AO and the DSAWG.

c. The GIG Waiver Panel develops the recommendation to grant or deny the waiver for presentation to the DoD CIO for formal approval.

d. If approved, the DoD Cloud Customer's AO grants an ATO for use of the cloud service for the DoD Cloud Customer's mission. The DoD Cloud Customer's AO assumes the residual risk to the mission.

e. An approved GIG Waiver, granted by the DoD CIO through the GIG Waiver Process, is required for all deviations from DoD policy.

f. Current deployments of externally-provided cloud services that do not have an existing DoD PA, or an approved GIG Waiver, are required to submit a GIG Waiver request, coordinated via the Broker.

4.4. Command and Control/Network Operations (NetOps), Computer Network Defense (CND)/Incident Reporting, Threat Information Sharing

DoD-specific policy, guidance and operational constraints must be followed as appropriate by CSPs. The ECSB will evaluate equivalencies on a case by case basis.

- DoD Cloud Sponsor funds, acquires, and ensures Cybersecurity and contractual requirements have been met for externally provided cloud services within a CSP's container.
- DoD Cloud Customers are responsible for managing overall mission risk associated with hosting their data/services in cloud computing environments, and for attaining approvals from their Authorizing Official (AO) through the current DoD risk management process.

4.4.1.Threat Information Sharing

Threat information sharing between DoD entities and CSPs is accomplished through operational constructs defined within the Defense Industrial Base Cybersecurity and Information Assurance (DIB CS/IA) Program. Participation in DIB CS/IA is mandatory for CSPs in the ECSB Cloud Service Catalog at Impact Levels 3-6. Participation in the program enables CSPs to access DIBNet, the network used to share threat information and CYBERCOM notifications with CSPs, as well as report incidents to CNDSP Tier II. DIB CS/IA participation requires CSPs to sign an NDA to protect shared threat information [5].

CSPs must be able to receive, act upon and report compliance with warnings and notifications that are sent by CNDSP Tier II, as required by the FedRAMP Security Control Baseline. These notifications may be generated by CNDSP Tier I or II and may include guidance for or countermeasures to be taken by CSPs.

Implementation timelines for required actions communicated by the CNDSP Tier II, or threat-specific countermeasures will be specified in the terms/conditions/SLAs for the contract between a DoD Cloud Customer and the CSP.

4.4.2.DoD CNDSP and USCYBERCOM Incident Support

CNDSP Tiers I and II develop Information Requirements that identify the information necessary to accomplish their mission. In the course of performing CNDSP for their environments, CSPs will monitor their information systems to generate CND-relevant information, and report that information to the CNDSP. Transfer of relevant information from CSP to CNDSP Tier II is fulfilled by the CSP through following incident reporting guidelines. These guidelines, as well as incident categories and required reporting timelines incident categories and required reporting timelines from the CSP to CNDSP Tier II are described in the CSM.

CSPs will effectively function as CNDSP Tier III entities within the DoD structure. CSPs will provide local operational direction and support for CNDSP and will respond to direction from their designated CNDSP Tier II entity.

4.4.3. Incident Management and Response

The CNDSP Tier II entities will report incidents to USCYBERCOM as required. As the CNDSP Tier I, USCYBERCOM has visibility across all CNDSP Tier IIs, and may notify and coordinate among them as necessary. Those other CNDSP Tier II entities will, in turn, coordinate among their subscribers. USCYBERCOM will also be responsible for coordinating the DoD response with US-CERT and other entities, if that is warranted.

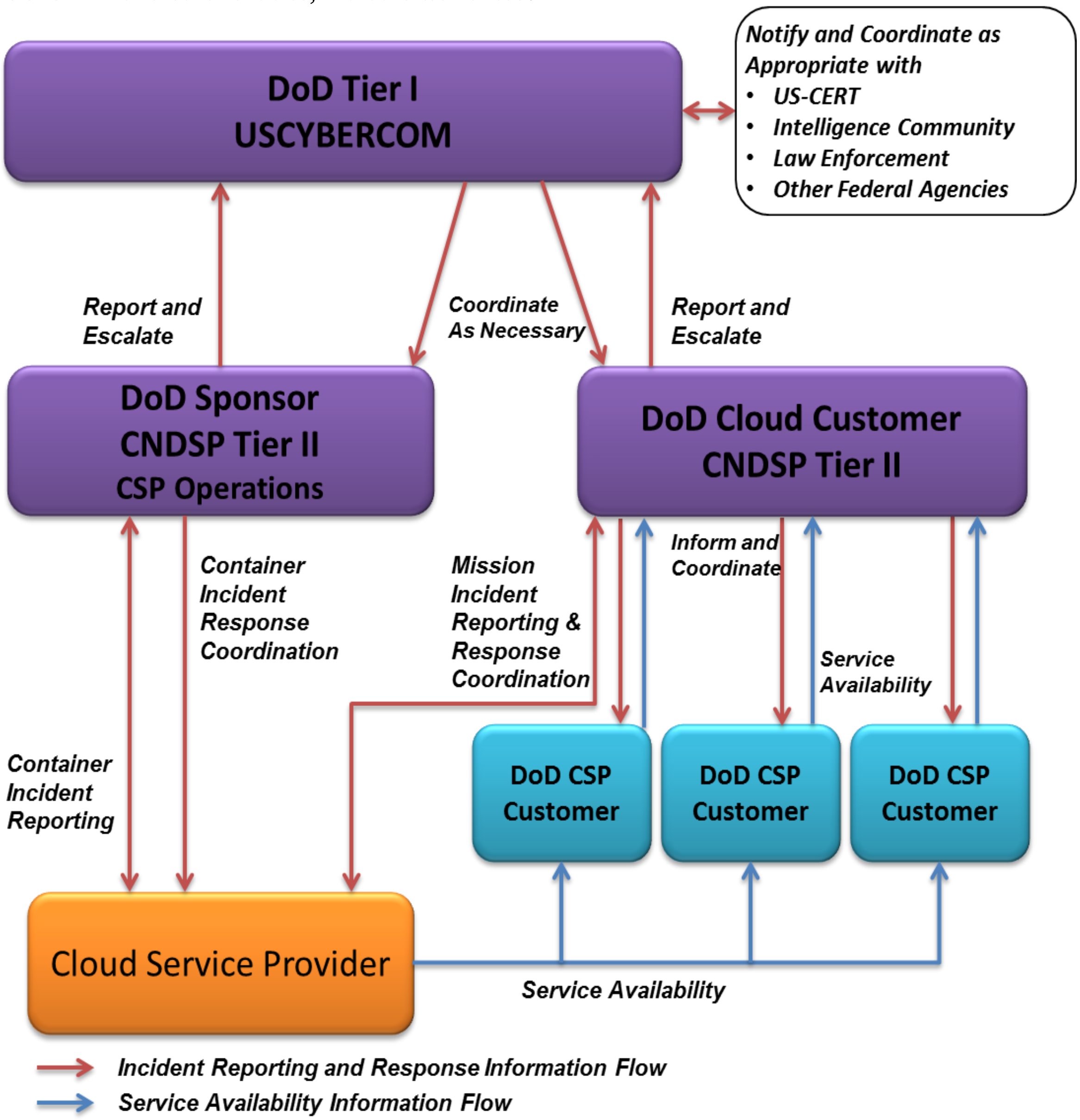


Figure 19 – DoD CNDSP Incident Reporting and Response Coordination

Approved for Public Release

5. Way Ahead

This section describes the legal policies and technical requirements that require continued action after the submission of this report. The Office of Primary Responsibility (OPR) for each activity is also identified. Although identified as the OPR, the organizations will require coordination and support from various other vested organizations.

5.1. ISRMC approval of changes to the CSM v2.1 derived from this report and summarized in Appendix A.
OPR: DISA

5.2. Work with the PAOs to identify sub-missions/systems within their mission area that may qualify as low-impact and the reduced security requirements. These systems would be initial targets for accelerated migration to CSP services.
OPR: DoD CIO

5.3. Synchronize JIE Single Security Architecture with new Cloud Security Architectures and submit for JIE approval. Cloud modifications to be inserted into Version 3 are currently in JSAP/Adjudication. Approval will be provided by the Enterprise Architecture and Engineering Panel and Enterprise Architecture Services Board.
OPR: NSA

5.4. Update DoD CIO Core Data Center Memorandum to recognize approved cloud services as appropriate destination in addition to CDCs.
OPR: DoD CIO

5.5. Issue policy allowing low-impact PII (i.e., business card information) to be maintained in Level 2 cloud services (currently, even low-impact PII is classified as CUI and would require Level 3 cloud services) Draft DoD CIO Memo to reflect change of Level 3 Data and new hosting options.
OPR: DoD CIO

5.6. Creation of a DoD specific categorization guide similar to that provided by NRO to assist DoD Cloud Customers in quickly selecting appropriate impact levels by system type.
OPR: DoD CIO

5.7. Reconcile the security levels represented in 8520.03 (Identity Authentication for Information Systems) with the CSM and update CSM or 8520 as appropriate. Include the results into an update of the CSM if required.
OPR: DoD CIO/DISA

5.8. Develop policy recommending that systems perform a risk assessment on their development and test systems to see if approved cloud services would be appropriate to support their dev/test activities. Dev/Test environments are typically 5-15 times larger than production environments, so migrating these to CSP may result in significant savings.
OPR: DoD CIO

5.9. Update CSM to reflect changes in this report and reflect updates from FedRAMP v2 (NIST SP 800-53 rev4) and 1253 v3 (NIST SP 800-53 rev4).

OPR: DISA

5.10. Revise draft DoDI for Acquisition of Externally-Provided Cloud Services to reflect the changes proposed in this report.
OPR: DoD CIO

5.11. Clarify/amend policy regarding resolving/redirecting .mil domains WRT DoD Instruction 8410.01, "Internet Domain Name Use and Approval," April 14, 2008. DoDI 8410.01 specifically states in section 4.d, "Not use .MIL domain names that redirect to non-.MIL domain named hosts (e.g., name.mil will not redirect to name.com)." This will hinder the push for moving outward facing websites to commercial CSPs. A risk assessment needs to be conducted prior to policy changes to ensure required changes do not create additional risk for the Department.
OPR: DoD CIO

5.12. Resolve acceptability of virtual separation with non-DoD tenants for impact Levels 3-5 (e.g., IG Act of 1978, or Fourth Amendment protections of data in public clouds). Requires addressing Legal/LE concerns, results from the NSA report on strength of virtual separation, potential creation of a virtual separation controls overlay and definition of cloud access point requirements.
OPR: DoD CIO

5.13. Update GIG Waiver Process documentation and GIG Connection Approval Process Guide to incorporate information and guidance on obtaining waivers for use of non-approved commercial cloud services.
OPR: DoD CIO

5.14. Develop plan and resource requirements to deliver enhanced cloud broker capabilities to support the adoption and use of approved commercial cloud services.
OPR: DISA

5.15. Develop additional guidance on the acquisition of commercial cloud services for DoD contract officers and acquisition professionals.
OPR: DoD CIO

5.16. Analyze the new set of controls resulting from the proposed changes to the CSM.
OPR: DoD CIO/DISA

5.17. Examine definitions of the CSM Impact Levels resulting from this effort and a controls analysis to collapse levels that no longer offer a distinct security difference (e.g., combine levels 1-2, combine levels 3-4).
OPR: DoD CIO/DISA

5.18. Define the cloud architect requirements and implementation plans to support Unified Capabilities and delivery of cloud-based office automation, email and collaboration services.
OPR: DoD CIO

5.19. Develop acquisition plan for DoD Cloud Sponsors to obtain cloud service from a CSP that is not is the ECSB Cloud Service Catalog.
OPR: DoD CIO/DISA

5.20. Address the requirements for support of multiple CNDSPs for different DoD Cloud Customers hosted at a single CSP. Characterize the CNDSP activities (levels of service required) based on the levels of data and type of service being provided e.g., IAAS, SAAS. Integrate results into an update of the CNDSP instruction.

OPR: DoD CIO/DISA

Appendix A - Summary of Changes

This appendix lists the proposed modifications from this effort to the current Cloud Security Model version 2.1. These recommended changes are based on guidance received from the DoD CIO indicating that the DoD was willing to accept additional risk to realize efficiencies and cost savings as part of DoD's move to cloud services.

1. Align Impact Levels 1 and 2 with FedRAMP Moderate

Modifying Impact Levels 1 and 2 to minimize requirements above those required by FedRAMP Moderate significantly reduces the effort required by CSPs to offer DoD services at these levels while aligning DoD with other federal government agencies for unclassified information. This modification proposes treating impact levels 1-2 as non-NSS. Impact level 1 changes from FedRAMP Low to Moderate, however, no CSPs to date have pursued authorization under FedRAMP Low and the increase in requirements from FedRAMP Low are offset by the removal of NSS controls.

2. Modify Impact Levels 3 and 4 to Accommodate Non-NSS CUI

Current policy to treat all systems as NSS is intended to protect NSS from attacks utilizing resources shared with non-NSS. However, the segmentation of resources provided by the CSM impact levels mitigates the risk posed from such attacks and presents an opportunity to protect non-NSS with more appropriate baselines of security controls. This change attempts to exploit this opportunity by dedicating two impact levels for non-NSS with CUI. The modified impact levels 3 and 4 are designed to provide low and moderate confidentiality options for non-NSS.

3. Modify Security Control Baselines for Impact Levels 5 and 6 from High-High to Moderate-Moderate

Feedback from version 2.1 of the CSM indicated that the High-High baseline for impact levels 5-6 exceeds the requirements of the vast majority of fielded DoD systems. Changing the control baselines to Moderate-Moderate better aligns with the expected needs of DoD missions and significantly lowers the number of security requirements CSPs would have to meet. DoD Cloud Customers will still have the option to negotiate additional security controls directly with CSPs if required.

4. Permit Non-DoD US Federal Government Tenants in Impact Level 3-6 Cloud Services

Version 2.1 of the CSM limits impact level 3-6 cloud services exclusively to DoD tenants. As part of the 45-day effort, changing this to permit public cloud services at levels 3-5 was investigated. However, legal opinions that the 4th Amendment would prevent the DoD from storing CUI data in public clouds precluded this option. Further research into possible ways to permit use of shared clouds at these impact levels without violating the 4th Amendment is recommended as part of the way ahead and discussed in Section 5.12 of this document.

However, a change that circumvents this legal issue is proposed in this document to open impact levels 3-6 to other US federal government agencies. This represents an option less restrictive than version 2.1 of the CSM that would lower costs for the DoD while avoiding 4th Amendment issues. Impact level 6 would be limited to other federal agencies that process classified information at SECRET or above.

5. ISRMC approval of reduced cybersecurity requirements for low-impact systems

This document introduces the concept of “Mission Impact” as a categorization tool. Systems determined to be “low-impact” are proposed as candidates for a reduced-set of security requirements. The ISRMC would need to approve this concept.

Appendix B - References

[1] Enterprise Cloud Service Broker (ECSB) Cloud Security Model (CSM), Version 2.1
http://iase.disa.mil/cloud_security/index.html

[2] Enterprise Cloud Service Broker (ECSB) Cloud Service Catalog
http://disa.mil/Services/DoD-Cloud-Broker

[3] Federal Business Opportunities webpage
www.fedbizopps.gov

[4] FedRAMP CONOPS and Continuous Monitoring Strategy Guide
http://cloud.cio.gov/document/continuous-monitoring-strategy-guide

[5] Defense Industrial Base Cybersecurity and Information Assurance (DIB CS/IA) Program
http://dibnet.dod.mil/staticweb/index.html

[6] Information Assurance Support Environment: External and Federal PKI Interoperability
http://iase.disa.mil/pki-pke/interoperability/

[7] FedRAMP Homepage
http://cloud.cio.gov

[8] ECSB Process Guide: not yet to be approved.

[9] DISA Cloud Service Request form
http://www.disa.mil/Services/DoD-Cloud-Broker/Cloud-Service-Request

[10] DoDI 8510.01: DoD Risk Management Framework

[11] GIG Waiver Process
http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide/Service-Appendices/OSD-GIG-Waiver-Process