



DEPARTMENT OF DEFENSE

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

CHIEF INFORMATION OFFICER

NOV 15 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF, NATIONAL GUARD BUREAU
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTOR, STRATEGIC CAPABILITIES OFFICE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings

- References: (a) DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations" Change 1, July 25, 2017
(b) DoD Cloud Computing Security Requirements Guide, March 6, 2017
(c) Memorandum of Agreement between the Department of Defense and The Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017.
(d) DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012

This memorandum expands upon Reference (a) to address the engagement in Defensive Cyber Operations as DoD networks transition data, applications, capabilities and services to DoD and commercial cloud capabilities and services. Specifically addressed are activities that can be performed only by a DoD Cybersecurity Service Provider (CSSP) or a designated DoD organization in coordination with the DoD CSSP, and activities other qualified providers can perform on behalf of the mission owner and the Authorizing Official (AO). Mission owner terminology, is defined in Reference (b). For the purpose of this memorandum the term "Cloud Service Provider (CSP)" can mean the on-site hosting CSP, off-premise hosting CSP, or a third party CSP offering cloud security services such as a Cloud Access Security Broker (CASB)¹.

¹ Gartner IT Glossary: Cloud access security brokers (CASBs) are on-premises or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.

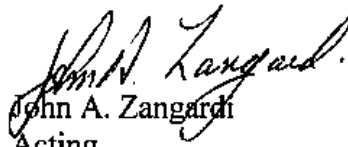
Throughout this memorandum, the term "DoD CSSP entity" will be used to describe a designated DoD organization in coordination with a CSSP.

This memorandum applies to Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the National Guard Bureau, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively as the "DoD Components"). In addition, this memorandum applies to the United States Coast Guard (USCG) in accordance with the direction in Paragraphs 4a, b, c, and d of Reference (c).

In accordance with the References (a) through (c), mission owners are required to register DoD networks, applications, data, and services that are migrating to DoD and/or commercial cloud capabilities and services. They are also required to identify the cloud service provider's alignment to an appropriate DoD CSSP in the DoD CIO System/Network Approval Process (SNAP) database. The mission owner is responsible for ensuring data migrated to a DoD or commercial cloud is at the appropriate security impact level In accordance with References (b) and (d).

Descriptions of those cybersecurity activities which must be performed specifically by a DoD CSSP or DoD CSSP entity, and those cybersecurity activities that could be performed on behalf of the mission owner by other service providers (e.g. CSP, DoD CSSP entity, CASB, milCloud, etc.) are provided at Attachment 1. A list of references is provided at Attachment 2. A list of abbreviations and acronyms is provide at Attachment 3.

The DoD CIO point of contact for this matter is, Dr. Mark Stanley, (703) 693-6685, mark.a.stanley38.civ@mail.mil.


John A. Zangardi
Acting

Attachments:
As stated

Apr 16, 2018

Attachment 1: Department of Defense Cloud Cybersecurity Activities

Department of Defense

OFFICE OF PREPUBLICATION AND SECURITY REVIEW

1. **Background Information:**

- a. Per the DODI 8530.01, DoD Components will:
 - (1) Conduct DoD information network (DODIN) operations and Defensive Cyberspace Operations–Internal Defensive Measures (DCO-IDM) in accordance with Commander, United States Strategic Command (CDRUSSTRATCOM) and DoD Component orders and directives to protect their respective portion of the DODIN.
 - (2) Oversee the implementation of all directed actions required by Commander, United States Strategic Command (CDRUSSTRATCOM) or its Component for their respective owned or operated portion of the DODIN. Implement directed actions in accordance with CDRUSSTRATCOM orders or other directives issued through the Commander, United States Cyber Command (CDRUSCYBERCOM) or subordinate Commander, Joint Force Headquarters-DODIN (CDRJFHQ-DODIN).
 - (3) Implement actions to ensure DODIN readiness, respond to potential adversary operations, or disrupt potential adversary presence in the DODIN.
 - (4) Support evaluation of DoD Component-wide CSSPs' activities. For Components not evaluated, or authorized to provide cybersecurity activities, forward a request for evaluation to the Defense Information Systems Agency (DISA) or Defense Intelligence Agency (DIA).
- b. Per the Federal Acquisition Regulation (FAR), Subpart 7.5, "Inherently Governmental Functions", the FAR does not prohibit a commercial entity from providing DoD cybersecurity activities. In accordance with ref (o) DFARS SUBPART 239.76— CLOUD COMPUTING, 239.7602-1 (b)(1), "Except as provided in paragraph (b)(2) of this section, the contracting officer shall only award a contract to acquire cloud computing services from a cloud service provider (e.g., contractor or subcontractor, regardless of tier) that has been granted provisional authorization by Defense Information Systems Agency, at the level appropriate to the requirement, to provide the relevant cloud computing services in accordance with the Cloud Computing Security Requirements Guide (SRG)". The DoD shall retain those activities that directly support decisions regarding the acceptance of risk. These activities support cloud offerings Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) for information Impact Levels 2, 4, and 5, per the DoD Cloud Computing SRG. **Note: Impact Level 6 will be further addressed as the capability matures. Initially, Impact Level 6 should identify the DoD CSSP that will perform the Incident Reporting and address who will perform all other activities or how the AO, PM, and Mission Owner plan to address each activity for Impact Level 6.**
- c. Table 1: The Cybersecurity Activities listed below, shall be used when establishing requirements to obtain cybersecurity services in order to be compliant with cybersecurity activities outlined in ref (a).

DoD Cybersecurity Activities
Performed for Cloud Service Offerings

Cybersecurity Activities		IaaS		PaaS		SaaS	
		Level 2	Level 4/5	Level 2	Level 4/5	Level 2	Level 4/5
Cybersecurity Activities, per DoDI 8530.01	Vulnerability Assessment and Analysis (VAA)						
	External Vulnerability Scans	○	○	○	○	○	○
	Web Vulnerability Scans	○	○	○	○	○	○
	External Assessment (*An external assessment must be performed annually. The AO will select the external assessment(s) that best fit the need of the application or mission system. The AO has the option to choose all of the external assessments, but only one is required annually.)						
	DoD Cyber Red Team Operations	●	●	●	●	●	●
	Non-DoD Red Team	○	○	○	○	○	○
	Penetration Testing	○	○	○	○	○	○
	Intrusion Assessment	○	○	○	○	○	○
	Vulnerability Management						
	Apply DoD required security configurations	○	○	○	○	○	○
	Perform actions to mitigate potential vulnerabilities or threats	○	○	○	○	○	○
	Monitor Vulnerability Management Compliance	○	○	○	○	○	○
	Report Vulnerability Management Compliance	●	●	●	●	●	●
	Malware Protection						
Malware Protection Implementation	○	○	○	○	○	○	
Malware Notification	●	●	●	●	●	●	
Information Security Continuous Monitoring (ISCM)							
Maintain continuous visibility into endpoint devices	○	○	○	○	○	○	
Correlate asset and vulnerability data with threat data	●	●	●	●	●	●	
Cyber Incident Handling							
Network Security Monitoring/Intrusion Detection for Boundary Cyberspace Protection (BCP) Functions (as defined in ref (r))	N/A	●	N/A	●	N/A	●	
Network and Endpoint Security Monitoring at the Enclave Level	○	○	○	○	○	○	
Incident Reporting	●	●	●	●	●	●	
Incident Response - Analysis	○	○	○	○	○	○	
Incident Handling Response	○	○	○	○	○	○	
DODIN User Activity Monitoring (UAM) for DoD Insider Threat Program							
Employ UAM capabilities to detect anomalous insider activity	○	○	○	○	○	○	
Maintain insider threat audit data	○	○	○	○	○	○	
Correlate insider threat audit data with Counter Intelligence	●	●	●	●	●	●	
Warning Intelligence and Attack Sensing and Warning (AS&W)							
AS&W for BCP	N/A	●	N/A	●	N/A	●	
AS&W at the Application	○	○	○	○	○	○	
Warning Intelligence	●	●	●	●	●	●	
Information Operations Condition (INFOCON) & Orders (e.g. TASKORD, OPORD, FRAGO, etc.) Compliance/Network Operations (NETOPS) Awareness							
INFOCON & Orders Implementation	○	○	○	○	○	○	
INFOCON & Orders Notification and Assistance	●	●	●	●	●	●	
Additional Activity							
Mission Owner Support and Cybersecurity Training	○	○	○	○	○	○	

"●" = CSSP function must be performed by a DoD CSSP or DoD CSSP entity; functions cannot be performed external to DoD hosting environments or by a commercial service provider.
 "○" = CSSP function may be hosted and performed by a DoD CSSP, DoD CSSP entity, or can be contracted out (internal to the Component or external to a Provider). An Authorizing Official (AO) needs to consider the risk and determine who will be responsible for providing the capability/activity.
 "N/A" = Not Applicable

Table 1: Cybersecurity Activities Listing

- d. For IaaS, PaaS, and SaaS offerings, the CSP(s) may offer cybersecurity solutions and services or tools to mission owners and provide or perform required cybersecurity functions as provided in the requirements (e.g. Request for Proposal (RFP), Statement of Work (SOW), etc.).
- e. It is required of the mission owner, program manager and AO to determine if the capabilities, hosting environment, and services made available to perform these activities will suffice, and whom will perform those activities to meet DoD cybersecurity requirements. In some cases, this may be a shared responsibility where the tool, a capability, application, or service is made available by the CSP and the functions are performed by a DoD CSSP or DoD CSSP entity.
- f. How to utilize Table 1: Cybersecurity Activities Listing, in accordance with paragraphs 1.d. and 1.e., above:
 - (1) Determine the proper Impact Level and Cloud Service Offering combination (e.g. Level 2, IaaS);
 - (2) Determine and align to a DoD CSSP that will perform Incident Reporting;
 - (3) In accordance with paragraph 2, below, evaluate what CSSP activities the CSSP or other designated DoD Component can perform and be identified as DoD or Government only functions (at a minimum, those identified as “●” which cannot be outsourced to a commercial entity);
 - (4) In accordance with paragraphs 2 and 3, below, evaluate what CSSP activities the CSP can perform and do not need to be performed by a DoD CSSP (identified as “○”);
 - (5) Fill in Table 2, “Cybersecurity Activities Tracking Template”, located at the end of Attachment 2;
 - (6) Obtain AO risk acceptance of any gaps in CSSP activities or coverage. An Authorizing Official (AO) needs to consider the risk and determine who will be responsible for providing each capability/activity and, where gaps exist, if this is an acceptable level of risk associated to the level of protection required for any hardware, software, or data placed into a cloud environment.
 - (7) The mission owner, PM, and AO must review and ensure, for those instances where a CSP is chosen to perform cybersecurity services, that the CSP has been evaluated successfully for those cybersecurity services during their FedRAMP evaluation.
 - (8) The mission owner is required to provide access to their capabilities, assets, and data to DoD inspection and assessment team(s). The CSP will ensure that access and permissions are granted to the mission owner, PM, AO, CSSP, and DoD inspection and assessment team(s). Access to all cybersecurity related information collected by CSPs shall be restricted to only those required to perform the cybersecurity activities on behalf of the DoD.

2. DoD Only Activities (designated in Table 1: Cybersecurity Activities Listing, above with an "•"):

- a. The following operational criteria was used to distinguish the CSSP activities that should be performed by a DoD CSSP or DoD CSSP entity:
 - (1) Lateral sharing amongst other interested DoD CSSPs. (Rationale: Commercial entities do not have access to the communication channels and classified systems operated by the DoD CSSP community for sharing information.)
 - (2) Defensive measures that require an AO risk acceptance decision.
 - (3) Prioritization of resource allocation based on operational requirements (i.e. prioritization of response actions, prioritizing vulnerabilities, responsiveness to directives, etc.).
- b. A mission owner identifies and addresses the mission/operational impact and works with the CSSP, which participates in comprehensive and elevated reporting to United States Cyber Command (USCYBERCOM) via secure transport and methods. Further, unlike the CSP, the CSSP is bound to follow the Command & Control direction, prioritization, and accountability enforced by the Joint Forces Headquarters-DODIN (JFHQ-DODIN) Command & Control (C2) execute order (EXORD) in accordance with DoD regulations.
- c. There are restricted DoD data sources that a commercial CSP will not be able to access and therefore must be maintained and updated by the DoD mission owner.
 - (1) The mission owner is required to register all implementations of DoD networks, applications, data, and services that are migrating to DoD and/or commercial cloud capabilities and services as well as identifying the alignment to an appropriate DoD CSSP in the DoD CIO System/Network Approval Process (SNAP) database. This information must be shared by the mission owner to all parties (DoD CSSP, DoD CSSP entity, AO, DoD Sponsor (when required), and CSP).
 - (2) The mission owner must maintain and distribute changes for DoD CSSP and CSP POCs to both parties and the AO.

3. Cybersecurity activities that may be performed by a DoD CSSP, DoD CSSP entity, or other service provider (e.g. CSP, CASB, milCloud, etc.) (designated in Table 1: Cybersecurity Activities Listing, above with an "o"):

Note: Cybersecurity activities performed by either a DoD CSSP, DoD CSSP entity, or another service provider (collectively referred to in this memorandum as the "provider") that best fits the needs and risk acceptance of the Component AO. An AO along with the PM of the system/application/data needs to consider the risk and determine who will be responsible for providing the capability/activity listed below that best fits the needs of the application or mission system.

- a. The activities designated in Table 1: Cybersecurity Activities Listing with a "o" can be performed by an entity other than a DoD CSSP as long as they are contractually binding in a formal contract. The formal agreement must detail the arrangement and expectations between the provider and mission owner for establishing, measuring, and maintaining a

required level of performance. Contracts often require explicit service level agreements (SLAs) when specific regulatory directives do not exist. Prior to the Cloud Service Offering being accepted, the AO must ensure that the capability to perform the cybersecurity activities listed in Table 1: Cybersecurity Activities Listing were evaluated during the FedRAMP and the Provisional Authorization.

- b. DoD CSSPs and other cyber elements also have responsibility for performing these activities for the DODIN, which may overlap with outsourced commercial entities responsibilities; therefore, coordination between mission owner, DoD CSSP, and the provider may be required. The mission owner must provide contract language that specifies the CSP share the results with the identified DoD CSSP for incident reporting.

4. Cybersecurity activities descriptions:

- a. **Vulnerability Assessment and Analysis:** The mission owner, in coordination with the PM and AO, will identify the need for Vulnerability Assessments and Analysis (VAA), which is most appropriate. The provider will support internal and external VAA by providing technical assistance, reporting requirements and situational awareness. For internal VAA scan results, the provider will analyze and coordinate remediation actions for identified vulnerabilities. The provider must develop a process to request and allow the execution of any of the VAA activities. The provider will maintain results locally, and share the results of all such assessments and provide situational awareness to the mission owner and the DoD CSSP of any known vulnerabilities, mitigation strategies, and major changes to the mission owner environment.

(1) **External Vulnerability Scans (may be performed by DoD or outsourced):** This activity is conducted in support of, or in augmentation to, the DoD Component's internal, DoD mandated vulnerability scanning and assessment actions. This activity is provided primarily for assistance in the protection of a mission owner's data. CSPs must have demonstrated that they effectively and within DoD standards/requirements have the ability to scan systems during their Federal Risk and Authorization Management Program (FedRAMP) authorization. The provider will send scan notification to the mission owner and the DoD CSSP. The provider will execute at least two scans per year and provide results to the mission owner and the DoD CSSP. The provider is required to report all vulnerabilities found to mission owner and the DoD CSSP. The provider will analyze and provide an executive summary for each scan to the mission owner and the DoD CSSP. Data obtained from the scans will be analyzed to determine potential impacts to the mission owner operations, and will identify and mitigate or remediate the identified findings. Analysis of the results may require additional scans to verify mitigation. The provider will support the DoD CSSP in monitoring the mission owner's corrective actions or mitigation strategies. The provider will share the results of all scans and provide situational awareness to the mission owner and the DoD CSSP of any known vulnerabilities or mitigation strategies. **Note: These scans are different than the monthly vulnerability scans that are performed by the system owner and reported per the USCYBERCOM cyber task order (CTO).**

(2) **Web Vulnerability Scans (WVS) (may be performed by DoD or outsourced):** This activity is conducted to assist the mission owner in complying with

USCYBERCOM TASKORD 13-0613 for public facing web presence. This activity is provided to assist the mission owner in protecting DoD demilitarized zone (DMZ) whitelisted web sites. CSPs must have demonstrated that they effectively and within DoD standards/requirements have the ability to scan systems during their Federal Risk and Authorization Management Program (FedRAMP) authorization. The provider will conduct WVS and provide results to the mission owner and the DoD CSSP. The provider will analyze and provide an executive summary for each scan to the mission owner and the DoD CSSP. Any data obtained from WVS activities will be analyzed to determine potential impacts to mission owner network operations, and will identify and mitigate or remediate the identified findings. Analysis of the results may require additional scans to verify mitigation. The provider will use documented policies and procedures, to test and evaluate WVS tools on their effectiveness, appropriateness, and safety prior to use on mission owner systems in order to provide for the safeguarding of these systems. The provider will support the DoD CSSP in monitoring the mission owner's corrective actions or mitigation strategies. The provider will make available situational awareness reports to the mission owner and DoD CSSP of any known vulnerabilities, mitigation strategies, and major changes to the environment.

- b. **External Assessment:** External assessments are conducted in support of AO requirements appropriate to the needs of the system. The provider has responsibility to support mission owners with the coordination of these activities. The provider also coordinates remote assessments prior to Commander Cyber Readiness Inspection (CCRIs)/Commander Cyber Operational Readiness Inspections (CCORIs) for mission owners scheduled for CCRIs/CCORIs. External assessments are performed without DoD intelligence, and do not emulate threat actors against DoD assets. CSPs must have demonstrated that they effectively and within DoD standards/requirements have the ability to perform an external assessment as part of their incident handling capabilities during their FedRAMP authorization. The mission owner, in coordination with the PM and AO, will identify the need for External Assessments, the most appropriate type of external assessment and possible sources for external assessments. The provider(s), in conjunction with the mission owner, will develop a process to request and allow the execution of any of the External Assessment activities. The provider will supply technical assistance, reporting requirements and situational awareness for external assessments. For external assessment results, the provider will analyze and remediate identified vulnerabilities and deliver an After Action Report that details the exploited vulnerable points of the in-scope targets, with general remediation recommendations. The provider will maintain results locally, and share the results and situational awareness reports of all such assessments for any known vulnerabilities, mitigation strategies, and major changes to the mission owner environment with the mission owner and the DoD CSSP.
- (1) **DoD Cyber Red Team Operations (must be performed by DoD):** DoD Cyber Red Team operations effectively exploit U.S. Military and, as authorized, Government networks by emulating a potential adversary's exploitation or attack capabilities against targeted DoD missions or resources. DoD Cyber Red Teams are certified by NSA and accredited by USCYBERCOM to conduct live play on the DODIN. DoD Cyber Red Team operations are designed to identify exposed information and

vulnerabilities of the DoD's security posture, improve the skills and capabilities of DoD cyber forces, and develop mitigation strategies to improve enterprise cybersecurity. To accomplish these tasks, Red Teams must coordinate within the DoD and Intelligence Communities to obtain information on a potential threat actors' tactics, techniques, and procedures (TTPs), identify indicators of compromise, and demonstrate the potential operational impact of found vulnerabilities. The requirement that threat emulation on the DODIN can only be done by a certified DoD Red Team prohibits a commercial entity from performing operations on the live network. Although CSPs advertise Red Team capabilities, this is not the same capability as DoD Cyber Red Team Operations. The provider shall support mission owner required DoD Cyber Red Team Operations as required by the mission owner and the DoD CSSP. Results from the DoD Cyber Red Team Operations will include corrective actions that must be performed, therefore, the provider shall execute corrective actions and mitigations for those identified vulnerabilities and report actions to the mission owner and the DoD CSSP. **Note: Due to legal liability concerns, the mission owner must include a description of their implementation accreditation boundary for DoD Red Team Operations contracts with CSPs.**

- (2) **Non-DoD Red Team (may be performed by DoD or outsourced):** Non-DoD Cyber Red Team operations are an independent group that challenges an organization to improve its effectiveness. One type of commercially offered Red Team provides a more realistic picture of the security readiness than exercises, role playing, or announced assessments. The Red Team may trigger active controls and countermeasures within a given operational environment. The key theme is that the aggressor is composed of various threat actors, equipment and techniques that are at least partially unknown by the defenders. The use of cyber red teams provides real-world attack simulations designed to assess and significantly improve the effectiveness of an entire information security program. Benefits include challenges to preconceived notions and clarifying the problem state that planners are attempting to mitigate. More accurate understanding can be developed of how sensitive information is externalized and of exploitable patterns. The provider will prepare a detailed description, to include architectural diagrams, of the Non-DoD Red Team Operation to the mission owner and the DoD CSSP after obtaining approval from the mission owner to perform or conduct Non-DoD Red Team Operation. Upon conclusion of the Non-DoD Red Team Operation, the provider will make available the results that detail the exploited vulnerable points of the in-scope targets with general remediation recommendations to the mission owner and the DoD CSSP. The provider will execute approved corrective actions and mitigations and report actions to the mission owner and the DoD CSSP for identified vulnerabilities. **Note: Due to legal liability concerns, contracts with CSPs must include a description of the accreditation boundary and licensing agreements for non-DoD Red Team Operations or Penetration Testing.**
- (3) **Penetration Testing (may be performed by DoD or outsourced):** Under direction of the mission owner, the chosen assessors attempt to breach the security features of an application, system, or network in a controlled manner. Penetration testing often involves conducting actual attacks on real systems and data, using the same tools and

techniques used by actual attackers. This type of testing is used to determine the effectiveness of the implemented technical security controls in a goal-oriented, overt manner. CSPs must have demonstrated that they effectively and within DoD standards/requirements have the ability to perform penetration testing during their FedRAMP authorization. The provider is required to deliver a detailed description of the Penetration Test to the mission owner and the DoD CSSP along with obtaining approval from the mission owner to perform or conduct Penetration Test. Upon conclusion of the Penetration Test, the provider will deliver the results that detail the exploited vulnerable points of the in-scope targets with general remediation recommendations to the mission owner and the DoD CSSP. The provider will create and disseminate lessons learned to the mission owner and the DoD CSSP. The provider will track and execute approved corrective actions and mitigations for identified vulnerabilities and report actions to the mission owner and the DoD CSSP. **Note: Due to legal liability concerns, contracts with CSPs must include a description of the accreditation boundary and licensing agreements for non-DoD Red Team Operations or Penetration Testing.**

- (4) **Intrusion Assessment (may be performed by DoD or outsourced):** This activity provides a mechanism for the identification of previously unidentified intrusion activity. The end goal of an intrusion assessment is to identify whether a data has been compromised, highlight unauthorized activity, identify any critical vulnerabilities, and provide direction for the enhancement of local mission owner cyber defense. CSPs must have demonstrated that they effectively and within DoD standards/requirements have the ability to perform intrusion assessments as part of their incident handling capabilities during their FedRAMP authorization. The provider will need to make available a detailed description of the Intrusion Assessment to the mission owner and the DoD CSSP and obtain approval from the mission owner to perform or conduct Intrusion Assessment. Upon conclusion of the Intrusion Assessment, the provider will make available the results and remediation recommendations to the mission owner and the DoD CSSP.
- c. **Vulnerability Management:** USCYBERCOM directly alerts all Combatant Commands, Services, DoD Agencies, and Field Activities of new/emerging threats and vulnerabilities. Providers support mission owners and facilitate communication with component vulnerability management SMEs for vulnerability management implementation and compliance. This is a patch management program and CSPs must have demonstrated they effectively and within DoD standards/requirements have the ability to manage patches during their FedRAMP authorization process. While the support to the vulnerability management program is not a DoD-specific activity, the compliance reporting/status is specific to DoD and must be submitted to the mission owner and the DoD CSSP.
- (1) **Apply DoD Required Security Configurations (may be performed by DoD or outsourced):** Establish a comprehensive vulnerability management plan (e.g. CSP System Security Plan (SSP)) for the approval of the mission owner and the DoD CSSP. The plan will address vulnerability remediation, STIG compliance management, and patch testing.

- (2) **Perform Actions to Mitigate Potential Vulnerabilities or Threats (may be performed by DoD or outsourced):** Provide feedback to the mission owner and the identified DoD CSSP POC on the relationship between the vulnerability management status of assets and any malicious incidents that occur. The provider ensures proper protection of data at rest and data in transit, in accordance with DoD policies.
 - (3) **Monitor Vulnerability Management Compliance (may be performed by DoD or outsourced):** The provider collects and manages Plans of Actions and Milestones (POA&M) for open vulnerabilities. The POA&M is supplied by the mission owner to the provider. The POA&M process helps identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in programs and systems. The provider produces required documentation, ensures timely reporting of compliance statistics for each Information Assurance Vulnerability Alert (IAVA) and Computer Network Directive to the mission owner, aggregates acknowledgement and compliance reports, and updates the POA&M accordingly.
 - (4) **Report Vulnerability Management Compliance (must be performed by DoD):** Information Assurance Vulnerability Management (IAVM) employs positive control mechanisms to mitigate potentially critical software vulnerabilities, through the rapid development and dissemination of actions to all Component Heads. The mission owner is responsible to ensure the proper acknowledgement and reporting of vulnerability management notices via generated messages as directed by USCYBERCOM and/or JFHQ-DODIN.
- d. **Malware Protection:** The DoD mission owner ensures that Anti-virus/Anti-Malware software is implemented and maintained by a provider. The mission owner is responsible for compliance with USCYBERCOM and JFHQ-DODIN requirements and conducts timely reporting of the detection of unknown/emerging malware to the DoD CSSP. The mission owner, working with their provider, is required to identify, remediate, mitigate and deliver an acceptable plan of action and milestones (POA&M) to the AO.
- (1) **Malware Protection Implementation (may be performed by DoD or outsourced):** For malware defense, the mission owner will ensure that malware implementation is delivered by a provider. The chosen provider shall establish the capability to capture, correlate, analyze, and provide continuous visibility into DoD assets. The provider assesses the compliance, effectiveness, and changed state of security controls protecting the DoD Component-owned or -operated system(s) and/or application(s) and data. The provider maintains ongoing awareness of information security, threats, and vulnerabilities to support organizational risk management decisions. The provider supports DODIN operations by providing ongoing awareness of threats and security status of traffic, fault, performance, bandwidth, route, and associated network management areas. The provider also supports monitoring of employee use of the DODIN to detect anomalous activity. The provider will implement the capability to detect and prevent malware incidents (e.g. malicious code, malicious logic, malicious applets, etc.) by employing malware detection and remediation mechanisms to detect and remove malicious code. The provider contains the spread of malware to prevent further damage and eradicate the malware from infected hosts. Employ mitigating actions to prevent reinfection and restore functionality. The provider will configure

malware detection mechanisms to perform periodic scans of the mission owner's environment in accordance with current DoD and DoD Component guidance. The provider will maintain and access Anti-Virus and Anti-Malware software for latest updates and releases. The provider will have the capability to support virus responses and self-reporting 24x7. The provider is to ensure that proper protection of data at rest and data in transit, in accordance with DoD policies. The provider shall track and execute corrective actions as appropriate and report actions to the mission owner and the DoD CSSP POC. The mission owner, PM, and/or AO should ensure that the provider has documented procedures on reporting of malware to mission owner; provides detailed reports immediately following all malware incidents; and at least annually, provides a trending analysis report from malware incidents.

- (2) **Malware Notification (must be performed by DoD):** This is the act of “notifying” the mission owner and assisting when required, as opposed to the act of “applying” the Malware Protection performed by a commercial vendor or other DoD entity that has the skill sets to perform this act of applying the protection. These are the processes by which the DoD CSSP alerts mission owners to new malware and assists the mission owner when an incident occurs. The DoD CSSP maintains contact with anti-malware software vendors so that effective countermeasures are developed, tested, and deployed as quickly as possible. DoD is informed in advance of the commercial world of malware across the board. So in some instances a CSP can react quickly (e.g. when a vulnerability is associated directly with its vendor products), but in other cases the CSP would not be privy to the information until it was public (e.g. when a 3rd party application is operating within the CSP environment). Reporting shall be done by the DoD CSSP in accordance with ref (d).
- e. **Information Security Continuous Monitoring (ISCM):** ISCM provides constant observation and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations. Overall ISCM furnishes ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, cyber hygiene, and cybersecurity operational readiness. It is a government responsibility to declare the category and severity of the incident or event. This additionally involves the filing and safeguarding of all incident reports for current and future analysis. Reporting shall be done by the DoD CSSP in accordance with ref (d). More guidance on ISCM can be found in NIST SP 800-137, NIST SP 800-37, and NIST SP 800-39.
- (1) **Maintain Continuous Visibility into Endpoint Devices (may be performed by DoD or outsourced):** The mission owner will ensure that visibility into endpoint devices is delivered by a provider. The chosen provider shall establish the capability to capture, correlate, analyze, and provide continuous visibility into DoD assets. The provider will assess the compliance, effectiveness, and changed state of security controls protecting the DoD Component-owned or -operated system(s) and/or application(s) and data, and report changes in the state of security controls to the mission owner and the identified DoD CSSP POC. The provider will support DODIN operations by providing ongoing awareness of threats and security status of traffic, fault, performance, bandwidth, route, and associated network management areas via the DoD CSSP. The provider monitors employee use to detect anomalous activity.

The provider must maintain ongoing awareness and security status of reportable cyber events and incidents to support timely, informed, and actionable cyber incident handling decisions and report all threats (both perceived and confirmed) to the mission owner and the DoD CSSP POC.

- (2) **Correlate Asset and Vulnerability Data with Threat Data (must be performed by DoD):** The DoD CSSP shall aggregate all information from the provider and correlate that information with intelligence information received through intelligence community channels within the DoD. The DoD CSSP will support DODIN operations and DCO internal defensive measures by providing ongoing awareness and security status of reportable cyber events and incidents. This capability supports timely informed and actionable cyber incident handling decisions in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B. The incident reporting shall be performed by the DoD CSSP in accordance with ref (d). The DoD CSSP shall maintain ongoing awareness and security status of reportable cyber events and incidents to support timely, informed, and actionable cyber incident handling decisions. The DoD CSSP will support the Risk Management Framework (RMF) by providing ongoing awareness and security status of the posture of an organization's information and systems. This capability supports timely informed and actionable risk decisions and continued RMF decisions. The DoD CSSP will synchronize requirements through the DoD assigned governance body for ISCM collaboration, cooperation, and coordination; to synchronize policy, strategy, and requirements for ISCM implementation across DoD national security systems (NSSs) and non-NSSs.

f. **Cyber Incident Handling**

- (1) **Network Security Monitoring/Intrusion Detection for Boundary Cyberspace Protection (BCP) Functions (BCP is defined in ref (r)) (must be performed by DoD):** This is a DoD-performed activity since boundary cyberspace protection is positioned to monitor ingress and egress points to commercial cloud service provider environments of the Defense Information Systems Network (DISN) to detect and report unauthorized activity and determine if network and host activity is intrusion related. The information provides analysts with technical event and incident data to process into intrusion analysis, correlation, and reporting. This involves vertical and horizontal information sharing internal to the DoD on classified networks utilizing classified channels. This activity is also the focal point for both USCYBERCOM and JFHQ-DODIN to maneuver cyber forces to properly defend and control access to the DODIN. Note that this activity is not applicable for Impact Level 2 Cloud Service Offerings.
- (2) **Network and Endpoint Security Monitoring at the Enclave Level (may be performed by DoD or outsourced):** This activity is accomplished through the monitoring of connections on or accessing the host to detect unauthorized activity. The information provides analysts with technical event and incident data to process into intrusion analysis, correlation, and reporting. The mission owner will ensure that network and endpoint security monitoring is delivered by a provider. The chosen provider will monitor and detect the mission owner's environment and will report anomalous events detected to the mission owner and the DoD CSSP. The provider is

required to review and analyze logs in a timely manner to detect intruders and shall provide copies of audit/system logs as requested by the DoD CSSP POC for correlation activities and requirements from USCYBERCOM and/or JFHQ-DODIN. The provider must ensure proper protection of data in transit and data at rest in accordance with DoD policy. The provider will correlate vulnerability management data with Network and Endpoint Security Monitoring to provide fewer false positives, a higher level of fidelity for incident detection, handling, and countermeasure. The provider will track and execute corrective actions as appropriate and report actions to the mission owner and the DoD CSSP. This activity can be performed by a commercial entity; however, all information gathered will be sent to the DoD CSSP that performs incident reporting for the mission owner within the timelines identified in CJCSM 6510.01B. **Note: For IaaS and PaaS, per USCYBERCOM and JFHQ-DODIN, if the DoD CSSP has the technical capability to leverage intel-derived signatures specific to the DoD, then the activity should be performed by a DoD CSSP.**

- (3) **Incident Reporting (must be performed by DoD):** Per guidance in JFHQ-DODIN Subordinate Campaign Plan (to be released before the end of 2017), and JFHQ-DODIN Annual Operational Order ref (q), Operation Gladiator Shield 17, only DoD CSSPs will have access to the classified incident reporting system and access to the classified information channels for disseminating and reporting incidents and events. The reporting system and classified channels are utilized to direct intelligence-based operational requirements and rapid distribution for law enforcement and intelligence sharing. It is a government responsibility to declare the category and severity of the incident or event. This involves the filing and safeguarding of all incident reports for current and future analysis. The DoD CSSP will enter incidents into the internal DoD Joint Incident Management System (JIMS) on behalf of the mission owner. Reporting shall be done by the DoD CSSP in accordance with ref (d). **Note: The DoD CSSP responsible for incident reporting must be identified by the mission owner in the SNAP database.**
- (4) **Incident Response – Analysis (may be performed by DoD or outsourced):** This activity is used to determine the effect of incidents on mission owner networks to prevent further damage and aid in the recovery process. The activity focuses on identification of system compromises, remediation, and prevention. This activity can consist of volatile data analysis, forensic media analysis, reverse engineering, malware analysis, and intrusion assessments. All information gathered will be sent to the DoD CSSP that performs incident reporting for the mission owner within the timelines identified in CJCSM 6510.01B. The mission owner will ensure that incident response analysis is delivered by a provider. The chosen provider will develop and implement a process and procedures to conduct incident handling in accordance with DoD incident handling procedures and provide a copy to the mission owner and DoD CSSP. The provider must report events under investigation and all potential incidents and correlated information from these incidents and events that occur on mission owner systems using documented procedures in accordance with DoD guidance. These events/incidents will be provided to the mission owner and the DoD CSSP POC, who will report it utilizing secure internal DoD systems to

USCYBERCOM. Reporting by the DoD CSSP POC shall be done in accordance with ref (d). The provider shall deliver all notes and information related to incidents upon request from the identified DoD CSSP for the purposes of law enforcement and/or counter intelligence requirements. The provider will report all incidents and questionable events in a timely manner to the mission owner and the DoD CSSP. The provider will verify, validate, and provide the operational impact on incidents reported to the provider by the mission owner or the DoD CSSP and provide feedback in a timely manner. The provider shall implement passive countermeasures where feasible and notify the mission owner and the DoD CSSP. The provider will retain all incident report documentation for one year and share collected data with the mission owner and the DoD CSSP POC via means specified by the mission owner upon request.

(5) Incident Handling Response (IR) (may be performed by DoD or outsourced):

This activity is the rapid deployment of an incident response team to a mission owner's location to counter a known, uncontained threat. The team is responsible for discovering malicious activity, quarantining the threat, and restoring the integrity of the mission owner's network. All information gathered will be sent to the DoD CSSP that performs incident reporting for the mission owner within the timelines identified in CJCSM 6510.01B. The mission owner will ensure that incident handling response is delivered by a provider. The chosen provider will be able to perform various incident response activities. The provider should have a portfolio of offerings which can perform volatile data analysis (VDA), forensic media analysis (FMA), and/or reverse engineering/malware analysis (RE/MA) from suspected compromised systems or files as requested or required by the mission owner and the DoD CSSP. The provider will perform an intrusion assessment or incident response as requested or required by the mission owner or DoD CSSP. The status and analysis of findings will be reported to the mission owner and the DoD CSSP upon request. The provider is required to acknowledge, maintain, and reference all trend analysis or post-incident analysis disseminated by the DoD CSSP or mission owner and provide any applicable follow-up and timely feedback to post-incident analysis. The provider will develop countermeasures and mitigation strategies or remediation for common vulnerabilities and will track and execute corrective actions as appropriate and report actions to the mission owner and the DoD CSSP.

- g. **DODIN User Activity Monitoring (UAM) for DoD Insider Threat Program:** The actual implementation and capability could be performed by a DoD CSSP, DoD CSSP entity, or a CSP. The correlation and reporting of counterintelligence events must be performed by a DoD CSSP or DoD CSSP entity. This could lead to other intelligence driven reporting and collection of information/events.

- (1) Employ UAM Capabilities to Detect Anomalous Insider Activity (may be performed by DoD or outsourced):** The implementation and actions to detect anomalous activity can be performed by a CSP, in coordination with the DoD CSSP, depending on the risk that the AO deems appropriate. The AO must ensure that the UAM and auditing capabilities used to identify and evaluate anomalous activity are performed in accordance with DoD Directive (DoDD) 5205.16, "The DoD Insider Threat Program," September 30, 2014. The provider shall document UAM

procedures and share with the mission owner. Implement capabilities and procedures to respond to anomalous user activity on the mission owner's environment, including procedures to mitigate potential damage to data on the mission owner's environment and report activity to the mission owner and the DoD CSSP. Provide a detailed report, track, and execute corrective actions, as appropriate, and report actions to the mission owner and the DoD CSSP POC. Share collected data with the mission owner and the DoD CSSP via means specified by the mission owner.

- (2) **Maintain Insider Threat Audit Data (may be performed by DoD or outsourced):** Implement procedures to maintain audit data and preserve audit data chain of custody. Secure data collected in support of insider threat in compliance with Federal and DoD regulations (e.g., Privacy Act Information, Personally Identifiable Information (PII), Protected Health Information (PHI), Health Insurance Portability and Accountability Act (HIPAA), Law Enforcement (LE)/ Counter Intelligence (CI)). Document all procedures for chain of custody of UAM data and share with mission owner.
 - (3) **Correlate Insider Threat Audit Data with Threat Data (must be performed by DoD):** Acknowledge, maintain, and reference any trend analysis to identify common vulnerabilities, and develop countermeasures and mitigation strategies or remediation. Coordinate with LE/CI to correlate insider threat profiles.
- h. **Warning Intelligence and Attack Sensing & Warning (AS&W):** Warning Intelligence is defined in Joint Publication 2-0 as "those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (Approved for inclusion in JP 1-02.)". Attack Sensing & Warning is defined in the CNSSI-4009 as "Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed."
- (1) **Attack Sensing & Warning (AS&W) for BCP Functions (BCP is defined in ref (r)) (must be performed by DoD):** This is a DoD-performed activity since boundary cyberspace protection is positioned to monitor ingress and egress points to commercial cloud service provider environments of the Defense Information Systems Network (DISN), which is driven by intelligence collected. It is the collection, normalization, and correlation of event incident data to identify intentional unauthorized activity across a large spectrum, including computer intrusions or attacks. AS&W data is generated and correlated from device logs, security application logs, incident tickets, archives, other DoD CSSPs, and mission owners. This type of analysis requires specially trained DoD Defensive Cyber Operations (DCO) analysts and hinges on collaboration with all stakeholders in the cybersecurity hierarchy. This activity must be closely coupled to decision makers in order to assess operational risk and develop appropriate responses. Note that this activity is not applicable for Impact Level 2 Cloud Service Offerings.
 - (2) **Attack Sensing and Warning (AS&W) at the Application (may be performed by DoD or outsourced):** For IaaS and PaaS, if the DoD CSSP has the technical capabilities to leverage classified intel-derived signatures then the activity must be

performed by a DoD CSSP. For SaaS, since the commercial entity owns the operating systems and applications, the CSP is better suited to perform this activity.

- (3) **Warning Intelligence (must be performed by DoD):** Warning intelligence activities are intended to detect and report time-sensitive intelligence collected on foreign developments that forewarn of hostile actions or intentions against United States' partners or interests. Relevant warning intelligence relating to DoD information systems and computer networks received from USSTRATCOM or other intelligence sources is distributed to mission owners via the DoD CSSPs for situational awareness.
- i. **Information Operations Condition (INFOCON)/ORDERS/Network Operations (NETOPS) Awareness:** The assignment of an INFOCON level, as defined in ref (a), is a specific DoD activity that cannot be outsourced to a commercial entity. The INFOCON system provides a framework of prescribed actions and cycles necessary to reestablish the confidence level and security of information systems. The DoD CSSP, or DoD CSSP entity, monitors the mission owner's INFOCON level, providing technical subject matter experts (SMEs) to the commander, as requested, to assist with determining INFOCON measures, and tracking and reporting INFOCON compliance. This is very specific to the DoD. The Orders process (e.g. Task Order (TASKORD), Warning Order (WARNORD), Fragmentation Order (FRAGO), Operational Order (OPORD), etc.) activity to prioritize and disseminate information and/or requirements are specific to DoD and cannot be outsourced to a commercial entity, as described in ref (q). Similar to INFOCON, the DoD CSSP, or DoD CSSP entity, monitors the mission owner's compliance with the order and provides technical SME support to the commander upon request. These orders are very specific to the DoD. **Note: The implementation of INFOCON measures and DoD Orders can be performed by a CSP depending on the risk that the AO deems appropriate.**
 - (1) **INFOCON and Orders Implementation (may be performed by DoD or outsourced):** Execute approved INFOCON level and DoD orders actions specified by the mission owner and/or the DoD CSSP. Share operational and/or technical impacts of any change or execution of a DoD order and a Tailored Readiness Option (TRO) with the mission owner and DoD CSSP via means specified by the mission owner. The provider must keep the mission owner and DoD CSSP apprised to the status of implementation as requested.
 - (2) **INFOCON and Orders Notification and Assistance (must be performed by DoD):** Per ref (q), the mission owner must report compliance of executed DoD order and INFOCON level actions and coordinate with the DoD CSSP on any issues. The DoD CSSP shall notify mission owner of any INFOCON changes or orders that are received. The DoD CSSP, or DoD CSSP entity, monitors the mission owner's compliance with the order and provides technical SME support to the mission owner upon request. The mission owner, in coordination with the DoD CSSP or DoD CSSP entity, will prioritize and disseminate information and/or requirements to the CSP as required.
- j. **Mission Owner Support and Cybersecurity Training (may be performed by DoD or outsourced):** Support to mission owner cybersecurity training is not a DoD-specific task.

DoD can choose to perform the training itself, or outsource the training to a commercial entity. DoD's responsibility for outsourced training is to develop the training requirement, provide compliance oversight, and develop the criteria for measuring effectiveness.

- k. **Definitions of Activities:** For complete definitions of cybersecurity activities, refer to reference (a).
- l. The DoD Component AO in coordination with the PM will determine who will be responsible for providing the CSSP activity that best fits the needs of the mission owner.
 - (1) The mission owner shall ensure the provider performs their activities in accordance with references (a) through ref (i) and in compliance with references (j) through (q).
 - (2) In order for the program manager, mission owner, and/or AO to have proper defensive measures in place to protect the DoD data and information stored within a cloud instance, the template at Table 2: Cybersecurity Activities Tracking Template provides a guide to ensure they can track and maintain which provider is performing the cybersecurity activity along with up-to-date points of contact for each activity.

DoD Cybersecurity Activities
Performed for Cloud Service Offerings

Cybersecurity Activities DoD Component NOSC or DoD CSSP:	Type of Service Offering (Circle one): IaaS PaaS SaaS	Impact Level (Circle One): Level 2 Level 4 Level 5
Vulnerability Assessment and Analysis (VAA) External Vulnerability Scans Web Vulnerability Scans	<i>Provider Company/DoD Org</i> <i>Provider Company/DoD Org</i>	
External Assessment (Circle One) DoD Cyber Red Team Operations Non-DoD Red Team Penetration Testing Intrusion Assessment	<i>DoD Component Org/POC</i> <i>Provider Company/DoD Org</i> <i>Provider Company/DoD Org</i> <i>Provider Company/DoD Org</i>	
Vulnerability Management Apply DoD required security configurations Perform actions to mitigate potential vulnerabilities or threats Monitor Vulnerability Management Compliance Report Vulnerability Management Compliance	<i>Provider Company/DoD Org</i> <i>Provider Company/DoD Org</i> <i>Provider Company/DoD Org</i> <i>DoD Component Org/POC</i>	
Malware Protection Malware Protection Implementation Malware Notification	<i>Provider Company/DoD Org</i> <i>DoD Component Org/POC</i>	
Information Security Continuous Monitoring (ISCM) Maintain continuous visibility into endpoint devices Correlate asset and vulnerability data with threat data	<i>Provider Company/DoD Org</i> <i>DoD Component Org/POC</i>	
Cyber Incident Handling Network Security Monitoring/Intrusion Detection for Boundary Cyberspace Protection (BCP) Network and Endpoint Security Monitoring at the Enclave Level Incident Reporting Incident Response - Analysis Incident Handling Response	<i>DoD POC (only if IL4 or IL5. IL2 = N/A)</i> <i>Provider Company/DoD Org</i> <i>DoD POC (from Line 3 of Table)</i> <i>Provider Company/DoD Org</i> <i>Provider Company/DoD Org</i>	
DODIN User Activity Monitoring (UAM) for DoD Insider Threat Program Employ UAM capabilities to detect anomalous insider activity Maintain insider threat audit data Correlate insider threat audit data with Counter Intelligence	<i>Provider Company/DoD Org</i> <i>Provider Company/DoD Org</i> <i>DoD Component Org/POC</i>	
Warning Intelligence and Attack Sensing and Warning (AS&W) AS&W for BCP AS&W at the Application Warning Intelligence	<i>DoD POC (only if IL4 or IL5. IL2 = N/A)</i> <i>Provider Company/DoD Org</i> <i>DoD Component Org/POC</i>	
Mission Owner Support and Cybersecurity Training	<i>Provider Company/DoD Org</i>	
Information Operations Condition (INFOCON) & Orders (e.g. TASKORD, OPORD, FRAGO, etc.) Compliance/Network Operations (NETOPS) Awareness INFOCON & Orders Implementation INFOCON & Orders Notification and Assistance	<i>Provider Company/DoD Org</i> <i>DoD Component Org/POC</i>	
Instructions: (1) Fill in DoD Component NOSC or DoD CSSP information (3) Circle Type of Service Offering on the Top (4) Circle Impact Level for Service Offering on Top (5) Replace <i>Italicized</i> information with the Provider information (6) Ensure "Incident Reporting matches the DoD Component NOSC or DoD CSSP" block at the top, and add POC information (7) As a reminder, only select one (1) External Assessment type		

Table 2: Cybersecurity Activities Tracking Template

Attachment 2: REFERENCES

- (a) DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations" Change 1, July 25, 2017
- (b) DoD Cloud Computing Security Requirements Guide, current version listed at http://iase.disa.mil/cloud_security/Pages/index.aspx
- (c) Memorandum of Agreement between the Department of Defense and The Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017. Current version listed at <https://dcms.uscg.afpims.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6-/The-Office-of-Information-Management-CG-61/Interagency-Agreements/>
- (d) CJCSM 6510.01B, "Cyber Incident Handling Program," July 10, 2012
- (e) DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems" of June 6, 2012
- (f) NIST SP 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations"
- (g) Federal Risk and Authorization Management Program (FedRAMP)
- (h) Presidential Executive Order 13800 – "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017
- (i) DoDM 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)" February 24, 2012
- (j) 32 CFR Part 236, "DoD Defense Industrial Base Cybersecurity Activities"
- (k) 32 CFR 2002, "Controlled Unclassified Information"
- (l) FAR (48 CFR) Subpart 4.19, "Basic Safeguarding of Contractor Information Systems" (see also FAR Subparts 7, 12, & 52)
- (m) DoDI 5000.02, Enclosure 14, "Operation of the Defense Acquisition System" August 10, 2017
- (n) DFARS Subpart 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting" (see also DFARS Subparts 202, 212, & 252)
- (o) DFARS Subpart 239.76, "Cloud Computing" (see also DFARS Subpart 252)
- (p) DoDD 8140.01, "Cyberspace Workforce Management," 31 July 2017
- (q) JFHQ-DODIN Annual Operational Order, Operation Gladiator Shield 17

Attachment 3: ABBREVIATIONS AND ACRONYMS

AO	Authorizing Official
AS&W	Attack, Sensing, & Warning
BCP	Boundary Cyberspace Protection
C2	Command and Control
CASB	Cloud Access Security Broker
CCORI	Commander Cyber Operational Readiness Inspections
CCRI	Commander Cyber Readiness Inspection
CDRJFHQ-DODIN	Commander, Joint Force Headquarters-DODIN
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CI	Counterintelligence
CJCSM	Chairman of the Joint Chiefs of Staff manual
COOP	Continuity of Operations Plan
CSP	Cloud Service Provider
CSSP	Cybersecurity Service Provider
DCO	Defensive Cyber Operations
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DODIN	Department of Defense Information Network
DRP	Disaster Recovery Plan
EXORD	Executive Order
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FMA	Forensic Media Analysis
FRAGO	Fragmentation Order

DoD Cybersecurity Activities
Performed for Cloud Service Offerings

HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IDM	Internal Defensive Measures
INFOCON	Information Operations Condition
ISCM	Information Security Continuous Monitoring
IR	Incident Handling Response
JFHQ-DODIN	Joint Force Headquarters-DODIN
LE	Law Enforcement
NetOps	Network Operations
NIST	National Institute of Standards and Technology
NOSC	Network Operations Security Center
NSS	National Security Systems
OPORD	Operations Order
OSD	Office of the Secretary of Defense
PaaS	Platform as a Service
PHI	Personal Health Information
PII	Personally Identifiable Information
PM	Program Manager
POC	Point of Contact
RE/MA	Reverse Engineering/Malware Analysis
RMF	Risk Management Framework
SaaS	Software as a Service
SLA	Service Level Agreement
SME	Subject Matter Expert
SNAP	System/Network Approval Process
SP	Special Publication
SRG	Security Requirements Guide
STIG	Security Technical Implementation Guide
TASKORD	Tasking Order
TRO	Tailored Readiness Option

TTP	Tactics, Techniques, and Procedures
UAM	User Activity Monitoring
USCYBERCOM	United States Cyber Command
VAA	Vulnerability Assessments and Analysis
VDA	Volatile Data Analysis
WARNORD	Warning Order
WVS	Web Vulnerability Scan