Department of Defense

Cybersecurity
Test and Evaluation Guidebook
Addendum

Cybersecurity Test and Evaluation of Department of Defense Systems Hosted on Commercial Cloud Service Offerings

December 2019

Version 1.0

REVISION HISTORY

Version	Date	Changes	Revised By
1.0	12/4/2019	Initial release	OUSD(R&E) D(DT&E)

Table of Contents

List of Figures

List of Tables

1 Introduction

The purpose of this addendum to the Department of Defense (DoD) Cybersecurity Test and Evaluation (T&E) Guidebook (hereafter referred to as “the Guidebook”) is to provide additional considerations for cybersecurity T&E of DoD systems hosted in the commercial cloud. The addendum is a cloud-specific supplement to the six phases of cybersecurity T&E described in the Guidebook.

The addendum does not describe how to conduct cybersecurity T&E of commercial cloud systems. In addition to those items already described in the Guidebook, the addendum discusses new considerations such as contracting, system documentation, test environments, and the diverse and complex shared cybersecurity approaches for cloud systems. The addendum supports developing T&E strategies that are tailored to each DoD system in a commercial cloud.

The Chief Developmental Tester (CDT), Operational Test Agency (OTA) and Cyber Working Group (CyWG) for a DoD acquisition program deploying in a commercial cloud environment should implement the phases of cybersecurity T&E and supplement with the additional considerations from this addendum. The term “CDT”, which is used throughout this addendum, applies only to Major Defense Acquisition Programs (MDAP) and Major Automated Information Systems (MAIS). For non-MDAP/MAIS systems, replace “CDT” with the individual within the Program Management Office (PMO) who is assigned the roles and responsibilities associated with developmental testing.

This addendum advocates for the CDT and OTA to ensure cybersecurity T&E contract language is included in all commercial cloud Requests for Proposal (RFPs), or other requests for services. The Defense Acquisition University (DAU) DoD Cloud Computing Acquisition Guidebook provides examples of contractual language applicable to cloud-hosted information technology (IT) systems contracted under the DoD. The addendum seeks to heighten understanding of the fundamental differences between cybersecurity T&E in cloud versus non-cloud environments to ensure early planning and analysis for cybersecurity T&E is performed.

Commercial cloud service providers (CSPs) provide computing capabilities through cloud service offerings (CSOs). The scope of cloud-hosted DoD system cybersecurity testing should include CSOs, supporting infrastructure, and the interfacing infrastructure for networks physically or logically connecting to the end user. All people, processes and tools involved from the Department of Defense Information Network (DoDIN) to the end user and associated interfaces should be tested in Phases 3 through 6. This addendum uses the terms “cloud-hosted DoD system”, “system”, and “System Under Test (SUT)” interchangeably.

This addendum contains the following additional sections:

- Section 2 provides general cybersecurity T&E considerations for cloud-hosted DoD systems.
- Section 3 provides cybersecurity T&E considerations for cloud-hosted DoD systems specific to each of the six phases defined in the Guidebook.
- Section 4 provides a brief overview on cloud deployment models, DoDIN architecture interfacing with cloud systems, roles and responsibilities as well as documents for T&E planning.
- Section 6 provides a Glossary of Terms and an Acronym List.
- Section 7 provides a list of References.

2 Cloud Cybersecurity T&E Considerations

This section discusses cybersecurity T&E considerations that are unique to cloud-hosted DoD systems, and may not be comprehensive. As explained in the DoD Cloud Acquisition Guidebook, an "important cybersecurity fact is for DoD acquisition professionals to clearly understand that (Cyber) Security in the Cloud is a shared responsibility between the cloud service provider and the mission owner." The mission owner is the DoD Services/Component and their sub-components that use CSOs, for example, the "cloud customer" or CSP's customer.

2.1 Cloud Services and Shared Responsibilities

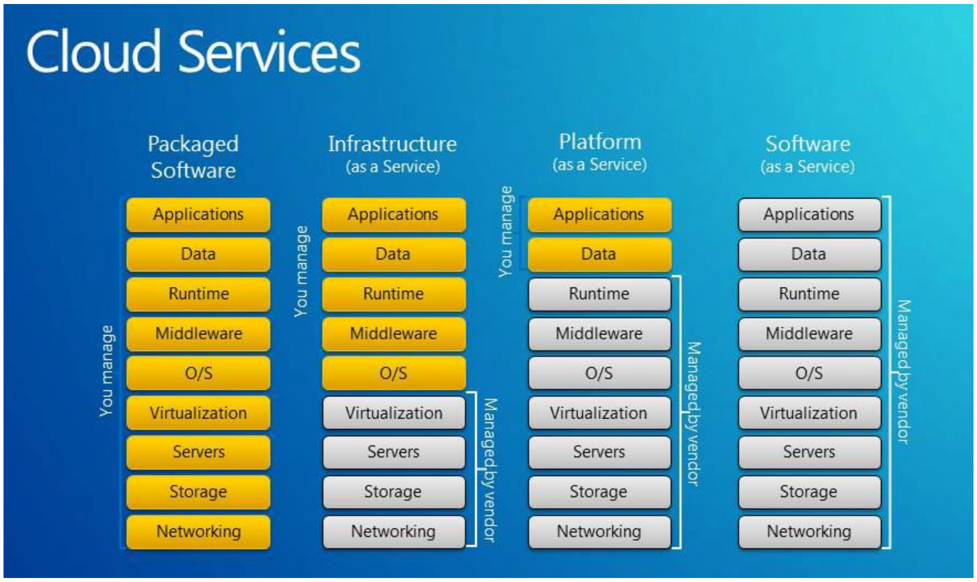


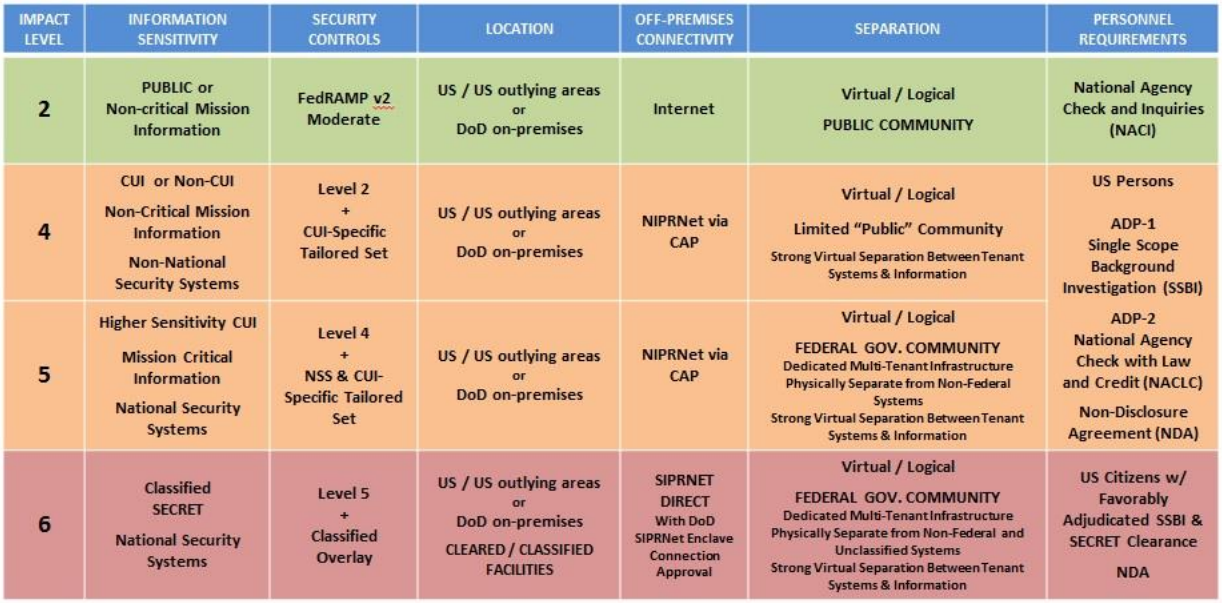
Figure 1. Cloud Service Models

The National Institute of Standards (NIST) defines three types of CSOs under the cloud service model: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Figure 1 shows the multiple stacks of cloud capability in a CSO and the typical division of responsibility for managing the capability between the CSP (vendor) and the DoD program for each type of cloud service. While these are the standard recognized services, hybrid modifications of the model may be designed for specific DoD acquisition programs.

2.1.1 FedRAMP+

A CSP must be authorized to provide services to the federal government through a program called Federal Risk and Authorization Management Program (FedRAMP). One element of FedRAMP is the granting of Provisional Authority to Operate (P-ATO) for a CSO. P-ATO maintenance involves periodic reassessments by an accredited Third Party Assessment Organization (3PAO). CSPs offering CSOs to DoD must adhere to FedRAMP requirements for the relevant Impact Levels (ILs) (Table 1). The CSP must follow additional steps and implement more controls to provide services to DoD organizations for data at ILs above Level 2. This is called FedRAMP+. The Defense Information Systems Agency (DISA) Authorizing Official (AO) issues Provisional Authorizations (PAs) to CSOs that meet FedRAMP+ requirements.

Table 1. Cloud Information Impact Levels



IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

The FedRAMP+ process serves as the minimum security baseline for all DoD cloud services. The CDT and OTA should understand that FedRAMP+ and PAs are considered necessary but not sufficient for evaluating the shared responsibilities of CSPs and DoD programs deploying to the commercial cloud.

The CSPs, 3PAOs and DISA develop and maintain artifacts and test results as part of the PA process (Section 4).

2.1.2 Cybersecurity "Of the Cloud" and "In the Cloud"

The CSP's role in providing the cloud environment, including the infrastructure and virtualization layers, gives the CSP primary responsibility for cybersecurity of the cloud. FedRAMP+/3PAO activities only assess cybersecurity of the cloud for that specific CSO and cannot replace the need for comprehensive cybersecurity T&E which DoD requires to evaluate the effectiveness of cybersecurity in the cloud.

Although the CSO PA provides inherited security assessments under DoD Risk Management Framework (RMF), the DoD Program Management Office (PMO) is responsible for the DoD implementation of security configurations within the CSO. This includes planning and implementing cybersecurity, survivability, and resilience in the cloud, as well as selecting and implementing additional RMF controls that apply to the DoD system or are shared with the CSO. The cloud service model determines generally which areas of the CSO the PMO is responsible for securing in addition to the system under test. The cloud deployment model—private, community, public, or hybrid—determines how much of the underlying cloud infrastructure is dedicated for DoD use and is under direct DoD management. Full system testing includes testing cybersecurity of and in the cloud especially at the "seams" of responsibility to evaluate the security, survivability and resilience through supporting infrastructure, and across interfaces, down to the end user. The testing is not a reassessment of FedRAMP+ controls, but of the actual defensive capabilities for the system.

2.1.3 Shared Responsibilities for Security

A significant difference between a traditional DoD data center-based information system and cloud-based system is security responsibility sharing. The responsibility for cybersecurity in cloud-hosted DoD systems is shared among DoD Cybersecurity Service Providers (CSSPs), the mission owner, the PMO, and the CSP. Each are responsible for configuring and defending different portions of the overall cloud environment.

Roles and responsibilities should be clearly described in the contract and Service Level Agreements (SLAs) with the CSP and the IT operations and support (O&S) personnel, as well as in the Memorandum of Agreement (MOA) with DoD CSSP(s). Often, the mission owner is responsible for authorizing new users and roles, requesting configuration changes and monitoring the DoD service. These areas of responsibility shift depending on cloud service model and the portion under the CSP's operational control. The shift in security responsibilities should be important areas of focus for DoD testing moving forward.

During developmental test and evaluation (DT&E), the CDT should evaluate the coordination of cybersecurity operations among all entities supporting the DoD system: CSSP, mission owner, PMO, CSP, and the IT O&S personnel. While the OTA will evaluate this coordination as part of cybersecurity operational test and evaluation (OT&E), during DT&E, the CDT should understand and evaluate the technical tools, people, and processes needed to make this coordination work in support of fixing any identified issues prior to OT&E.

In preparation for cybersecurity T&E as an iteration of Phase 1 post contract award, the CDT and OTA should review MOAs with the DoD CSSP(s), IT O&S roles and responsibilities for all entities, and CSP SLAs. The CDT and OTA should also work with the PMO to understand gaps and deficiencies in these roles and responsibilities prior to these agreements/contracts being approved.

2.2 Support to DoD Cybersecurity T&E

To plan for and conduct adequate cybersecurity T&E under the shared responsibility construct, the CDT and OTA will need support from various entities. The following sub-sections identify these entities and provide guidance on obtaining this support.

CSP Support:

The CDT and OTA will need cybersecurity-related T&E support from the CSP documented in the RFP, the contract, and the SLA between the PMO and the CSP. The CSP should be contractually obligated to support cybersecurity T&E.

Examples of items the CDT and OTA should address when providing input to the RFP, contract, and SLA to facilitate CSP support to DoD T&E:

- CSO test environment integrates with representative DoDIN integration points and services to create an operationally realistic and operationally representative test environment.
- CSP supports DoD cybersecurity testing of external functions, interfaces, and integration points to the CSO, including the DoDIN integration points and services.
- CSO performance metrics to demonstrate the CSP is delivering the mission owner's cybersecurity, survivability and operational resilience capabilities.

- DoD oversight of cybersecurity testing in the CSO environment where other DoD programs are being implemented or developed.
- DoD evaluation of CSP, CSSP and O&S in execution of the shared responsibilities.
- DoD is granted physical and logical access to the CSO to conduct DoD cybersecurity T&E.
- DoD access to CSP technical support and documentation for DoD cybersecurity T&E activities, including participation in mission-based cyber risk assessments such as cyber table top exercises.
- DoD access to system logs, packet capture, and other CSO information to support problem resolution, test results, and test reporting.
- DoD access to FedRAMP+ and DoD PA-related artifacts.

CSSP Support: The PMO should include CSSP support for cybersecurity T&E in the CSSP MOA.

Other Support: Cybersecurity T&E for cloud-hosted DoD Systems requires testers who understand testing of, and in, commercial cloud environments. DoD cybersecurity T&E teams will additionally require support and participation from cloud architects, cloud security architects, 3PAOs, and the DISA cloud assessment team.

2.3 Test Environments for Cloud Cybersecurity Testing

The CDT and OTA should work in collaboration with the Mission Owner during Phases 1 and 2 to ensure that operationally realistic and operationally representative test environments are provisioned to support cybersecurity T&E.

Mission owners deploying systems into cloud environments may be using agile development methods and/or employing development security operations (DevSecOps) to develop and deploy software (Appendix C of the Guidebook, Version 2.0, Change 1). The Development, Test, and Pre-Production DevSecOps environments can be used to conduct cybersecurity testing. The CyWG should ensure they have identified the need for access to these environments, tools and products delivered for early phases of cybersecurity T&E.

If the PMO ensures the test environment fully replicates all architectural and operational aspects of the cloud environment, then cybersecurity T&E can include a full spectrum of verification, performance, and disruptive tests against the identical fully functional instantiation of that environment without scheduling constraints or fear of adverse effects to the development or production system.

The CyWG should identify test limitations and their associated risk early to the CDT and OTA to allow more time to mitigate the limitations and risks. For example, the contract may restrict or prohibit testing against layers provisioned, operated and sustained by the CSP. The CDT and OTA should evaluate 3PAO assessments to mitigate that limitation.

2.3.1 Cybersecurity T&E of Integration Points and Services

The CDT and OTA should include the cybersecurity aspects of integration points and services within the scope of their cybersecurity T&E planning, execution, and reporting. DISA is responsible for managing, and defending the primary DoDIN integration points and services. As

DoD migrates to commercial cloud, CSOs may need to interoperate with other DoD component systems either on an enduring basis or during the service transition period. Some DoD components use their own mid-point protection between the Defense Information Systems Network (DISN) and DoD component Base/Post/Camp/Station (B/P/C/S) networks instead of the DISA-provided mid-point protection capability known as the Joint Regional Security Stacks (JRSS).

Figure 2 shows examples of key architectural elements (red boxes) or integration points where interoperability and cybersecurity must be evaluated by the cybersecurity T&E testers, including Internet Access Points (IAPs), Cloud Access Points (CAPs), and Domain Name System (DNS) infrastructure. These elements are where the security responsibilities may be poorly defined or improperly understood. The CDT and OTA should plan to include all integration points into the test environment to ensure a comprehensive test infrastructure. Figure 2 shows examples of the key operational elements (red ovals), including the CSSP and the end users, that also should be incorporated into the test environment. The CyWG should identify, and document in appropriate artifacts, these essential architectural and operational elements during Phases 1 and 2 to ensure that operationally realistic and operationally relevant environments are available for later phases of cybersecurity T&E. Other elements in Figure 2 are discussed in section 4.

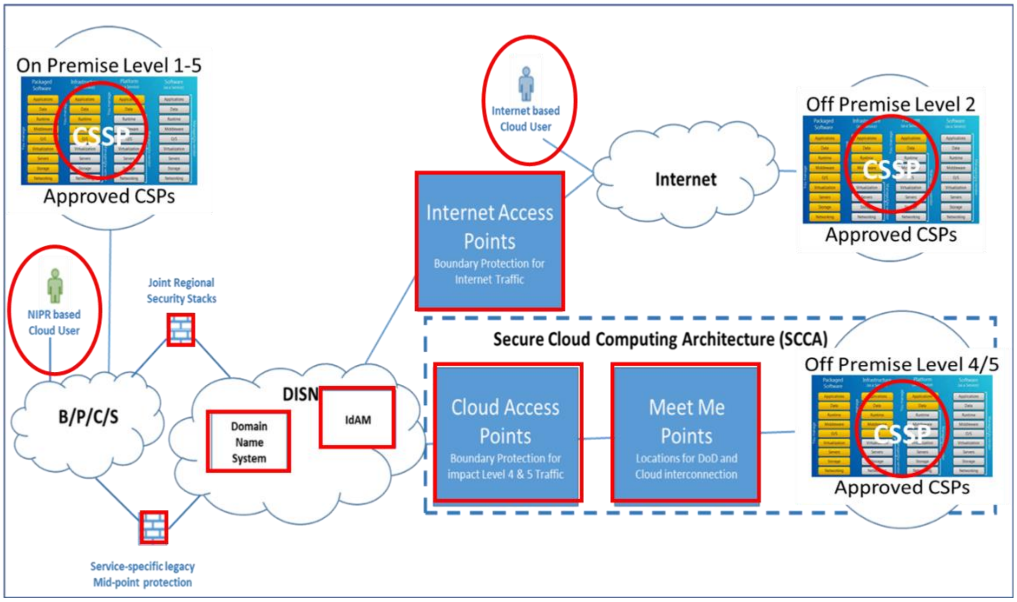

On Premise Level 1-5
CSSP
Approved CSPs
Internet based Cloud User
Internet
Off Premise Level 2
CSSP
Approved CSPs
Internet Access Points
Boundary Protection for Internet Traffic
NIPR based Cloud User
Joint Regional Security Stacks
Secure Cloud Computing Architecture (SCCA)
Off Premise Level 4/5
B/P/C/S
DISN
Domain Name System
IdAM
Cloud Access Points
Boundary Protection for impact Level 4 & 5 Traffic
Meet Me Points
Locations for DoD and Cloud interconnection
CSSP
Approved CSPs
Service-specific legacy Mid-point protection

Figure 2. Examples of Key Architectural and Operational Elements

2.4 Test Considerations by Cloud Service Model

Test scope is determined by the cloud service model used by the DoD System. Figure 3 illustrates how test scope changes based on the most common cloud service models. Cloud research has shown that most breaches are by caused by cloud security misconfiguration of the cloud service customer-provisioned services. Therefore, the scope of cybersecurity T&E should include configuration of all PMO-provisioned services.

For SaaS CSOs, testers should plan to test the CSO use of DoDIN integration points and services, data protections (such as access controls, use of encryption, etc.), and system recovery and availability of the provided SaaS applications as well as shared responsibilities for security.

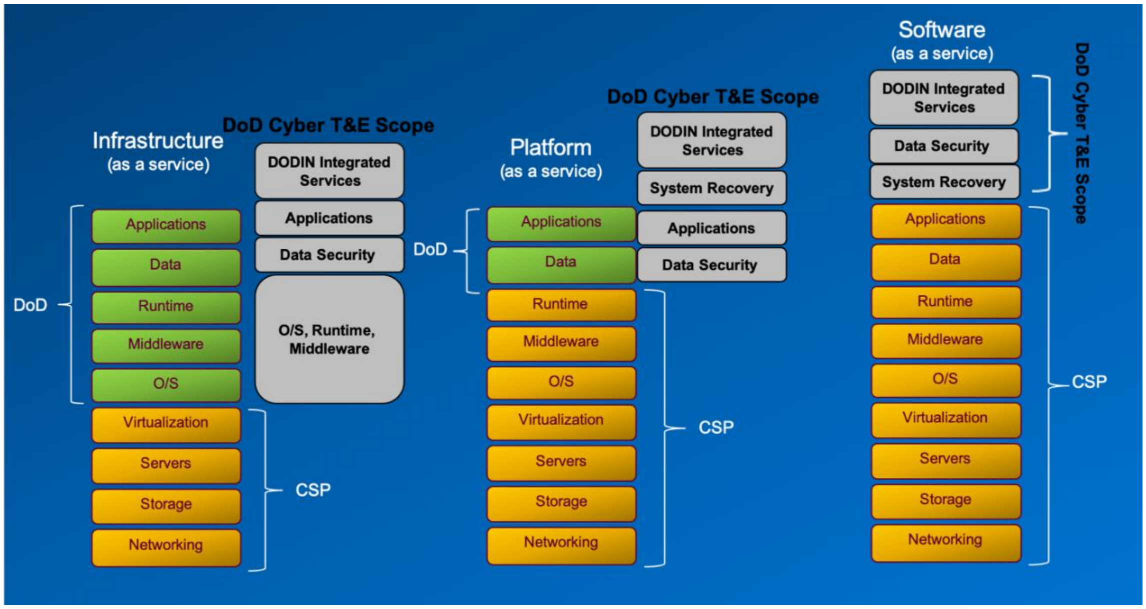


Figure 3. DoD Cybersecurity T&E Scope by Cloud Service Model Type

For IaaS and PaaS CSOs, the DoD System will use the CSO as a platform on which to operate a DoD application. The PMO is therefore responsible for testing the DoD application in addition to the data security provided by the DoD application and the use of the DoDIN integration points/services.

2.4.1 Infrastructure as a Service (IaaS)

IaaS delivers compute infrastructure as a service (typically a virtualized server environment), along with raw storage and networking capability.

The DoD PMO is responsible for IaaS implementations, and for providing the operating system and any runtime and middleware software needed to run DoD applications. CDT and OTAs and T&E leads should plan to test at the operating system and software middleware and runtime layers in addition to the DoD PMO application and development process, any DoDIN integration points, and Defensive Cybersecurity Operations (DCO) capabilities provided by the government and the CSP (if applicable).

2.4.2 Platform as a Service (PaaS)

PaaS CSOs allow the DoD PMO to replicate, scale, host, and secure consumer-created or acquired applications on the cloud infrastructure. The PaaS is often used to provide a development environment to support DevSecOps software factories, or application platforms such as databases, file storage and collaboration, or even proprietary application processing such as machine learning, big data processing, or direct Application Programming Interface (API) access to features of a full SaaS application.

For PaaS, the DoD PMO is responsible for any configuration and application software installation on top of the CSO. CDTs, OTAs, and T&E leads should plan to test the DoD application, development environments/software factories, data security, system recovery, and any DoDIN integration points and services.

2.4.3 Software as a Service (SaaS)

SaaS CSOs are the CSP's applications running on a cloud infrastructure managed and hosted by the CSP. The DoD user will typically access the applications with a web browser, mobile application, or a lightweight client app installed on their workstation. With a SaaS, DoD data is stored and maintained in a non-DoD-developed system. For IL4, IL5 and IL6 SaaS, the test scope should include the data security mechanisms implemented to protect DoD tenant data. CDTs, OTAs, and T&E leads should also plan to verify the application's operational resilience through testing consistent with the service contract as the application itself is not something that can be changed.

The test scope should include data on how long it take the application to be recovered in the event of a CSP system failure or network outage. Focused evaluation is needed of the portions of the CSO where the:

- PMO is responsible for configuring or customizing portions of the CSO, usually through a CSP-provided management API or web application.
- CSP and PMO security-related responsibilities are shared.
- CSO is dependent on government services, such as DoDIN integration point interfaces between the government networks and the CSP.

3 Cloud-related T&E Considerations by Guidebook Phase

The Guidebook defines six cybersecurity T&E phases as follows:

- Phase 1 – Understand the Cybersecurity Requirements
- Phase 2 – Characterize the Attack Surface
- Phase 3 – Cooperative Vulnerability Identification (CVI)
- Phase 4 – Adversarial Cybersecurity DT&E
- Phase 5 – Cooperative Vulnerability and Penetration Assessment (CVPA)
- Phase 6 – Adversarial Assessment

3.1 Phase 1 Considerations

The CyWG for a commercial cloud program should include cloud architects and engineers, cloud security architects, and cloud cyber testing personnel from the Lead Developmental Test Organization (LDTO) and OTA, or cloud cyber test contractors hired by the LDTO and the OTA. After contract award, the CSP should also be represented in the CyWG to help inform test planning and execution.

Early Phase 1 activities are necessary to ensure the RFP, contract, SLA, CSSP MOAs and other artifacts all capture the appropriate considerations for T&E.

After contract award, the CyWG should examine the relevant contracts, service agreements, system designs, and pre-existing test results and reports. These activities should be repeated iteratively by the CyWG prior to and during Phase 3 – 6 testing.

The CyWG should accomplish the following in Phase 1:

- Examine the previous test results to determine if and what additional testing may be needed to ensure end-to-end assessment of the system in the cloud. Doing so requires the following steps:
    - Understand the scope of testing already performed by reviewing the 3PAO’s SAP.
    - Review available test results such as the 3PAO’s Security Assessment Report (SAR).
    - Identify and proceed with any additional testing required.
- Understand all interfaces to other systems, including the DoD integration points and services.
- Review the PMO’s contract vehicle or SLA that describes cybersecurity roles and responsibilities, including test roles.
- Identify the CSO (IaaS/PaaS/SaaS), Cloud Deployment Model (public, private, community, hybrid), and the IL assigned to the CSO (Level 2, 4, 5, or 6).
- For IaaS/PaaS, review the Joint Enterprise Defense Infrastructure (JEDI) integration contract/task order to determine whether it covers T&E support and, if not, work with the PMO to bridge any gaps or at a minimum ensure that the risk is documented.

- Identify how CSO aligns with DoD Cloud Strategy (Section 1.3)-is it a JEDI IaaS/PaaS cloud, a custom general purpose cloud, or a new "fit-for-purpose" cloud?
- Obtain the preliminary design for the SUT, including touch points into CSO (interfaces, DoDIN integration points and services, and CSO-provided services such as data backup and storage).
- Determine which DoD integration points and services the CSO needs and which are relevant to security.
- Identify the CSP-provided system-level users of the SUT (such as administrators, help desk personnel, application administrators, etc.) and the types of cloud-based data each is authorized to view and modify.
- Conduct design reviews to understand the testability of the cloud-deployed application, data protections, and DoDIN integration points.
- Participate in design reviews to ensure cloud security engineering expertise is used to design cloud security controls.
- Ensure the PMO has contracted for DoD DCO support and understands what the CSP will provide to protect government data and detect data breaches.
- Request, obtain and review FedRAMP+ and PA artifacts to understand the cybersecurity capabilities the system will inherit when using the selected CSP. FedRAMP+ artifacts are discussed in Section 4.
- Determine any external DoD systems the CSO will need to interoperate with and which ones are relevant to security.
- Determine if the program is deploying a new application or development project in the cloud, or migrating an existing system to a CSO. The test scope may change for new application development, and migrating existing systems may involve testing of both the legacy and new application. Legacy and new applications may co-exist for a period of time.

3.2 Phase 2 Considerations

The CyWG should conduct attack surface analysis for cloud-hosted DoD systems that includes the CSO, and interfaces to DoDIN integration points/services and DoD Component systems (if applicable).

CDTs, OTAs, and T&E leads should consider the following cloud-hosted specific areas of focus for Phase 2 Cybersecurity DT&E of cloud-hosted DoD systems:

- Conduct cyber threat assessment and kill chain analysis for the government-controlled portions of the system and the portions provided by the CSO; include areas where configuration, hardening, monitoring, or response responsibilities overlap.
- Conduct attack surface analysis for interfaces (DoDIN integration points).
- Identify and analyze the attack surface: A pre-existing and/or pre-assessed CSO environment may have documented threats specific to that layer of the technical architecture, which the CyWG should use if it is available, and existing vulnerabilities and threat vectors should be well understood. Identify key cyber terrain or mission-relevant cyber terrain associated with critical mission functions.

- Consider that attack vectors for cloud-based services include exploits targeting misconfiguration of CSO security, remote access, architecture, and authentication services by the CSO customer.
- Examine CSO APIs used to integrate with DoDIN services which may expose customer configuration to vulnerabilities and threats.
- Plan to use the cloud CSO as a test instantiation to provide a robust test environment for adversarial DT&E as preparation for Phase 3 and Phase 4 cybersecurity DT&E events.
    - Develop a test environment strategy with the CSP.
    - For SaaS, understand the CSP infrastructure layers that will not be accessible to testers, and the types of tests that the CSP may not allow.

3.3 Phase 3 Considerations

When an IaaS or PaaS cloud service model is used, the PMO is responsible for the development and testing or an application that is hosted on the IaaS/PaaS CSO. Standard Phase 3 CVI as defined in the Guidebook should be followed for the portions of the CSO above the virtualization layer.

For Phase 3 cybersecurity T&E of cloud-hosted DoD systems, the following supplemental information should be considered:

- The 3PAO may perform the equivalent of CVI test activities for a CSO as part of the assessment “of the cloud” needed to obtain a PA (at the appropriate IL) or as part of subsequent periodic continuous monitoring assessments. The CDT and CyWG should review these artifacts to determine gaps on which to focus their CVI analysis.
- In addition to the standard tools and events used to perform CVI, the CSP can provide additional visibility into the CSO environment through native tools in the CSO as part of the service contract or through additional professional services. It may be possible to contract directly with the 3PAO who has access to test artifacts and specific CSO subject matter expertise during Phase 3 testing.
- Data to satisfy cloud cybersecurity test objectives may come from several sources. That data may be generated by a 3PAO, by the PMO for the cloud-hosted DoD system or by the cybersecurity T&E team responsible for conducting testing during Phase 3 and 4. Table 2 below lists generic cloud-related test objectives. This table is not necessarily comprehensive, nor required to be used. The test objectives are applicable to all Cloud Service Models.

Table 2. Example Generic Test Objectives

Test Objective	Treacherous 12 Security Threats (See References)
Verify mechanisms to ensure government data is protected from unauthorized disclosure and remains under government control	• Data breaches • Account hijacking • Insecure APIs • System and application vulnerabilities • Advanced persistent threats
Verify access control and identity management and all DoDIN integration points	• Account hijacking • Weak identity, credential and access management • Insecure APIs

Test Objective	Treacherous 12 Security Threats (See References)
Verify remote administration and management of services, configurations, and other consumer-defined service items	• Account hijacking • Weak identity, credential and access management • Malicious insiders • Insufficient due diligence
Understand reuse/disposal of compute resources, storage media and hardware, enforcing confidentiality	• Insufficient due diligence • Abuse and nefarious use of cloud services • Data loss • Shared technology issues
Verify configuration and protections of external and internal data flows between applications, containers, virtual devices, virtual machines, CSO infrastructure, and DoD infrastructure including encryption	• Data breaches • Malicious insiders • Insecure APIs • Abuse and nefarious use of cloud services • Shared technology issues
Verify configuration, protection, and resilience of external services such as commercial or DoD CSSPs, storage, or DNS	• Data loss • Denial of service • Shared technology issues
Verify data at rest encryption on CSP infrastructure leveraging DoD Key Management capability	• Data breaches • Data loss
Verify data leak protection between applications, virtual machines, or physical infrastructure	• Data breaches • Data loss
Ensure no backdoors to the CSO exist through management networks or other CSP infrastructure	• Abuse and nefarious use of cloud services • Shared technology issues • Weak identity, credential and access management • Insecure APIs
Validate security monitoring (physical security and system monitoring)	• Abuse and nefarious use of cloud services • Shared technology issues • Insecure APIs • Weak identity, credential and access management
Verify application-level data security policy on user actions and tools to monitor implementation	• Weak identity, credential and access management • Data breaches • Data loss • Malicious insiders • Abuse and nefarious use of cloud services
Verify capabilities to ensure service continuity including application and data backup and restoration, load and capacity management	• Data loss • Denial of service • Shared technology issues
Verify data spillage prevention, detection, reporting, and remediation, off boarding and sanitization processes	• Data breaches • Data loss • Abuse and nefarious use of cloud services • Shared technology issues

3.4 Phase 4 Considerations

Adversarial testing is limited to the portions of the DoD system for which the PMO is responsible – the "in the cloud" aspects and the shared responsibilities for security. This includes all SUT components, interfaces, and integration points. This also includes the DCO capabilities provided by the government CSSP and the CSP. The FedRAMP assessment may include adversarial test results in the form of 3PAO Penetration Testing of the CSO. Refer to the FedRAMP Penetration Test Guidance for more information about 3PAO penetration testing. Section 2.1.1 provides more information regarding FedRAMP penetration test results.

Note that the 3PAO Penetration Testing covers only the CSO ("of the cloud"). It does not cover the cloud-hosted DoD system ("in the cloud"). It also is not focused on the DoD mission or threat.

For Phase 4 Cybersecurity DT&E of cloud-hosted DoD systems, consider the following:

- CSPs usually expose a set of APIs that customers use to manage and interact with cloud services. Organizations, via the Internet, use these APIs to provision, manage, orchestrate, and monitor their assets and users. These APIs and management configuration items are targeted by adversaries. The CSP will need to participate in developing and enabling government testing for insider, external, and advanced persistent threat system abuse and misuse especially for those configuration items (e.g., CSP-provided APIs) or services provided by the CSO.
- Adversarial test teams should focus on the government-controlled portions of the developmental system and the portions provided by the CSP, including any areas where configuration, hardening, monitoring, or response responsibilities overlap.
- Assess operational resilience and survivability.
- Test DCO capabilities during adversarial test activities.
- SaaS services: The tester is not responsible for threat focused testing of the specific software application. However, the tester should test DoDIN integrated services, data security and system recovery during adversarial testing.
- Ensure data remains secure in transmission between the DoDIN and cloud services.
- Ensure data is stored securely and is accessible in accordance with the CSO SLA.
- Ensure the SaaS service is operationally resilient and recoverable within the contracted parameters (e.g., services available 85 percent of the time during standard business hours or some other requirements) in the event of system corruption or loss. The CSP may provide a test instantiation of the SaaS service for CDTs to test system resilience and survivability.
- IaaS services: If possible, the software portion of the cloud-hosted DoD system should be tested in a system integration lab before transition to the CSO infrastructure.
- Restrictions can limit adversarial testing in commercially provided implementation environments (CSOs). An alternative for testing would be to replicate the CSO in a dedicated environment at a cyber range or other DoD owned environment to allow for destructive testing. Another is to use a DoD private cloud for development, test, and fielding.
- Rules of Engagement (ROE) for adversarial testing should be coordinated with any external service provider, including the CSP.

- Coordinating with the CSP provides the potential to use CSO artifacts produced during PA and other assessments. Configuration documents provided by the CSP can identify where the system development team may have left gaps or introduced vulnerabilities into the system that can be exploited during adversarial assessment of those layers of the CSO, within the scope allowed by the CSP.

3.5 Phase 5 Considerations

The scope of the CVPA should include the CSO component of the DoD SUT to ensure that appropriate reconnaissance of the CSO is done to support the Phase 6 Adversarial Assessment (AA), in accordance with DOT&E requirements for this phase.

In addition to those items already described in the Guidebook and DOT&E guidance, the OTA should plan for Phase 5 Cybersecurity OT&E of cloud-hosted DoD systems to also include the following:

- Ensure that a representative sample of the real-world CSO operators and defenders participate in the CVPA.
- Ensure the CSP-provides subject matter experts to the OTA for the CSO portion of the SUT.
- Identify CSP trusted agents.
- Coordinate ROEs with the CSP.
- Determine whether the government/CSP contract explicitly addresses penetration testing of the CSO. Several commercial cloud service providers allow penetration testing by external organizations. If penetration testing of the CSO is not explicitly addressed in the contract, research to determine what the CSP allows.
- Ensure the CVPA scope covers the cybersecurity activities performed by both the CSSP and the CSP.
- Provide the OTA with documentation on the cybersecurity roles and responsibilities of the CSSP and CSP for the DoD SUT.
- Ensure CVPA results are provided to the CSP to support their development of a Plan of Actions and Milestones (POA&M) to address CSO-related vulnerabilities discovered during the CVPA. The tester should expect the DoD system PMO to track progress of this POA&M for resolution. Note that this should be the last activity before the exiting this phase.
- Provide CVPA results to the planners for Phase 6.

3.6 Phase 6 Considerations

DOT&E Memorandum *Enterprise Cloud Adoption—Operational Test Considerations*, October 1, 2018, recommends that the threat-representative cyber activities performed by National Security Agency-certified DoD-sponsored cybersecurity test teams include the CSO component of the DoD SUT (both physical and logical). Phase 6 assesses the cybersecurity services provided by the CSP, the CSSP, the IT O&S team and any others involved in the shared responsibilities for security.

In addition to those items already described in the Guidebook and DOT&E guidance, the OTA should plan for Phase 6 Cybersecurity OT&E of cloud-hosted DoD systems to include:

- Coordinating adversarial testing ROEs with the CSP. Identify CSP trusted agents.
- Ensuring the AA team includes adversarial cloud testers as well as mission performance testers.
- Ensuring the AA scope covers the cybersecurity activities performed by all cyber defenders (e.g., CSSP, CSP),
- Providing the OTA with documentation on the cybersecurity roles and responsibilities of the CSSP and CSP for the DoD SUT.
- Ensuring the OTA provides the AA results to FedRAMP and to the DoD PA authority as these results may impact the FedRAMP certification and/or DoD PA of the CSO.

4 Cloud Overview

The background information provided below is not comprehensive and does not include all the terminology used across DoD cloud efforts, nor the various CSPs, but provides a framework to allow a general level of understanding necessary for cybersecurity T&E planning and execution of DoD systems hosted on commercial CSOs. For a more detailed understanding of cloud computing, refer to the References section.

4.1 Cloud Deployment Models

Cloud infrastructure deployment models host the cloud services. The cloud deployment models are:

- Private: Provisioned for a single organization comprising multiple consumers (e.g., business units).
- Community: Provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.
- Public: Provisioned for open use by the general public.
- Hybrid: Composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology.

During Phases 1 and 2, the CyWG should seek a comprehensive understanding of the specific cloud service models, cloud deployment models, and how their implications are shared between the CSP and PMO. Each party must understand any additional elements in the stack and required interfaces between the DoDIN, the cloud deployment, and potentially the rest of the Internet. The specifics may not be fully understood until a CSP is selected, which is why Phases 1 and 2 are iteratively performed to inform all test events for Phases 3-6.

4.2 Cloud Technology and DoDIN Architecture

Figure 4 depicts the DoDIN architecture's required integration with cloud architectures. The DoDIN is protected from the Internet by "boundary protections" such as IAPs and CAPs. JRSS (between the DISN and B/P/C/S networks) provide the enterprise mid-point boundary protection for the DoDIN. (Some B/P/C/S use legacy mid-point protections.)

Figure 4 shows how various CSOs interface with infrastructure in the DoDIN depending on their location (on-premise/off-premise) and the CSO IL. An on-premise CSO (e.g., MilCloud V2.0) resides on a military installation or facility (B/P/C/S) and is within the DoDIN boundary.

An off-premise CSO is hosted in a CSP owned facility external to a DoD installation. An off-premise IL 2 CSO (sufficient when hosting only unclassified information) is directly accessible to internet-based DoD users via the Internet and accessible to DoD users on the DoDIN via an IAP.

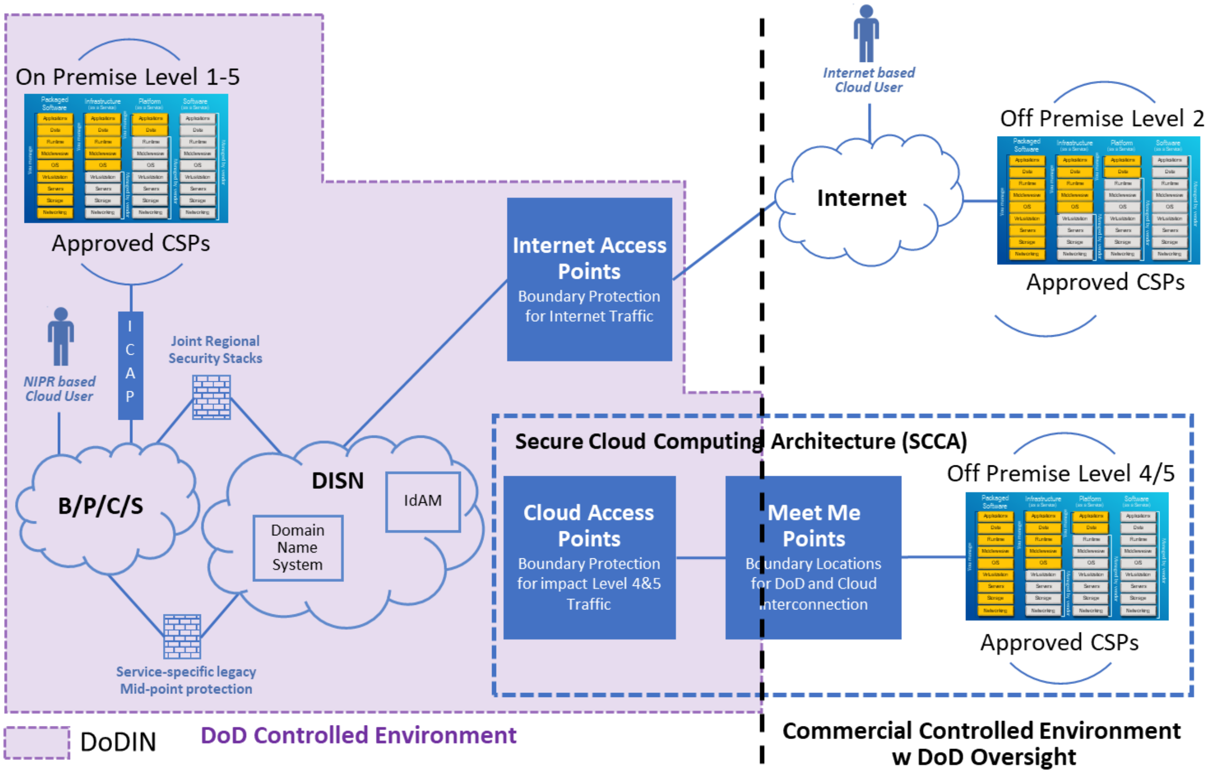

On Premise Level 1-5
Approved CSPs
NIPR based Cloud User
I C A P
Joint Regional Security Stacks
B/P/C/S
DISN
Domain Name System
IdAM
Service-specific legacy Mid-point protection
Internet Access Points
Boundary Protection for Internet Traffic
Internet based Cloud User
Internet
Off Premise Level 2
Approved CSPs
Secure Cloud Computing Architecture (SCCA)
Cloud Access Points
Boundary Protection for impact Level 4&5 Traffic
Meet Me Points
Boundary Locations for DoD and Cloud Interconnection
Off Premise Level 4/5
Approved CSPs
DoDIN
DoD Controlled Environment
Commercial Controlled Environment w DoD Oversight

Figure 4. Cloud Integration with the DoDIN Architecture

As shown in Figure 4, the DoDIN has integration points/services that CSOs must use to work in the DoDIN architecture. For example, a SaaS application that grants privileges to a user based on their identity would need to connect to the DoDIN Identity and Access Management capability to confirm the user's identity via their Common Access Card. DoDIN integration points/services include, but are not limited to:

- **Identity, Credential, and Access Management (ICAM)**: ICAM provides a single DoD authoritative source of enterprise identity supplemented with DoD component-specific attributes as necessary.
- **Public Key Infrastructure (PKI)**: The PKI service checks for certificate expiration, verifies a trusted certificate authority issued the certificate, and confirms that the certificate has not been revoked.
- **Domain Name System (DNS)**: DoDIN provides authoritative DNS servers on the DoDIN; CSOs must use the authoritative DNS servers.
- **Cloud Access Points (CAP)**: DoDIN provides CAPs for off-premise IL 4/5 CSOs to access the DoDIN
- **Internet Access Points (IAP)**: DoDIN provides IAPs as the boundary protection for Internet traffic
- **Joint Regional Security Stacks (JRSS)**: DoDIN provides JRSS as the cybersecurity boundary for traffic to/from individual military installations.

The DoD Secure Cloud Computing Architecture (SCCA) requires that traffic from the CSP traverse boundary protection (a CAP owned, configured, and defended by DISA or another DoD component) for monitoring and inspection before crossing a direct physical interconnect between the CSP and the DoDIN (a commercial Meet Me Point contracted by DISA), in lieu of connecting across the Internet. The DoD Enterprise recommends an Internal CAP (ICAP) for on-premise CSOs, although comparable boundary security may be substituted. Each CAP must have an ATO issued by the appropriate AO. The Meet Me Point is within the scope of the CAP ATO. Therefore, Internet-based DoD users will access off-premise IL4/5 CSOs through the DoDIN (IAP, DISN, CAP, Meet Me Point). For more information about the SCCA, refer to the DoD SCCA Functional Requirements Document.

4.2.1 Risk Management Framework

While the system inherits controls through the PA, as mentioned in section 2.1.2, there are additional controls the DoD PMO will have to implement, assess and authorize through the mission owner's AO. The eventual authority to operate (ATO) is granted at the DoD system level and testing should be conducted at that level to support the ATO. The CDT and OTA should be aware of this program and coordinate cybersecurity T&E with security control assessments.

The DoD Cloud Computing Security Requirement Guide (CC SRG) explains that cloud computing resulted in adjustments to the RMF process in support of using commercial CSOs. The DoDI 8510.01 RMF policy focuses on physical DoD owned and managed hardware systems and software applications in the DoDIN, to include DoD "on-premise" cloud infrastructures. When DoD does not own or manage the cloud infrastructure, as with commercial cloud infrastructures, also known as "off-premise" in cloud terminology, then the risk aspects, like the security responsibilities, change with the implemented CSO model.

4.3 Common Cloud-Related Roles and Responsibilities

This section provides a general overview of security roles and responsibilities for commercial cloud and is not intended to be all encompassing. Figure 1 depicts a baseline of the separation in responsibilities, but every contract will be unique.

4.3.1 CSP Responsibilities for Security

The CSP is responsible for maintaining the PA for the CSO and for cybersecurity "of" the cloud. The CSP's responsibilities for security depend on the type of service model used and where the line between the CSP and the PMO is drawn. Although there is potential for overlapping responsibilities, the PMO may negotiate responsibilities with the CSP. The CDT and OTA will need to fully understand where the CSP responsibilities end and where there is overlap with the mission owner or the CSSP as well as what tools are available and employed by the CSP or made available to the mission owner. The contract will describe these details. At the network level, the CSP is responsible for managing and defending the interfaces between the CSO and DoDIN, involving firewalls, encryption, and automated defensive cybersecurity operations, all of which may have some government overlap as defined in the contract with the CSP. The CSP is responsible for the physical security of the servers and data storage, but the government may share responsibility for configuring ports or user authorizations regarding these devices, depending upon the Cloud Service Model, the CSO, and the contract. The CSP will frequently virtualize the hardware to provide the CSO. The hypervisor needed to control this virtualization is a CSP responsibility. Cybersecurity, survivability and resilience testing may include evaluating this feature.

4.3.2 Cloud-hosted DoD System Program Manager Responsibilities for Security

The PMO is responsible for developing the SLA with the CSP, which is a section of a cloud computing agreement that defines the service and service levels provided and sets performance characteristics for the CSP/CSO. Even when an SLA is preset by the CSP, it is important for the PMO to understand and test it.

The PMO selects the cloud service model and implements the additional controls required "in" the cloud to obtain an ATO for the DoD system. The PMO defines CSP and CSSP responsibilities. An IaaS CSO provides the PMO with the most control, flexibility, visibility, and responsibility (Figure 1). The program should create its own virtual data center above the CSP virtualization layer, including software, servers, network management, and cybersecurity monitoring and protection. SaaS provides the least amount of PMO and mission-owner control. The PMO only has purview over the data entry, access interfaces and any integration with external DoD systems. PaaS offerings fall in between, with everything but the actual application system software and data, including the operating system and database clusters, closed to the PMO. The exact boundary lines and specific areas of responsibility can vary significantly among CSOs.

Figure 1 does not illustrate hidden shared responsibility or seams between the PMO and CSO, where the CSO delivers the service but the PMO is responsible for configuring it. Testers should be able to detect misconfiguration or misapplied APIs. PMOs should ensure that any external integration points are fully tested. Programs using a commercial cloud may use an external security service provider in addition to CSP-provided security services, which can augment and support the DoD requirement to align DoD systems with a CSSP.

"Cloud configuration management" refers to the operations and support (O&S) of cloud resources (e.g., storage, network, software and access control, etc.), which is an important responsibility for the PMO and mission owner during O&S. This function may be done by in-house DoD personnel or by a managed service provider, a company contracted by the government to manage IT infrastructure.

Cloud configuration changes frequently, and by various means (CSP management interface, manual adjustment, automation scripts, etc.). Section 4.3.3 describes the majority of cloud-hosted system breaches are attributed to customer misconfiguration of cloud resources. Cybersecurity testing of cloud configuration is crucial, and PMOs should plan and resource for this testing as well as coordinate the testing with the cloud O&S team.

4.3.3 CSSP Responsibilities for Security

In support of DoD DCO, DoD Instruction (DoDI) 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* requires the PMO to subscribe to the service of a DISA certified CSSP. DoD Chief Information Officer (CIO) Memorandum, *DoD Cybersecurity Activities Performed for Cloud Service Offerings* expands on the DoDI 8530.01 to specify cybersecurity activities for cloud-hosted DoD systems (Table 3). Activities with "•" must be performed by a CSSP, while the others may be performed by other qualified providers.

Table 3. Cybersecurity Activities for CSO (from DoD CIO Memorandum)

Vulnerability Assessment and Analysis	
○ External Vulnerability Scans	○ Web Vulnerability Scans
External Assessment	
● DoD Cyber Red Team Operations	○ Non-DoD Red Team Operations
○ Penetration Testing	○ Intrusion Assessment
Vulnerability Management	
○ DoD Required Security Configuration	○ Potential Vulnerability Mitigation
○ Compliance Monitoring	● Compliance Reporting
Malware Protection	
○ Malware Protection Implementation	● Malware Notification
Information Security Continuous Monitoring	
○ Endpoint Device Visibility	● Asset-Vulnerability Correlation
Cyber Incident Handling	
○ Boundary Protection Monitoring	○ Network and Endpoint Monitoring
● Incident Reporting	○ Incident Response
User Activity Monitoring	
○ Anomalous Insider Activity Detection	○ Audit Data Maintenance
● Audit Data-Counter Intelligence Correlation	
Attack Sensing & Warning (AS&W)	
● Boundary Protection AS&W	○ Application AS&W
● Warning Intelligence	
Information Operations Condition and Orders Compliance	
○ Implementation	● Notification and Assistance
Mission Owner Support and Cybersecurity Training	

PMOs should identify and engage a CSSP early in the program and include them in cybersecurity test events. Most of the DCO activities have T&E implications to the program. It is important to plan and coordinate tests with the CSSP to ensure all activities are satisfied.

4.4 Cloud-related Documents and Standards Relevant to Cybersecurity T&E Planning

1. **DoD Cloud Strategy**: The September 13, 2017, Deputy Secretary of Defense memorandum, “Accelerating Enterprise Cloud Adoption,” directs DoD to accelerate the adoption of cloud technology to maintain the DoD’s technological advantage and defines roles and responsibilities to develop and execute a “strategy to accelerate the adoption of cloud architectures and cloud services , focusing on commercial solutions.” On December 18, 2018, the Deputy Secretary of Defense released the *DoD Cloud Strategy*, which defines a DoD “enterprise cloud environment” composed of a general purpose cloud JEDI and multiple “fit-for-purpose” clouds. JEDI will be the DoD enterprise general purpose IaaS/PaaS cloud service offering for DoD. Once the JEDI contract is awarded, DoD CIO approval will be required for a program to use a "custom general purpose cloud" instead of

JEDI. Additionally, DoD CIO is preparing a separate contract vehicle for pre-approved contractors to assist DoD non-JEDI cloud programs with migrating to JEDI. Testers of cloud-based DoD systems should understand how their SUT is aligned with the DoD-mandated enterprise cloud environment.

2. **DoD Cloud Computing Security Requirements Guide (CC SRG):** The CC SRG details a cloud cyber assessment process that supports DoD's decision to grant a PA to a CSP, which allows that CSP to host DoD mission data. DoD Component AOs use the cloud SRG to assess a CSO's security posture and decide whether to grant an ATO to the DoD system using the CSO.

3. **FedRAMP Penetration Test Guidance Version 2.0, November 24, 2017**: This document provides guidelines for CSP, 3PAOs, and AOs regarding planning and conducting Penetration Testing (PT) and analyzing and reporting on the findings. The FedRAMP PT Guidance for 3PAOs is available at: https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf

4. **Defense Acquisition University Cloud Acquisition Guidebook:** The DAU cloud Acquisition Guidebook is the primer on DoD-specific requirements for acquiring cloud services.

4.4.1 FedRAMP Artifacts

Table 4 lists the FedRAMP artifacts; the CDT and OTA and OTA should leverage these artifacts for cybersecurity T&E.

Artifacts produced as part of the DISA PA process documentation should be requested directly from the CSP or its 3PAO. The PMO should ensure the contract with the selected CSP articulates the need for these artifacts to be provided to the government test organization. The CDT and OTA should ensure the RFP includes this expectation. (See Phase 1 in Section 3.)

Table 4. FedRAMP Artifacts

FedRAMP Artifact for use by Cybersecurity T&E
CSP System Security Plan (SSP)
SSP Attachment 1 - Information Security Policies and Procedures
SSP Attachment 2 - User Guide
SSP Attachment 3 - Electronic Authentication Plan
SSP Attachment 4 - Privacy Impact Assessment
SSP Attachment 5 - Rules of Behavior
SSP Attachment 6 - Information System Contingency Plan
SSP Attachment 7 - Configuration Management Plan
SSP Attachment 8 - Incident Response Plan
SSP Attachment 9 - Control Implementation Summary Workbook
SSP Attachment 10 - FIPS-199 Categorization
SSP Attachment 11 - Separation of Duties Matrix
SSP Attachment 12 - Laws and Regulations

FedRAMP Artifact for use by Cybersecurity T&E
SSP Attachment 13 - Integrated Inventory Workbook
3PAO Security Assessment Plan (SAP)
SAP Appendix A - Security Test Case Procedures
SAP Appendix B - Penetration Testing Plan and Methodology
SAP Appendix C - 3PAO Supplied Deliverables
3PAO Security Assessment Report (SAR)
SAR Appendix A - Risk Exposure Table
SAR Appendix B - Security Test Case Procedures
SAR Appendix C - Infrastructure Scan Results
SAR Appendix D - Database Scan Results
SAR Appendix E - Web Application Scan Results
SAR Appendix F - Assessment Results
SAR Appendix G - Manual Test Results
SAR Appendix H - Documentation Review Findings
SAR Appendix I - Auxiliary Documents
SAR Appendix J - Penetration Test Report
Plan of Action and Milestones (POA&M)
Continuous Monitoring Plan

5 Threats to Cloud-Based Systems

This section supplements Appendix X2 of the Guidebook, “Using Cyber Threat Assessments for Cybersecurity T&E”. The CyWG should maintain currency and relevancy in understanding the threat with respect to the system to be tested. Documented cloud security threats to commercial cloud services may compromise cloud-hosted DoD systems. Threats heavily target CSPs, and cloud computing services and data. Defense contractors and governmental entities worldwide are targets regardless of which hosting environment, cloud or conventional data center. The goal may be to steal or modify data, gain access to commercial and government clients’ networks, or to maintain persistence for the purpose of gathering intelligence, prepositioning code for later effects, and financial gain through ransomware or crypto-mining using the commercial cloud’s powerful computing resources, thus increasing risk to DoD.

While CSPs implement many advanced security protections, research shows that customer misconfiguration of cloud-provided security services has been the cause of most reported breaches. For example, customers have misconfigured virtual servers for public access or did not configure them to require username and password for access. These customer configuration issues highlight the need for rigorous security validation for the DoD system. Government testers should develop a rigorous test strategy that addresses the following cloud-based vulnerabilities:

The Treacherous 12 (see references):

1. Data breaches
2. Weak identity, credential and access management
3. Insecure APIs
4. System and application vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats
8. Data loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. Denial of service
12. Shared technology issues

6 Acronyms and Glossary of Terms

6.1 Acronyms

3PAO	Third Party Assessment Organization
AA	Adversarial Assessment
AO	Authorizing Official
API	Application Programming Interface
AS&W	Attack Sensing & Warning
ATO	Authority to Operate
B/P/C/S	Base/Post/Camp/Station
CAP	Cloud Access Point
CC SRG	Cloud Computing Security Requirement Guide
CDT	Chief Developmental Tester
CIO	Chief Information Officer
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CSSP	Cybersecurity Service Provider
CVAT	Cybersecurity Vulnerability Assessment Team
CVI	Cooperative Vulnerability Identification
CVPA	Cooperative Vulnerability and Penetration Assessment
CyWG	Cybersecurity Working Group
DAU	Defense Acquisition University
DCO	Defensive Cybersecurity Operations
DevSecOps	Development Security Operations
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DNS	Domain Name System
DT&E	Developmental Test and Evaluation
DoDIN	DoD Information Network
FedRAMP	Federal Risk and Authorization Management Program
IaaS	Infrastructure as a Service
IAP	Internet Access Point
ICAM	Identity, Credential, and Access Management
IL	Impact Level
LDTO	Lead Developmental Test Organization
MAIS	Major Automated Information Systems
MDAP	Major Defense Acquisition Programs
MOA	Memorandum Of Agreement
NIST	National Institute of Standards and Technology
JEDI	Joint Enterprise Defense Infrastructure
JRSS	Joint Regional Security Stack
O&S	Operations and Support
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency

PA	Provisional Authorization
PaaS	Platform as a Service
P-ATO	Provisional Authority To Operate
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
RFP	Request For Proposal
RMF	Risk Management Framework
ROE	Rules Of Engagement
SaaS	System as a Service
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCCA	Secure Cloud Computing Architecture
SLA	Service-Level Agreement
SRG	Security Requirements Guide
SSP	System Security Plan
SUT	System Under Test
T&E	Test and Evaluation

6.2 Cloud Cybersecurity T&E Glossary of Terms

This abbreviated glossary supplements the DoD Cybersecurity T&E Guidebook.

Cloud Service Provider (CSP): See DoD Cloud Computing SRG

Cloud Service Offering (CSO): See DoD Cloud Computing SRG

Cybersecurity Service Provider (CSSP): See DoDI 8530.01

Infrastructure as a Service (IaaS): See NIST SP 800-145

Platform as a Service (PaaS): See NIST SP 800-145

Software as a Service (SaaS): See NIST SP 800-145

7 References

- Defense Acquisition University (DAU) Cloud Acquisition Guidebook, Version 1, December 2018
- DEOS System Design Document (SDD), DRAFT Version 1.0, October 24, 2018
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network, Change 1, July 25, 2017
- DoD CIO Memo, Cybersecurity Activities Performed for Cloud Service Offerings, November 15, 2017
- DoD CIO Memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, December 15, 2014
- DoD Cloud Computing Security Requirement Guide (SRG), Version 1 Release 3, March, 6, 2017
- DoD Cybersecurity Test and Evaluation Guidebook, Version 2.0, April 25, 2018
- DoD Secure Cloud Computing Architecture (SCCA) Functional Requirements, Version 2.9, January 31, 2017
- DOT&E Memorandum, Procedures for Operational test and Evaluation of Cybersecurity in Acquisition Programs, April 3, 2018.
- DOT&E Memorandum, Enterprise Cloud Adoption – Operational Test Considerations, October 1, 2018
- FedRAMP Penetration Test Guidance Version 2.0, November 24, 2017
- The Treacherous 12 - Top Threats To Cloud Computing + Industry Insights, Cloud Security Alliance, 2017
- National Institute of Standards Special Publication (NIST SP) 800-145, “The NIST Definition of Cloud Computing”, September 2011