DEPARTMENT OF DEFENSE (DOD)
CLOUD CYBERSPACE PROTECTION GUIDE

16 October 2017

Incorporating Change 1, 19 December 2017

Developed by the
Defense Information Systems Agency (DISA)
for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DOD, DISA, or any non-Federal entity, event, product, service, or enterprise.

CLOUD CYBERSPACE PROTECTION GUIDE

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

EXECUTIVE SUMMARY

The Cloud Cyberspace Protection guide defines a set of reporting and incident handling procedures for the organizations that will protect the Department of Defense (DOD) Information Network (DODIN) in the cloud, as specified in the DOD Cloud Computing Security Requirements Guide (SRG) section on cyberspace protection and incident response. This guide defines how mission owners, organizations providing mission cyberspace protection (MCP), boundary cyberspace protection (BCP), cloud service providers[1] (CSPs), and Joint Force Headquarters DODIN (JFHQ-DODIN) will cooperate in response to cyber incidents and events in accordance with DOD Cloud Computing (SRG) and DOD Instruction (DODI) 8530.01.

This document introduces BCP and MCP functions that are accomplished through the execution of a collection of cybersecurity activities and defensive cyberspace operations (DCO) internal defensive measures with the objective of protection for the DODIN with regards to cloud services:

1. BCP Function: Protects the Defense Information Systems Network (DISN) from an event or incident that utilizes external cloud services.

2. MCP Function: Protects systems, applications, and data hosted within cloud services.

The guide provides additional guidance to the DOD Cloud Computing SRG and DOD Instruction (DODI) 8530.01 by defining reporting and data-sharing relationships between organizations providing protection. The procedures described in each annex establish specific interactions between organizations conducting BCP and MCP cybersecurity activities and DCO internal defensive measures, their interactions with mission owners and CSPs, and the reporting requirements of cyber events and incidents to JFHQ-DODIN. The procedures apply to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) Cloud service offerings (CSOs) installed as: On-Premises CSO Level 2/4/5; Off-Premises CSO Level 2; or Off-Premises CSO Level 4/5. This document does not apply to Level 6 CSOs.

The responsibilities and functions are elaborated in the annexes:

- Annex A – Responsibilities: DOD Component & JFHQ-DODIN
- Annex B – Boundary Cyberspace Protection Function
- Annex C – Mission Cyberspace Protection Function
- Annex D – Mission Owner
- Annex E – CSP

This document is expected to evolve as the procedures are put into practice and new best practices emerge. As such it should be treated as a foundation upon which to improve in addition to providing uniformity and efficient cooperation in cloud cyberspace protection.

[1] Mission owner, MCP, BCP, and CSPs are defined in Section 6.3 of reference (d), the DOD Cloud Computing SRG

CLOUD CYBERSPACE PROTECTION: BASE PLAN

1. Introduction

1.A. General.

Protection for cloud services consists of two major functions, which are defined in Sections 1.B - 1.C.

1.B. Boundary Cyberspace Protection (BCP) Function

The primary function of organizations that perform BCP is executing cybersecurity activities and DCO internal defensive measures to protect the Defense Information Systems Network (DISN) from events or incidents that utilize public, private, hybrid, or community clouds, through approved CSPs that can impact the DISN through a dedicated connection via a boundary cloud access point (BCAP).

1.C. Mission Cyberspace Protection (MCP) Function

The primary function of organizations that perform MCP is executing cybersescurity activities and DCO internal defensive measures to protect mission owners' systems, applications, and data hosted in the three cloud service models. MCP monitors all traffic within the cloud environment, whether connected via BCAP, virtual private network (VPN), internet access point (IAP), direct internet access to public servers, or other. MCP monitors privileged actions (e.g. cloud management or mission owner application administration) and monitors for events or incidents against the mission owner applications (e.g. structured query language (SQL) injection). MCP supports BCP to identify correlations between related events or incidents reported via the Joint Incident Management System (JIMS) that impact multiple mission owners, or CSPs.

The reference procedures defined in this document establish specific interactions between the organizations performing BCP and MCP, mission owner, Joint Force Headquarters DODIN (JFHQ-DODIN), and the CSP to execute DODIN operations and DCO missions to protect the DODIN. These interactions are defined in a way to support the full range of cloud solutions that DOD may utilize and to support the transition to the Joint Information Environment (JIE).

1.D. Purpose and Audience.

The purpose of this document is to establish procedures between organizations providing BCP and MCP, mission owners, JFHQ-DODIN, and the CSPs who together will protect the applications, data and systems on DOD and non-DOD cloud solutions. This document does not replace existing reporting requirements.

1.E. Applicability.

This document:

a) Applies to all organizations providing BCP and MCP; mission owners; CSPs; and JFHQ-DODIN as they relate to cloud protection.

b) Applies to .mil domains.

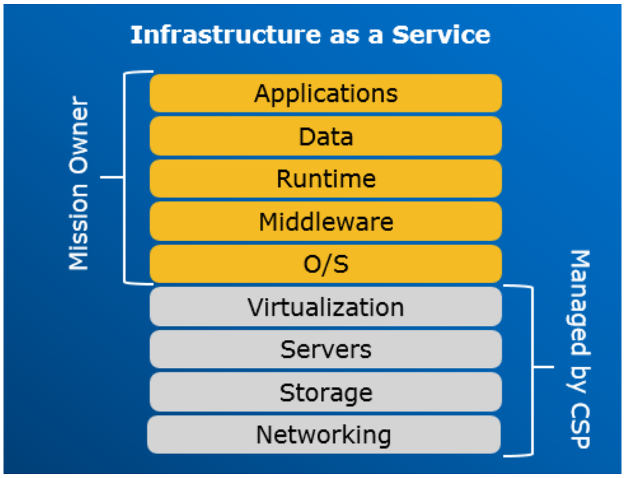
c) Does not apply to mission owners that typically operate networks that may not be part of the DISN or .mil domain (e.g., commissaries; exchanges; Morale, Welfare and Recreation (MWR) organizations; Non-Appropriated Fund (NAF) organizations; educational entities (e.g., National Defense University (NDU)), etc.). These mission owners will follow the guidance from the Cloud Computing SRG.

2. Background

2.A. Cloud Service Models

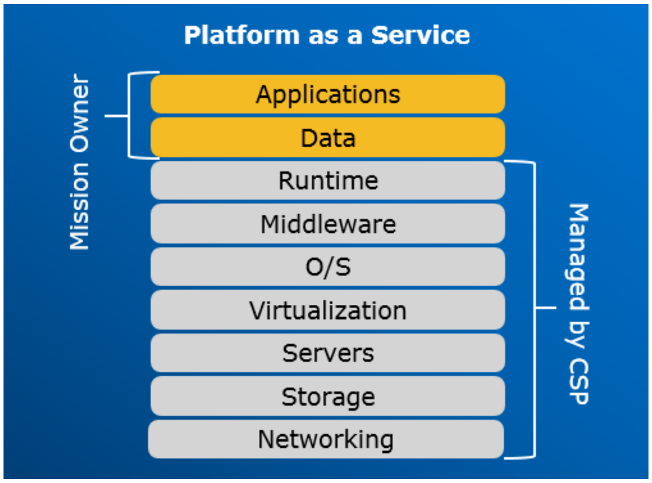
As applications and capabilities are moved to the cloud, mission owners will select CSOs offered by CSPs. CSOs will be offered in three Service Models[2]:

- Infrastructure as a Service (IaaS): The capability provided to a mission owner is to provision processing, storage, networks, and other fundamental computing resources where a mission owner is able to deploy and run arbitrary software, which can include operating systems and applications. A mission owner does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

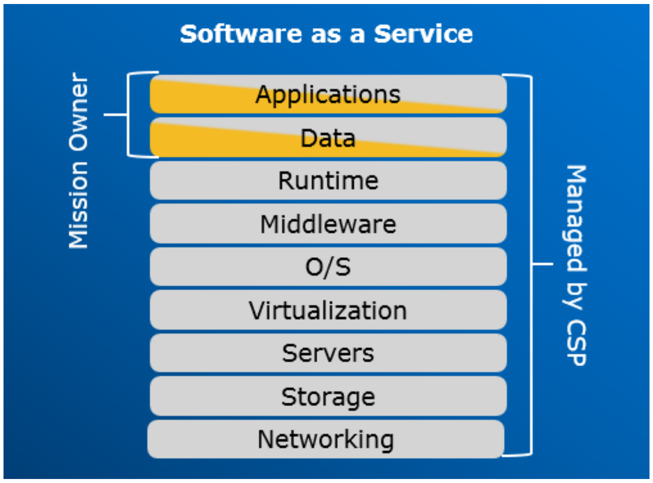


[2] Ref (i): Definitions from National Institute of Standards and Technology (NIST) SP 800-145: The NIST Definition of Cloud Computing

- Platform as a Service (PaaS): The capability provided to a mission owner is to deploy onto the cloud infrastructure mission owner-created or acquired applications created using programming languages, libraries, services, and tools supported by the CSP. (This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.) A mission owner does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.



- Software as a Service (SaaS): The capability provided to a mission owner is to use the CSP's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. A mission owner does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.



2.B. CSO Connection Models

There are three CSO connection models that a mission owner can select to host their data. Off premises connection models are dependent on the Information Impact Levels as defined in the DOD Cloud Computing SRG. The connection models are On-Premises CSO Level 2/4/5 (including milCloud), Off-Premises CSO Level 2, and Off-Premises CSO Level 4/5. Below is an explanation of the protection requirements for each offering:

On-Premises CSO Level 2/4/5 (Including milCloud): A mission owner utilizing a CSP on-premises must acquire through a contract or perform MCP (authorized cybersecurity service provider (CSSP)) to protect systems, applications, and/or data hosted in the cloud service model. It does not establish a dedicated connection via the BCAP (see Figure 1) or require support from an organization providing

BCP. Monitoring and protection from events or incidents originating from the Internet are accomplished at the IAP or the internal cloud access point (ICAP).

Off-Premises CSO Level 2: A mission Owner utilizing an off premises CSO requires support from an organization providing MCP (authorized CSSP) to protect systems, applications, and/or data hosted in the cloud service model. For an Information Impact Level 2 CSO, the CSP off premises does not use a BCAP and does not require support from an organization providing BCP (see Figure 1).

Off-Premises CSO Level 4/5: A mission owner utilizing an off premises CSO requires support from an organization providing MCP (authorized CSSP) to protect systems, applications, and/or data hosted in the Cloud. If the mission owner utilizes an off premises CSO for Information Impact Level 4/5 (see Figure 1), they must establish a dedicated connection via a BCAP. The BCAP requires support from an organization providing BCP for all connections through that BCAP.

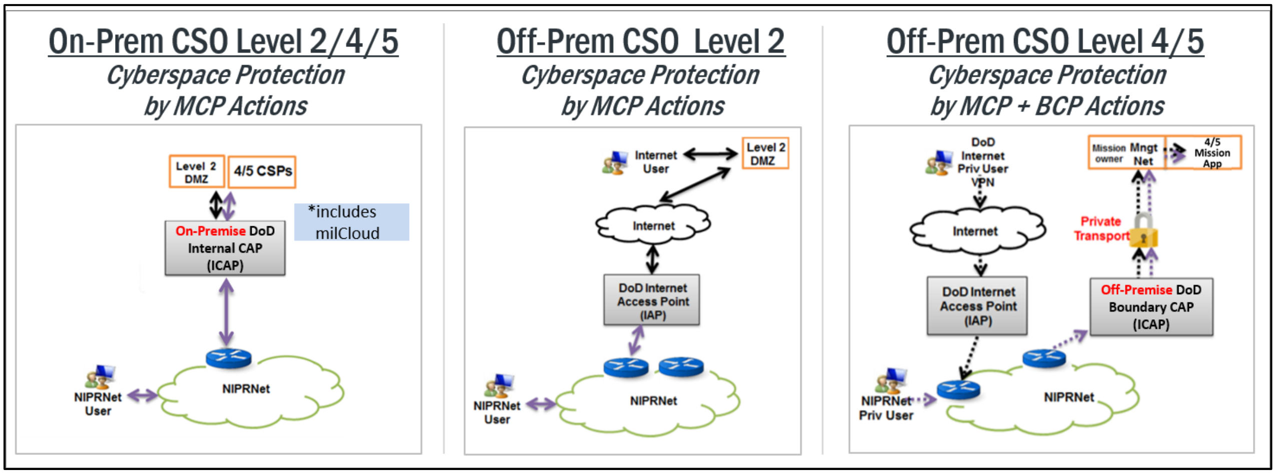


Figure 1 – Depiction of the Various Cloud Access Points[3]

2.C. Cloud Cyberspace Protection Information Sharing Structure

The DOD Cloud Computing SRG defines a reporting and communication function structure for cloud services. This structure supports the information flows that will be necessary to support global cyber situational awareness. The DOD Cloud Computing SRG defines the BCP and MCP actions. BCP actions monitor and protect the DISN perimeter where BCAP connections to CSPs are supported. MCP actions will monitor and protect the systems, applications, and data that are remotely hosted on the cloud service model on behalf of their mission owners. Each mission owner will identify an authorized CSSP to provide MCP for its systems, applications, and data. Each BCAP will have an authorized CSSP to perform the BCP for that BCAP.

The scope of responsibility for organizations providing MCP and the CSP will depend on the features of the cloud service. In the case of off premises SaaSs, for example, the CSP would perform 24x7 incident

[3] Ref (k) extracted from CAP Security FRD

and event detection. The mission owner is responsible for coordinating the CSP compliance with United States Cyber Command (USCYBERCOM) and JFHQ DODIN directives and orders (e.g. tasking order (TASKORD)).

Given that a single CSP may provide multiple and simultaneous service offerings for different mission owners, JFHQ-DODIN will analyze potential impacts across mission owners, cloud services, and CSPs based on information coming from the organizations providing MCP and BCP.

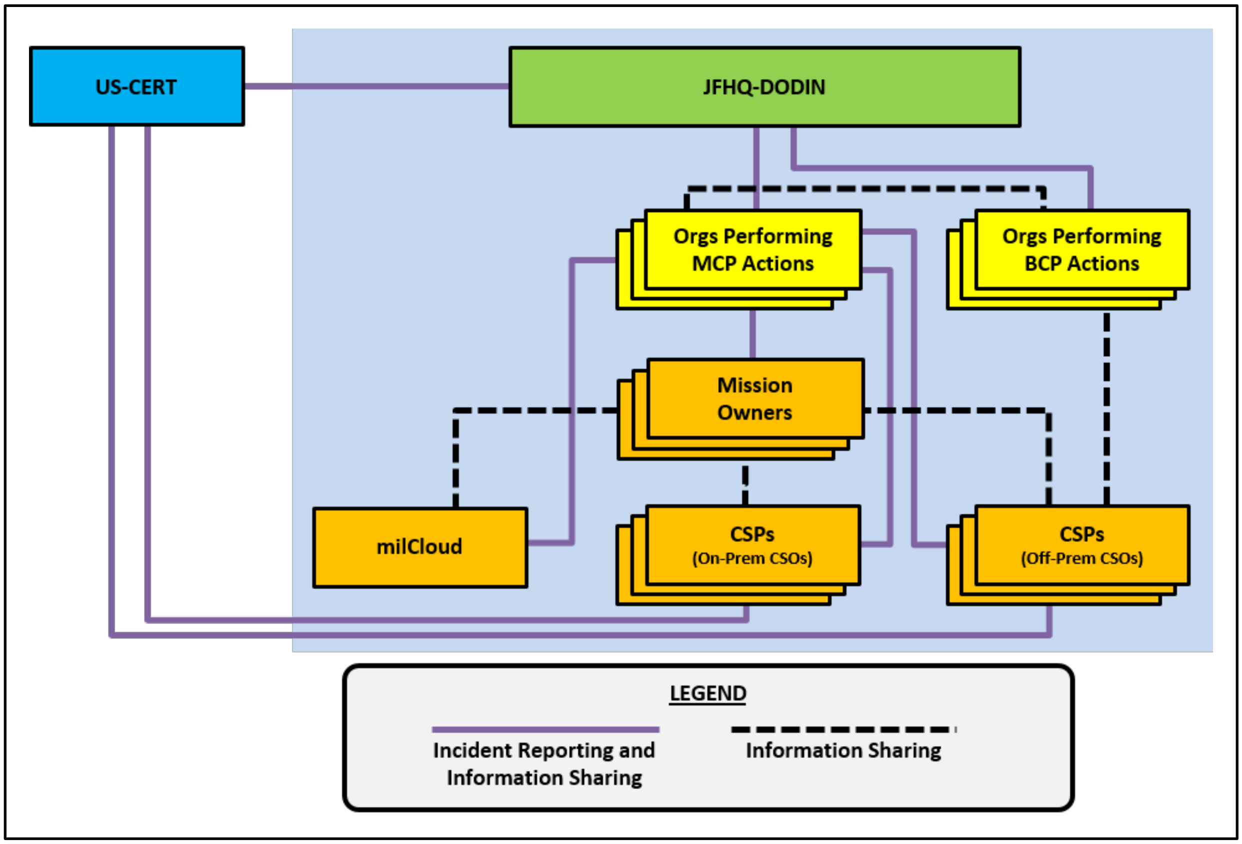


Figure 2 - DOD Cloud cyberspace protection information sharing model

The cloud protection information sharing model builds a comprehensive cyber situational awareness (SA) picture across the organizations providing BCP and MCP, JFHQ-DODIN, and the CSPs. Incident and event data is correlated at the JFHQ-DODIN to minimize duplication of effort, minimize miscommunication (e.g. different descriptions for “same” incident spanning multiple CSPs), improve responsiveness and enable greater proactive defense for the mission owners across all of the cloud services.

2.D. Cyberspace Protection Methodology

The desire for a consistent protection methodology to conduct analysis will require collaboration between the organizations providing BCP and MCP for some incidents and events. For example, advanced persistent threats (APTs) could attempt to target data hosted on premises, or use the applications and virtual servers hosted on off premises cloud services to attempt to access the DISN via the BCAP. In such instances, the organizations providing BCP and MCP would each hold part of the cyber SA picture that through collaboration would provide richer cyber SA and further enable an information-driven defense.

3. Cyber Event and Incident Response Matrix

Table 1 lists the DOD incidents and events and their associated response procedures. In addition, events of relevance for protection (e.g. Spillage/Unauthorized Disclosure, Annual Assessment) are listed with their response procedures. The subparagraphs that follow in this annex will introduce each of these procedures from Table 1, describing the event in a cloud service context and providing an overview of the procedure.

Table 1 – Cyber Event and Incident Response Matrix

DOD Category[4]	Function	Response and Protection Procedure
CAT 1 - Root Access CAT 2 - User Access	Respond	Response to Unauthorized Access or Intrusion
CAT 3 - Unsuccessful Activity Attempt	Respond	Response to Unsuccessful Activity Attempt
CAT 4 - Denial of Service (DoS)	Respond	Response to DoS
CAT 5 - Non-Compliance Activity	Respond	Response to Non-Compliance Activity
CAT 6 – Reconnaissance	Respond	Response to Reconnaissance
CAT 7 - Malicious Logic	Respond	Response to Malicious Logic
CAT 8 – Investigating	Respond	Initial Cloud Activity Assessment
CAT 9 - Explained Anomaly	Respond	Response to Explained Anomaly
CAT 0 - Training and Exercises	Respond	Response to Training and Exercises
Spillage or Unauthorized Disclosure	Respond	Response to Spillage or Unauthorized Disclosure
Vulnerability Scans	Protect	Performing vulnerability scans
Annual Assessments	Protect	Performing Annual External Assessments
Configuration Management (CM) and Patching	Protect	Performing CM and Patching
Planned Outage	Protect	Performing Planned Outage
Unplanned Outage	Respond	Response to Unplanned Outage
Disaster Recovery	Respond	Performing Disaster Recovery

[4] Reference (a): Chairman of the Joint Chiefs of Staff Manual 6510.01B "Cyber Incident Handling Program"

3.A. Initial Cloud Activity Assessment

The initial cloud activity assessment is invoked by procedures that are part of the initial investigation of a event or incident. The purpose of this procedure is to determine the extent of a event or incident, survey the impact, communicate findings to relevant organizations, and if needed initiate a response.

The initial cloud activity assessment is a self-standing response for DOD CAT 8 "Investigating" incidents. The organization that first identifies the incident must establish initial notification to provide SA to all cyberspace protection organizations and ensure that the incident is logged in the JIMS in accordance with the cyber incident handling program. Any incidents or events reported by commercial CSPs to DOD mission owners and organizations providing MCP regarding FedRAMP accredited CSOs must also be reported by the CSP to United States Computer Emergency Readiness Team (US-CERT).

Other procedures may first invoke an investigation phase by referencing the use of the initial cloud activity assessment as the first of many steps. For those procedures, the findings from the initial cloud activity assessment may be used to determine correct next steps. In such cases the procedures will branch based on findings.

If the incident or event impacts multiple organizations providing BCP and MCP, or cloud services, the JFHQ-DODIN will monitor the CSP response for SA.

If the CSP submits a situational awareness report[5], the recipient mission owner will post or distribute the situational awareness report to the organization providing MCP. If a CSP detects a event or incident that potentially affects DOD information confidentiality, integrity, or availability, information about the event or incident should be made available to the mission owner via a situational awareness report, who will post or distribute it to the organization providing MCP. Organizations providing MCP will share situational awareness reports with peer organizations providing MCP and BCP, and the JFHQ-DODIN to enable collaboration.

3.B. Response to Unauthorized Access and Intrusion

Three points of entry for unauthorized access and intrusion are of interest in a cloud service context.

a) Cloud-hosted mission: An intrusion into the DOD mission applications, systems or data residing on the cloud service.

b) DISN via BCAP: An intrusion that originates from outside the DISN and enters via the BCAP, possibly from a cloud-hosted application, system, or data with persistent access into the DISN via the BCAP.

c) CSO: An intrusion into the underlying cloud service management plane or infrastructure that may threaten the DOD mission applications, systems or data residing on the cloud service.

[5] Situational awareness reports are created and updated throughout the life of an incident. If a situational awareness report was issued any time before closure, an update will be issued to highlight lessons learned and countermeasures developed/implemented.

The organization providing MCP will detect, investigate, and respond in the case of (a), the organization providing BCP in the case of (b), and the CSP in the case of (c).

Unauthorized access or intrusion becomes relevant to the CSP if the incident or event occurs within the cloud service. Examples include:

- Below-hypervisor access or intrusion to an IaaS hosting DOD missions
- Mission cloud access or intrusion to services software that formulates the PaaS
- Web server intrusion to a SaaS hosting DOD missions, such as cross-site scripting (XSS) and SQL injections

In such instances the CSP will report the incident to the mission owner's organization providing MCP to initiate an investigation for possible DOD impact.

3.C. Response to Unsuccessful Activity Attempt

Unsuccessful activity attempts are events but not incidents, per the Cyber Incident Handling Program (Ref (a)). The organization providing MCP will be made aware of all suspicious unsuccessful activity attempts and will report them via JIMS.

3.D. Response to Denial of Service (DoS)

The primary factor in determining the appropriate response is to identify the Recovery Time Objective (RTO) of the impacted systems. The response will be different in the case of a DoS against an application with a RTO of 5 days (for example) vs. an application with an RTO of 1 hour. In addition, if mission owners are impacted by a coordinated event or incident then JFHQ-DODIN may coordinate the response across the organizations providing BCP and MCP.

3.E. Response to Non-Compliance Activity

Execute initial cloud activity assessment, Section 3.A.

3.F. Response to Reconnaissance

Identified reconnaissance are events but not incidents, per the cyber incident handling program, and therefore do not in themselves trigger JIMS reporting. Reconnaissance can occur against the BCAP, externally-hosted cloud services, or other targets. However, when it is determined by the detecting organization (whether by the organization providing MCP or BCP, or CSP) that reconnaissance events potentially affect DOD information confidentiality, integrity, or accessibility, the reconnaissance events will be reported via JIMS and information about the event will be made available by the detecting organization to the other organizations via a situational awareness report.

3.G. Response to Malicious Logic

Malicious logic (aka malware) can reside on a cloud solution of any delivery model: IaaS, PaaS, and SaaS. Malicious logic can infect operating systems, network devices, applications, or data files (e.g. PDF or MS Word files). In addition to traditional malware impact analysis, analysts will monitor for malware that specifically exploits the cloud infrastructure, software, or exploits the dedicated BCAP connections to the DISN.

3.H. Response to Explained Anomaly

An explained anomaly is an event caused by non-malicious activity, such as malfunctions or false alarms[6]. When it is determined by the detecting organization (whether by the organization providing MCP or BCP, or CSP) that the explained anomaly events potentially affect DOD information confidentiality, integrity, or accessibility, information about the events should be made available by the detecting organization to the other organizations via a situational awareness report.

3.I. Response to Spillage or Unauthorized Disclosure

Although not defined as a incident or reportable event, reporting spillage or unauthorized disclosure is still necessary for the maintenance of global cyber SA. Spillage[7] is defined as “Contamination of lower level networks with material of a higher classification.” The JFHQ-DODIN should be notified of any spillage or unauthorized disclosure of controlled unclassified information (CUI), personally identifiable information (PII), protected health information (PHI), or unclassified national security information (NSI) with an evaluation of impact not only to DODIN but also to national security and personnel.

Unauthorized disclosure includes:

- Transfer of information at a higher Information Impact Level than the cloud service is approved to (e.g. Impact Level 4 data on an Impact Level 2 CSO).
- Posting of information to an Impact Level 2 cloud service that has not been approved for public release (e.g. ITAR, PII, etc.).

The mission owner retains accountability for spillage and unauthorized disclosure remediation, whether the remediation process is executed by the mission owner or by the CSP. The steps taken depend on the configuration of the mission owner applications and data, the service level agreements (SLAs) in place for the cloud service, and the separations of authority for the systems on which the data resides. They will be carried out via the CSP’s data spill/unauthorized disclosure cleanup methods in accordance with (IAW) the Cloud Computing SRG[8], and reported as a Category 5 incident via JIMS. In the case of spillage of classified data, investigation, reporting, and remediation must be performed IAW the Cloud Computing SRG and DOD Manual 5200.01 Vol 3[9] or DOD 5400.11-R. In the case of spillage or unauthorized disclosure of PII or PHI, incident reponse must be performed IAW OMB M-17-12.

[6] Ref (a): Cyber Incident Handling Program, Section 2: Categories

[7] Ref (l): Chairman of the Joint Chiefs of Staff Instruction 6510.01F, Enclosure C, Section 29: Spillage of Classified Information

[8] Reference (d): Cloud Computing SRG Section 5.7 states, “CSP’s data spill cleanup methods will be evaluated as part of the PA assessment and then made available to all mission owners utilizing that CSP. The CSP will be responsible for executing any of those methods upon report of a data spill by a mission owner.”

[9] Ref (p): DOD Manual 5200.01 Vol 3 Enclosure 7 Section 5 on Classified Data Spills

3.J. Performing Vulnerability Scans

The CSP retains responsibility for vulnerability scans for the cloud service. The extent of mission owner responsibility for vulnerability scans varies with the cloud service model. For IaaS, the mission owner retains responsibility for vulnerability scans for mission systems and mission applications on the cloud service. For PaaS and SaaS, the mission owner retains responsibility to confirm the results of continuous monitoring by the CSP, which should be enforced through the SLA.

3.K. Performing Annual External Assessments

Requirements for annual external assessments (e.g. Red Team, Blue Team, Penetration Testing, etc.) extend to systems, applications, and data hosted on cloud service model. This includes IaaS, PaaS, and SaaS service delivery models. While the CSPs (both commercial and DOD) are responsible for continuous monitoring and regular assessment of their CSPs, mission owners (and their mission administrators) are separately assessed on the proper configuration and use of those service offerings.

In the case of a SaaS or PaaS, the mission owner may elect to inherit a portion of their security controls from the CSP. Such an agreement should be negotiated during CSO acquisition and reflected in the SLA. The mission owner will coordinate the external assessment with the CSP.

3.L. Performing Configuration Management (CM) and Patching

If the service offering is an IaaS, then the mission owner retains responsibility for CM and patching of all systems in their virtual data center (e.g. virtual servers, virtual networks, applications, etc.). For PaaS and SaaS, the mission owner retains responsibility to ensure that the CSP conducts continuous monitoring per contractual agreement. Although the mission owner is responsible for performing or ensuring CM and patching, the organizations providing MCP and BCP must maintain awareness of CM and patching operations. Depending on the features of the cloud service model it may be possible for the mission owner to automate CM and patching validation with, for example, Assured Compliance Assessment Solution (ACAS) feeds into a central repository, which would alter/simplify this procedure (e.g. cloud-hosted DODIN utility services). The mission owner will maintain up-to-date CM and patching documentation and share with the organization providing MCP so the organization can detect malicious changes to network and system configurations and settings.

3.M. Performing Planned Outage

An outage can be planned by the CSP or by the mission owner. The CSP may plan an outage for scheduled maintenance or upgrades. The CSP notifies the mission owner of the planned outage through a contractually agreed upon method. As the mission owner evaluates downtime impact to the mission, the mission owner is simultaneously encouraged to review the SLA to monitor the performance of the CSP against SLA commitments.

DOD planned outages can originate from multiple organizations. The obvious case is a mission owner-directed outage to upgrade systems. In the case of a mission owner, this pertains primarily to IaaS and possibly to PaaS (in the instance of custom software upgrades, for example). The planned outage, however, can be in response to a TASKORD or a need to perform maintenance on the BCAP. In all instances the mission owner (or mission administrator) notifies the CSP and the organization providing

MCP of the planned outage. The mission owner will determine if Continuity of Operations (COOP) or devolution procedures need to be initiated.

3.N. Response to Unplanned Outage

The response procedures assume communication from a CSP of an unplanned service outage, or the discovery thereof. The response to an unplanned outage is similar to the response to a DoS. The mission owner will determine if COOP or devolution procedures need to be initiated.

3.O. Performing Disaster Recovery

Execute established disaster recovery procedures to restore cloud-hosted functionality IAW SLA between Mission Owner and CSP or in the MOU/MOA/SLA between Mission Owner and MCP.

3.P. Response to Training and Exercises

Execute initial cloud activity assessment, Section 3.A.

4. CSPs Reporting to US-CERT

CSPs that report events or incidents via the online DIB[10] Cyber ICF will characterize the event or incident IAW the US-CERT Federal Incident Notification Guidelines[11], which is reflected in Table 2. Impacted organizations providing MCP will relay the incident reported in the DIB Network (DIBNET) Incident Reporting Tool by the CSP to JFHQ-DODIN via JIMS. Table 2 reflects those DOD categories that directly map to US-CERT categories. The other DOD categories (categories 1, 2, 3, 9, and 0) are not listed on the table; however, they can be used by DOD to identify the incident or event.

Table 2 – Mapping US-CERT Categories to DOD Categories

US-CERT Category	DOD Category
Any	CAT 6 - Reconnaissance
Attrition	CAT 4 - Denial of Service
Email	CAT 7 - Malware
External/Removable Media	CAT 7 - Malware
Impersonation/Spoofing	CAT 5 - Non-Compliance Activity
Improper Usage	CAT 5 - Non-Compliance Activity
Lost/Stolen Equipment	CAT 8 - Investigating
Other	CAT 8 - Investigating
Unknown	CAT 8 - Investigating
Web	CAT 7 - Malware

[10] Ref (d): DOD Cloud Computing SRG Section 6.4.3 “Incident Reporting Mechanism”

[11] Ref (m) is available at https://www.us-cert.gov/incident-notification-guidelines, including the Impact Classifications table, Threat Vectors table, and the Cause Analysis decision tree to aid in selecting the proper threat vector. This reporting method s with NIST SP 800-61 Rev 2.

ANNEX A: DOD COMPONENT RESPONSIBILTIES

A-1. Designate a DOD Component-level organization (e.g., cyber command, agency center, or office) to exercise authority and direction of organizations performing BCP and MCP functions for internal and external cloud services.

A-2. Identify to JFHQ-DODIN the designated DOD-Component-level organization controlling operations of assigned or external organizations providing BCP and MCP for cloud services, and mission owners.

A-3. Maintain inventory of all internal and external cloud services utilized by subordinate organizations; including DOD systems, applications, and data deployed in various cloud service models; and formal agreements (e.g., SLA, contract, memorandum of agreements, or other agreement) for cloud services.

A-4. Implement process and standard procedures and agreements to delineate organizational responsibilities and accountability between mission owners of the cloud services; systems, applications, and data; and organizations providing BCP and MCP.

A-5. Ensure the organizations providing BCP and MCP have authority to conduct cybersecurity activities and DCO internal defensive measures IAW DODI 8530.01.

A-6. Ensure clear organization and individual accountability for the use of cloud services and protection of DOD systems, applications and information.

ANNEX B: BOUNDARY CYBERSPACE PROTECTION (BCP) FUNCTIONS

B-1. BCP Introduction

The primary objective of organizations providing BCP is executing actions to protect the DISN from events or incidents that utilize public, community, private, and hybrid cloud services, through approved CSPs, that can impact the DISN through a dedicated connection via a BCAP. BCP actions support MCP in their objectives of protecting their systems, applications, and data hosted in the cloud services. In that capacity, BCP identifies broader patterns of events or actions across mission owners, cloud services, and CSPs. Organizations providing BCP support the JFHQ-DODIN by providing reports and information for events and incidents for further aggregation to ensure that the incidents are not DODIN-wide or isolated to a particular BCAP. BCP can help consolidate related incident tickets, recommend mitigations, and confirm technical aspect of TASKORD compliance by organizations providing MCP that is verifiable from the boundary. Each BCAP requires support from an organization for the performance of BCP.

B-2. Responsibilities of Organizations Providing BCP Functions

B-2.A. CSSP

B-2.A.1. Will be an organization that provides one or more cybersecurity services to implement and protect the DODIN authorized IAW DODI 8530.01.

B-2.A.2. Will be the performing CSSP for the BCAP.

B-2.A.3. Will assist with enabling cyberspace protection at the BCAP, to include:

a) Installing and maintaining sensors

b) Connect systems providing BCP capabilities, such as a Security Information and Event Management (SIEM) solution, to BCAP logs

c) Monitoring sensor and log feeds

B-2.B. Perform analysis for BCAP incidents and events.

B-2.B.1. Will protect the DODIN at the BCAP.

B-2.B.2. Will monitor data in transit through the BCAP based on BCAP sensing capabilities[12].

B-2.B.3. Will monitor for unauthorized connections (attempted and actual).

B-2.C. Will coordinate with organizations providing MCP on the status of JFHQ-DODIN directives and orders.

B-2.C.1. Pass warning intelligence to organization providing MCP, other organizations providing BCP, and the JFHQ-DODIN.

B-2.C.2. Maintain points of contact (POC) lists from the JFHQ-DODIN and organizations providing MCP for mission owners utilizing the supported BCAP.

B-2.C.3. Disseminate TIPRs from Intel sources.

[12] Ref (k) CAP Security FRD defines the sensing capabilities at the CAP

B-2.C.4. Generate and aggregate metric and trending data for the supported BCAP.

B-2.C.5. Provide aggregated metric and trending data for the supported BCAP to the JFHQ-DODIN.

B-2.C.6. Combatant command and Joint Cyber Center (JCC) SA coordination.

B-2.D. Will establish communication plans.

B-2.E. Will maintain POC lists

B-2.E.1. Maintain current contact lists for POCs at the JFHQ-DODIN, organizations providing BCP and MCP, mission owners, and CSPs for:

a) Cyber event and incident response reporting (see Figure 2), including: guidance, orders, and reporting

b) Coordination (see Figure 2), including situational awareness reports distribution and cyberspace protection data sharing

c) Distribution lists for situational awareness reports, plan of action and milestones (POA&Ms), external assessments (plans, reports, findings), vulnerability scan schedules, and outage notices

B-2.E.2. Maintain BCP organization POC list; distribute changes to POC list to the JFHQ-DODIN, peer organizations providing BCP, relevant organizations providing MCP, mission owners, and CSPs.

B-3. Organizations Providing BCP Cyber Incident and Event Procedures Responsibilities

B-3.A. Initial Cloud Activity Assessment

B-3.A.1. Notify the JFHQ-DODIN if incidents are being reported with regard to multiple mission owners or CSPs.

B-3.A.2. Document the incident in JIMS. If the boundary impact is unknown, the incident is categorized as a CAT 8 “Investigating” incident.

B-3.A.3. Report incident to the JFHQ-DODIN for DOD CAT 1, 2, 4; CAT 3’s and 7’s as required per Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01B[13].

B-3.A.4. Consult and advise the JFHQ-DODIN to coordinate orders, as needed.

B-3.A.5. Notify impacted organizations providing MCP via situational awareness report.

B-3.A.6. Execute JFHQ-DODIN distributed TASKORDs.

B-3.A.7. Cooperate post intrusion, with the organizations providing BCP and MCP to support return to normal operations. If for example a server is compromised and the cloud and network is restored to a secure state[14], the organization(s) providing BCP and MCP should be monitoring to ensure that responses to eliminated adversaries were effective.

[13] Ref (a): Cyber Incident Handling Program

[14] Per CNSSI-4009, Secure State is the “condition in which no subject can access any object in an unauthorized manner.”

B-3.B. Response to Unauthorized Access and Intrusion

B-3.B.1. Execute initial cloud activity assessment, Section B-3.A.

B-3.B.2. If organization providing BCP finds no incident as a result of initial cloud activity assessment:

a) Close out JIMS as a Cat 9/report no incident to JFHQ-DODIN.

b) Update situational awareness report and send it to MCP.

c) Stop this procedure at this step.

B-3.B.3. If organization providing BCP discovers unauthorized access or intrusion:

a) Identify and document if access attempted misuse of DOD PKI certificates, DOD privileged credentials, cloud service or application management plane privileged credentials, or other privileges.

b) Identify and document if incident originated from DODIN, external internet, or the cloud service.

c) Notify organization providing MCP via situational awareness report

d) Transfer JIMS ticket to organization providing MCP and confirm update to category (e.g. CAT 1, CAT 2, etc.).

B-3.C. Response to Unsuccessful Activity Attempt

B-3.C.1. If the event is identified by the CSP, mission owner, or organization providing MCP then the organization providing BCP will receive situational awareness report from organization providing MCP.

B-3.C.2. If the event is identified by the organization providing BCP, then develop the situational awareness report and distribute to applicable organizations providing MCP.

B-3.C.3. Determine need, if any, for preventative countermeasures at the BCAP or IAP.

B-3.D. Response to DoS

B-3.D.1. Execute initial cloud activity assessment, Section 19B-3.A.

B-3.D.2. If DoS event or incident impacts DODIN via BCAP, document the incident in JIMS.

B-3.D.3. Determine need, if any, for preventative countermeasures at the BCAP or IAP.

B-3.D.4. Notify impacted organizations providing MCP and the JFHQ-DODIN via situational awareness report.

B-3.D.5. The JFHQ-DODIN may distribute TASKORDs to organizations providing BCP and MCP per initial cloud activity assessment. All TASKORDs distributed by the JFHQ-DODIN will be executed by organizations providing BCP and MCP.

B-3.E. Response to Non-Compliance Activity

B-3.E.1. Execute initial cloud activity assessment, Section B-3.A.

B-3.E.2. Notify relevant organizations providing MCP of non-compliance activity.

B-3.E.3. If impact to mission owner, notify organization providing MCP via situational awareness report and document in JIMS ticket. Track to resolution.

B-3.F. Response to Reconnaissance

B-3.F.1. If signs of unauthorized access cannot be determined/validated by evaluating sources of reconnaissance:

a) Investigate reported event or incident for DODIN boundary impact.

b) Develop a situational awareness report.

c) Distribute situational awareness report to the JFHQ-DODIN, peer organizations performing BCP, and applicable organizations performing MCP and CSPs (within classification constraints).

B-3.F.2. If the reconnaissance event is identified by the organization performing BCP, the organization:

a) Develops a situational awareness report.

b) Distributes the situational awareness report to the JFHQ-DODIN, peer organizations performing BCP, and applicable organizations performing MCP and CSPs (within classification constraints).

B-3.F.3. Determine source or cause of reconnaissance for signs of unauthorized access or malware.

a) If unauthorized access is detected, refer to the relevant procedure respective to organizations providing BCP, MCP, or mission owner, Section 3.B: Response to Unauthorized Access and Intrusion.

b) If malware is detected, refer to Section B-3.G: Response to Malicious Logic.

c) Update situational awareness report and resend.

B-3.F.4. Determine need, if any, for preventative countermeasures at the BCAP.

B-3.G. Response to Malicious Logic

B-3.G.1. Malware may be identified in the course of ongoing monitoring or in response to an organization providing MCP. If the organization providing BCP identifies the malware, the organization providing BCP notifies applicable organization providing MCP and the JFHQ-DODIN. The organization providing MCP will open a CAT 7 JIMS ticket.

B-3.G.2. The JFHQ-DODIN may distribute TASKORD to organizations providing BCP and MCP. All TASKORDs distributed by the JFHQ-DODIN will be executed by BCPs and MCPs.

B-3.H. Response to Explained Anomaly

B-3.H.1. Execute initial cloud activity assessment, Section B-3.A.

B-3.H.2. Implement process or tool update to reduce occurrence of explained anomaly, if possible.

B-3.I. Response to Spillage or Unauthorized Disclosure

B-3.I.1. If the organization providing BCP identifies the spillage or unauthorized disclosure, the organization providing BCP notifies organization providing MCP of impacted mission owner.

B-3.I.2. The organization providing BCP supports the organization providing MCP investigation and response to spillage or unauthorized disclosure to closure.

B-3.J. Performing Vulnerability Scans

B-3.J.1. Receive vulnerability scan schedule from the organization providing MCP.

B-3.J.2. Support mission owner during vulnerability scans (e.g. modify alert or response posture during vulnerability scans period).

B-3.K. Performing Annual External Assessments.

B-3.K.1. Receive notification of external assessment type and period from organization providing MCP.

B-3.K.2. Receive a full report of findings and recommendations from the organization providing MCP after the assessment is complete.

B-3.L. Performing Configuration Management (CM) and Patching

B-3.L.1. Receive notice from organization providing MCP of patch schedule/outage.

B-3.L.2. Receive notice of restoration of service and success of patch deployment from organization providing MCP.

B-3.L.3. Receive updated CM and patching documentation via the organization providing MCP.

B-3.M. Performing Planned Outage

B-3.M.1. Receive notice from organization providing MCP of outage schedule.

B-3.M.2. Receive notice from organization providing MCP after restoration of service.

B-3.N. Response to Unplanned Outage

B-3.N.1. Receive notice from organization providing MCP of outage and impact.

B-3.N.2. Track outages to closure.

B-3.O. Performing Disaster Recovery

B-3.O.1. Assist organization providing MCP and mission owner in executing disaster recovery procedures to restore cloud-hosted functionality for off premises cloud services via BCAP.

B-3.P. Response to Training and Exercises

B-3.P.1. Execute initial cloud activity assessment, Section B-3.A.

ANNEX C: MISSION CYBERSPACE PROTECTION (MCP) FUNCTIONS

C-1. MCP Introduction

The primary function of organizations that perform MCP actions is to protect mission owners' systems, applications, and data hosted in cloud services. The organization providing MCP protects all connections to the cloud services whether via BCAP, VPN, IAP, direct internet access to public servers, or other. The organization providing MCP monitors privileged actions (e.g. cloud management or mission owner application administration) and monitors for events or incidents against the mission owner applications (e.g. SQL injection). The organization providing MCP supports the organizations providing BCP when the mission owner uses a BCAP. MCP actions are performed by CSSPs on behalf of their organic organizations and subscribers.

C-2. Responsibilities of Organizations Providing MCP Functions

C-2.A. <u>CSSP</u>

C-2.A.1. Will be a DOD Component or authorized external DOD Component service provider that provides one or more cybersecurity services to implement and protect the DODIN[15].

C-2.A.2. Will be the performing CSSP for the mission owner

C-2.A.3. Will assist mission owners with enabling protection, to include:

a) Install and maintain sensors.

b) Connect systems providing MCP capabilities (e.g. SIEM) to logs from mission owner and cloud service systems.

c) Monitor sensor and log feeds.

d) Monitor for CSP communications via DIB Cyber Incident Reporting tool (for commercial CSPs).

C-2.B. <u>Perform analysis for cloud service incidents/events.</u>

C-2.B.1. Will detect cloud service events and analyze CSP incidents.

C-2.B.2. Will map events reported by commercial CSPs via US-CERT guidelines or DIB Cyber Incident Reporting tool to DOD cyber event and incident categories (see Table 1) and input into JIMS.

C-2.B.3. Will monitor JIMS for events impacting cloud services.

C-2.C. Distribute <u>situational awareness report</u> to the JFHQ-DODIN and organizations providing BCPs for Attack Sensing & Warning (AS&W)/<u>situational awareness report</u>.

C-2.D. Distribute guidance and orders (patch management) to mission owners.

C-2.E. Report events and incidents via JIMS.

[15] Ref (c) DOD Instruction 8530.01 Glossary

C-2.F. Identify inconsistencies and inaccuracies in the results provided by CSP vulnerability assessments and inform mission owners.

C-2.G. Will retain copy of the mission owner's SLA with CSP; should ensure mission owner has proper DOD-approved cloud service SLA.

C-2.G.1. Provide placement locations for sensors (if appropriate).

C-2.G.2. Assist with installation and feeds to systems providing MCP capabilities.

C-2.G.3. Perform and assist with external assessments.

C-2.G.4. Confirms setup of Host Based Security System (HBSS), ACAS, Continuous Monitoring and Risk Scoring (CMRS), and any other security capabilities as applicable.

C-2.H. Will maintain POC lists

C-2.H.1. Maintain current contact lists for POCs at the JFHQ-DODIN, organizations performing BCP, mission owner, and CSPs for:

a) Event and incident response reporting, including: guidance, orders and reporting

b) Coordination including situational awareness reportsdistribution and information sharing

c) Distribution lists for situational awareness reports, POA&Ms, external assessments (plans, reports, findings), vulnerability scans schedules, and outage notices

C-2.H.2. Maintain POC list; distribute changes to POC list to the JFHQ-DODIN, relevant organizations providing BCP actions, peer organizations providing MCP actions, mission owners, and CSPs.

C-3. Organizations Providing MCP Cyber Incident and Event Procedures Responsibilities

C-3.A. Initial Cloud Activity Assessment

C-3.A.1. Document the incident in JIMS. If mission owner impact is unknown, the incident is categorized as a CAT 8 "Investigating" incident.

C-3.A.2. Notify organization providing BCP.

C-3.A.3. Execute JFHQ-DODIN distributed TASKORDs.

C-3.B. Response to Unauthorized Access / Intrusion

C-3.B.1. Execute initial cloud activity assessment, Section C-3.A.

C-3.B.2. If organization providing MCP finds no incident as a result of initial cloud activity assessment:

a) Close out JIMS Cat 9/report no incident to the JFHQ-DODIN via situational awareness report; share with organizations providing BCP.

b) Send update to mission owner.

c) Stop this procedure at this step.

C-3.B.3. If the organization providing MCP finds DOD impact as a result of initial cloud activity assessment:

a) Update JIMS ticket to proper category (e.g. CAT 1; CAT 2).

b) Note if access attempted misuse of DOD PKI certificates, DOD privileged credentials, cloud service or application management plane privileged credentials, or other privileges IAW CJCSM 6510.01B.

c) Note if incident originated from DODIN, external internet, or the cloud service.

d) Notify the JFHQ-DODIN via situational awareness report; share with organizations providing BCP.

e) Notify mission owner via situational awareness report. If appropriate, notify CSP.

C-3.B.4. Execute JFHQ-DODIN distributed TASKORDs.

C-3.B.5. Send update to mission owner via situational awareness report. If appropriate, notify CSP.

C-3.C. <u>Response to Unsuccessful Activity Attempt</u>

C-3.C.1. Distribute the situational awareness report identifying event received from an organization providing BCP or CSP to the mission owners. If the cloud service is a PaaS or SaaS, the notice may come from the mission administrators. If so, organization providing MCP requests logs from mission administrators (who may, depending on SLAs, acquire them from the CSP).

C-3.C.2. If the event is identified by the mission owner or MCP, then the MCP distributes situational awareness report identifying an event received from the mission owner or the organization providing MCP. Direct changes by mission owners or request changes by organization providing BCP or CSP.

C-3.C.3. Determine need, if any, for preventative countermeasures on the mission data, cloud service, or connection configuration to the CSP, and direct changes by the mission administrators or request changes by the organization providing BCP or CSP.

C-3.D. <u>Response to DoS</u>

C-3.D.1. Execute initial cloud activity assessment, Section C-3.A.

C-3.D.2. Document the incident in JIMS, if DoS event or incident impacts mission owner,

C-3.D.3. Determine need, if any, for preventative countermeasures at the BCAP, virtual network devices hosted in the cloud service, or any other connections to the CSO.

C-3.D.4. Notify organization providing BCP via situational awareness report.

C-3.D.5. Report status of TASKORDs to the JFHQ-DODIN. The JFHQ-DODIN may distribute orders to organization providing MCP per initial cloud activity assessment, Section C-3.A.

C-3.E. <u>Response to Non-Compliance Activity</u>

C-3.E.1. Execute initial cloud activity assessment, Section C-3.A.

C-3.E.2. Notify mission owners of non-compliance activity; share with the JFHQ-DODIN and relevant organization providing BCP.

C-3.E.3. Document impact in JIMS; if impact to boundary, notify organization providing BCP via situational awareness report.

C-3.F. <u>Response to Reconnaissance</u>

C-3.F.1. If the organization providing MCP is notified of a reconnaissance event or incident by

CSP, organization providing BCP, or other:

a) Investigate reported event or incident for mission owner impact.

b) Develop a situational awareness report and distribute to mission owner, the JFHQ-DODIN, organization providing BCP, and CSP.

C-3.F.2. If the reconnaissance event is identified by the mission owner or organization providing MCP:

a) Develop a situational awareness report.

b) Distribute situational awareness report to mission owner, the JFHQ-DODIN, organization providing BCP, and CSP.

C-3.F.3. Determine source or cause of reconnaissance for signs of unauthorized access or malware.

a) If unauthorized access or malware is discovered, refer to those procedures.

b) Update situational awareness report and resend.

C-3.F.4. Determine need, if any, for preventative countermeasures on the mission owner systems, applications, cloud service, or connection configuration to the CSP, and direct changes by the mission owner or request changes by the organization providing BCP or CSP.

C-3.G. <u>Response to Malicious Logic</u>

C-3.G.1. Malware may be identified in the course of ongoing monitoring or in response to an organization providing BCP TIPR.

a) Notify CSP for awareness. If malware is detected, open JIMS ticket (CAT 7).

b) Investigate and report to JFHQ-DODIN with copies to organization providing BCP and CSP, if MCP is notified of a malware impact assessment (e.g. by organization providing BCP or triggered by identified malware on another mission owner system).

C-3.G.2. Support consolidating tickets at the direction of the JFHQ-DODIN, if the JFHQ-DODIN determines multi-mission owner impact.

C-3.G.3. Execute JFHQ-DODIN distributed TASKORDs.

C-3.G.4. Close ticket, if MCP still owns the JIMS ticket.

C-3.H. <u>Response to Explained Anomaly</u>

C-3.H.1. Execute initial cloud activity assessment, Section C-3.A.

C-3.H.2. Implement process or tool update to reduce occurrence of Explained Anomaly, if possible.

C-3.I. <u>Response to Spillage or Unauthorized Disclosure</u>

After organization providing MCP identifies or receives notice of a spillage/unauthorized disclosure:

C-3.I.1. Report spillage or unauthorized disclosure via situational awareness report to the JFHQ-DODIN; copy relevant organization providing BCP.

C-3.I.2. Support mission owner and CSP in the spillage or unauthorized disclosure investigation and remediation.

C-3.I.3. Periodically update the JFHQ-DODIN and relevant organization providing BCP for SA.

C-3.I.4. Notify the JFHQ-DODIN and relevant organization providing BCP of completion via updated situational awareness report when mission owner reports completion.

C-3.J. Performing Vulnerability Scans

C-3.J.1. Receive notice of vulnerability scans schedule from mission owner.

C-3.J.2. Share vulnerability scans schedule with the JFHQ-DODIN and organization providing BCP.

C-3.J.3. Receive results and POA&M from mission owner after performance of vulnerability scans.

C-3.J.4. Confirm reporting of compliance with USCYBERCOM per TASKORD.

C-3.J.5. Report POA&M to JFHQ-DODIN; share with organization providing BCP.

C-3.K. Performing Annual External Assessments

C-3.K.1. Coordinate mission owner request type (e.g. Red Team, Blue Team, Penetration Testing, etc.).

a) Evaluate capabilities required to perform requested external assessment and compare against current capability and capacity.

b) Share plan with organization providing BCP and the JFHQ-DODIN of type and period of assessment.

c) Confirm notification to CSP via mission owner.

C-3.K.2. Conduct coordination for requested assessment, if capable and follow reporting requirements per defined deconfliction process with the JFHQ-DODIN.

C-3.K.3. Send request to the JFHQ-DODIN, if the organization providing MCP cannot perform requested assessment.

C-3.K.4. Perform the assessment, provide a full report of findings and recommendations to the requesting mission owner and the JFHQ-DODIN; share report with organization providing BCP.

C-3.K.5. Receive remediation plan and POA&Ms from mission owner.

C-3.L. Performing Configuration Management (CM) and Patching

C-3.L.1. Receive notice from mission owner of patch schedule and outage.

C-3.L.2. Notify the JFHQ-DODIN and applicable organization providing BCP of patch schedule and outage.

C-3.L.3. Ensure after CM and patching is complete, mission owner reports restoration of service and success of patch deployment to organization providing MCP and the JFHQ-DODIN per orders process.

C-3.L.4. Notify the JFHQ-DODIN and BCP of restoration of service.

C-3.M. Performing Planned Outage

C-3.M.1. Receive notice from mission owner of outage schedule and notify the JFHQ-DODIN of outage schedule; share schedule with organization providing BCP.

C-3.M.2. Notify organization providing BCP of schedule updates or anomalies during execution.

C-3.M.3. Receive notice from mission owner after restoration of service.

a) Notify the JFHQ-DODIN of service restoration; share with organization providing BCP.

b) Provide updated CM and patching documentation to organization providing BCP.

C-3.N. <u>Response to Unplanned Outage</u>

C-3.N.1. Coordinate with mission owner to assess impact.

C-3.N.2. Report outage and impact to JFHQ-DODIN; share outage and impact information to relevant organization providing BCP.

C-3.N.3. Track status with mission owner and CSP until closure or resolution.

C-3.N.4. Provide periodic updates to JFHQ-DODIN until closure/resolution; share with relevant organization providing BCP.

C-3.O. <u>Performing Disaster Recovery</u>

C-3.O.1. Assist mission owner upon request in executing disaster recovery procedures to restore cloud-hosted functionality.

C-3.P. <u>Response to Training and Exercises</u>

C-3.P.1. Execute initial cloud activity assessment, Section C-3.A.

ANNEX D: MISSION OWNER

D-1. Mission Owner Introduction

A mission owner operates, and maintains the mission systems, applications, and data depending on cloud model (e.g. IaaS, PaaS, or SaaS). In this capacity, a mission owner is a DOD entity that acquires cloud services and dedicated connections in support of its mission. Per the DOD Cloud Computing SRG, a mission owner requires support from an organization providing MCP actions, and provides endpoint protection functions.

The Cloud Computing SRG defines the mission administrators and the mission owners as separate roles. Per the DOD Cloud Computing SRG, mission owners are individuals and organizations responsible for the overall mission environment, ensuring that the functional requirements of the system are being met. Mission owners are minimally responsible for:

- Engaging and funding organizations providing MCP to provide for the protection of the mission owner's systems, applications, and virtual networks in any CSP's IaaS or PaaS infrastructure (whether DOD operated or operated by a commercial/non-DOD entity).
- Negotiating the terms and requirements with the CSP for incident reporting and incident response, in coordination with the organizations providing BCP and MCP.
- Coordinating access for organizations providing BCP and MCP required.

Mission administrators are the administrators of mission owner's Cloud-based systems, applications, and virtual networks. They are minimally responsible for:

- Following directions of JFHQ-DODIN and organizations providing MCP.
- Installing and maintaining protective measures for the cloud-based mission systems, applications, and virtual networks
- For IaaS: maintaining and patching the cloud-based mission systems, applications, and virtual networks; configuring the virtual environment and access to it.
- For PaaS: maintaining and patching cloud-based mission applications; configuring the PaaS applications as appropriate and configuring access to the supported applications.
- For SaaS: configuring access to the supported applications.

D-2. Mission Owner Responsibilities

The mission owner designates a mission administrator, a person or group with technical responsibility for the configuration of the cloud service, commensurate with the cloud service model being used. The Mission Owner is to ensure that the CSP is made aware of and adheres to, as part of their contract, the applicable CSP responsibilities according to their CSO listed in Annex E and Annex F of this guide. The mission owner requires support from an organization providing MCP support. To enable the designated organization providing MCP, mission owners:

D-2.A. Will provide to the organization providing MCP:

D-2.A.1. Architecture drawings.

a) Physical and logical.

b) System descriptions (IP address, system name, description, operating system versions, list of expected protocols, configurations, etc.).

D-2.A.2. Mission owner POCs' information to be used by the organization providing MCP to request information or issue directives or orders.

D-2.A.3. Copies of SLA to the organization providing MCP.

D-2.B. Will Establish the Secure Logical Connection

D-2.B.1. For a dedicated connection to the CSO, request connection through a BCAP.

D-2.B.2. Provide CSP list of authorized connections.

D-2.B.3. Through CSP, confirm unauthorized attempts to connect to CSO are refused.

D-2.C. Will maintain a POC list.

D-2.C.1. Maintain current contact lists for POCs at organizations providing MCP and BCP , and CSP for:

a) Event and incident response reporting, including guidance, orders, and reporting.

b) Cyberspace protection coordination, including situational awareness reports distribution and information sharing.

c) Distribution lists forsituational awareness reports, POA&Ms, external assessments (plans, reports, and findings), vulnerability scan schedules, and outage notices.

D-2.C.2. Maintain mission owner POC list; distribute changes to POC list to organizations providing MCP, and BCP, and the CSP.

D-2.C.3. The CSP will maintain a current CSP Technical POC list, which the mission owner will provide to the relevant organizations providing MCP and BCP.

D-2.D. Will Establish Communication Plans

D-2.D.1. Add the organization providing MCP and BCP for off premises cloud services to Trusted Disclosure list in SLA.

D-2.D.2. Notify the organization providing MCP and CSP of maintenance windows.

D-2.D.3. Notify the organization providing MCP and CSP of Periods of Non-Disruption (PONDs)

D-2.D.4. In the case of a cloud service outage (planned or unplanned), the mission owner will report the outage or plan for outage to the organization providing MCP.

D-2.D.5. Establish plan for providing updates to open vulnerability POA&M to the organization providing MCP.

D-2.D.6. Incorporate situational awareness report communication requirements into SLA.

D-2.E. Will Prepare Mission Owner Data for Cyberspace Protection

D-2.E.1. Ensure coordination of scan results with CSP is incorporated into SLA

D-2.E.2. Ensure proper operation and maintenance (O&M) for applications.

D-2.E.3. Ensure compliance with security technical implementation guides (STIGs).

D-2.E.4. Comply with placement of sensors from the organization providing MCP.

D-2.E.5. Ensure feeds of host protection tools to the organization providing MCP.

D-2.E.6. Install host protection tools (e.g. HBSS, ACAS).

D-2.F. Incident Response Plan

D-2.F.1. Ensure CSP data spill cleanup method is incorporated into SLA.

D-2.F.2. Ensure CSP incident response plan is incorporated into SLA, including:

a) Communication plans

b) Thresholds for reporting

c) Requirement to comply with designated organization providing MCP

D-2.G. Review SLA every six months for potential updates (e.g. POCs, etc.).

D-3. Mission Owner Cyber Event and Incident Procedures Responsibilities

D-3.A. Initial Cloud Activity Assessment

D-3.A.1. Mission owner notifies the organization providing MCP of the suspected event or incident.

D-3.A.2. The mission owner will support any assessments requested by the organization providing MCP. This may be in relation to a TASKORD issued by JFHQ-DODIN to the organization providing MCP.

D-3.B. Response to Unauthorized Access or Intrusion

D-3.B.1. Execute mission owner initial cloud activity assessment, Section D-3.A.

D-3.B.2. The mission owner will support remediation actions as directed by the organization providing MCP in support of JFHQ-DODIN TASKORDs or unauthorized accesses and intrusions identified by the organization providing MCP.

D-3.C. Response to Unsuccessful Activity Attempt

D-3.C.1. If the event is identified by the mission owner, the mission owner notifies the organization providing MCP.

D-3.C.2. Support the development of a situational awareness report by organization providing MCP.

D-3.C.3. The mission owner will support preventative actions as directed by the organization providing MCP in support of the JFHQ-DODIN TASKORDs or unsuccessful activity attempt identified by the organization providing MCP.

D-3.D. Response to DoS

D-3.D.1. Execute mission owner initial cloud activity assessment, Section D-3.A.

D-3.D.2. The mission owner will support DoS courses of action as directed by the organization providing MCP in support of either JFHQ-DODIN TASKORDs or DoS activity identified by the organization providing MCP.

D-3.E. Response to Non-Compliance Activity

D-3.E.1. Execute mission owner initial cloud activity assessment, Section D-3.A.

D-3.E.2. The mission owner will implement non-compliance activity courses of action as directed by the organization providing MCP in support of JFHQ-DODIN TASKORDs or non-compliance activity identified by the organization providing MCP.

D-3.F. Response to Reconnaissance

D-3.F.1. Notify the organization providing MCP.

D-3.F.2. Support the development of a situational awareness report by the organization providing MCP.

D-3.F.3. Support the organization providing MCP effort to determine source or cause of reconnaissance for signs of unauthorized access or malware.

D-3.F.4. The organization providing MCP will determine the need, if any, for preventative countermeasures on mission owner systems. Mission owner applications, cloud service, or connection configuration to the CSP. Mission owner will comply with prescribed preventative countermeasures.

D-3.G. Response to Malicious Logic

D-3.G.1. Execute mission owner initial cloud activity assessment, Section D-3.A. In notification to organization providing MCP, note extent of impact (if any).

D-3.G.2. The mission owner will support malicious logic courses of action as directed by the organization providing MCP in support of JFHQ-DODIN TASKORDs or malicious logic identified by the organization providing MCP.

D-3.H. Response to Explained Anomaly

D-3.H.1. Execute initial cloud activity assessment, Section D-3.A.

D-3.H.2. If possible, implement process or tool update to reduce occurrence of explained anomaly.

D-3.I. Response to Spillage and Unauthorized Disclosure

D-3.I.1. Notify the organization providing MCP of spillage or unauthorized disclosure.

D-3.I.2. Organization providing MCP will report spillage or unauthorized disclosure via situational awareness report to the JFHQ-DODIN.

D-3.I.3. Remediate spillage or unauthorized disclosure IAW JFHQ-DODIN orders.

D-3.I.4. When complete, report closure to the organization providing MCP.

D-3.J. Providing Vulnerability Scans

D-3.J.1. Mission owner provides vulnerability scans and is responsible for reporting compliance to USCYBERCOM per TASKORD.

D-3.J.2. Mission owner creates POA&M.

D-3.J.3. Mission owner reports results compliance results, POA&Ms, open items to the organization providing MCP.

D-3.K. Providing Annual External Assessments

D-3.K.1. Coordinate request type (e.g. Red Team, Blue Team, Penetration Testing, etc.) with the organization providing MCP and the CSP.

D-3.K.2. Receive a full report of findings and recommendations from the organization that provides the assessment.

D-3.K.3. Report to the organization providing MCP on remediation plans, including applicable POA&Ms.

D-3.L. Providing CM and Patching

The following steps pertain to mission owners utilizing IaaS or PaaS.

D-3.L.1. Mission owner receives requirement to patch systems/apps (is accountable for compliance).

D-3.L.2. Mission owner acquires or develops patch.

D-3.L.3. Mission owner tests patch.

a) Mission owner follows configuration control board (CCB) process as defined by its component to ensure that any patches implemented do not adversely affect the functionality of the cloud-hosted systems and cloud service.

b) If outage is required, follow the planned outage for DOD to CSP and DOD authorized service interruption (ASI) process.

c) Validate operations.

D-3.L.4. Mission owner notifies the organization providing MCP of patch schedule and outage.

D-3.L.5. Mission owner applies the patch.

D-3.L.6. Mission owner reports restoration of service and success of patch deployment to the organization providing MCP and JFHQ-DODIN per orders process.

D-3.L.7. Mission owner provides updated CM and patching documentation to the organization providing MCP.

D-3.M. Providing Planned Outage

D-3.M.1. If the planned outage is initiated by the DOD organization.

a) Mission owner plans outage.

b) Mission owner notifies CSP.

c) Mission owner notifies the organization providing MCP of planned outage, including if COOP or devolution procedures are required.

d) At conclusion of planned outage, the mission owner notifies the organization providing MCP and CSP of restoration of service.

D-3.M.2. If the planned outage is initiated by the CSP.

a) Mission owner will be notified of planned outage by the CSP through a contractually agreed upon method.

b) Mission owner notifies the organization providing MCP.

D-3.M.3. Mission owner notifies the organization providing MCP and the CSP if COOP or devolution procedures were initiated.

D-3.N. Response to Unplanned Outage

D-3.N.1. Mission owner notifies the organization providing MCP and CSP of unplanned outage.

D-3.N.2. Mission owner notifies the organization providing MCP and the CSP if COOP or devolution procedures were initiated.

D-3.N.3. Mission owner supports the organization providing MCP impact assessment.

D-3.N.4. Mission owner updates CSP until closure or resolution; tracks status.

D-3.O. Providing Disaster Recovery

D-3.O.1. Mission owner notifies the organization providing MCP and CSP of initiation of disaster recovery procedures.

D-3.O.2. Execute disaster recovery procedures to restore cloud-hosted functionality.

D-3.P. Response to Training and Exercises

D-3.P.1. Execute mission owner initial cloud activity assessment, Section D-3.A.

ANNEX E: CSP

E-1. CSP Introduction

A CSP is responsible for the maintenance and operation of the cloud services that are procured, as specified in the contractual agreement, and used by mission owners. A CSP can be a commercial vendor or a Federal organization that provides cloud services for mission owner use. The scope of responsibility of a CSP for the protection of mission owner applications and mission owner data depends on the service delivery model used (IaaS, PaaS, or SaaS). A CSP provides services for their infrastructure and cloud service model provided. This complements the organization providing MCP for the mission owner applications and data residing on a CSP's infrastructure and cloud service model provided.

Per the DOD Cloud Computing SRG, all DOD information and data placed or created in a CSP's cloud service is owned by the DOD mission owner and information owner unless otherwise stipulated in a CSP's contract with the DOD organization[16].

CSP reporting channels will be different for cloud services under FedRAMP vs. DOD PA. All Level 2/4/5 Commercial CSPs will report all incidents via the online DIB Cyber ICF[17]. These and additional requirements for a CSP must be specified in the SLAs covering the relationships between a CSP and each of the mission owners.

A CSP is under contractual control of the mission owner. Via this relationship, a CSP is expected to support and comply with efforts to resolve issues under the direction of the mission owner.

E-2. CSP Responsibilities

The CSP will adhere to the applicable responsibilities as specified in the contractual agreement with the mission owner. The mission owner, through the contractual agreement, will ensure the CSP:

E-2.A. Provides to the mission owner

E-2.A.1. A copy of the SLA.

E-2.A.2. Assistance in developing future automated capabilities that could increase efficiencies.

E-2.A.3. A current CSP Technical POC list.

E-2.A.4. Vulnerability scan results and POA&M.

[16] Reference (d): DOD Cloud Computing SRG Section 5.5.2 states, "All DOD information and data placed or created in a CSP's cloud service is owned by the DOD mission owner and information owner unless otherwise stipulated in the CSP's contract with the DOD organization. The CSP has no rights to the DOD's information and data. DOD information and data includes logs and monitoring data created within a mission owner's system and application implemented in IaaS or PaaS. CSPs seeking a DOD PA must agree that DOD remains the owner of all DOD data in a cloud service. CSPs are prohibited from using DOD data in any way (e.g., for data mining) other than that required to provide contracted services to DOD (e.g., customer access/usage logs used for billing)."

[17] Ref (d): DOD Cloud Computing SRG Section 6.4.3 "Incident Reporting Mechanism"

E-2.B. Maintains a POC list

E-2.B.1. Maintain current lists of POCs at US-CERT, mission owners, and relevant the organizations providing MCP and BCP:

a) Event and incident response reporting including: guidance, orders and reporting.

b) Cyberspace protection coordination, including situational awareness reports distribution and data sharing.

c) Distribution lists for situational awareness reports, POA&Ms, external assessments (plans, reports, and findings), vulnerability scan schedules, and outage notices.

E-2.B.2. Maintain CSP POC list with every POC change, distribute changes to POC list to JFHQ-DODIN, the relevant organizations providing BCP and MCP, and relevant mission owners.

E-2.B.3. Email the mission owner, the organizations providing BCP and MCP for alert notification as part of the incident reporting procedures; include DIB ID number.

E-2.C. Meets Continuous Monitoring and Incident Reporting Requirements

E-2.C.1. If the CSO is authorized through FedRAMP, the CSP will report for continuous monitoring and incident reporting via FedRAMP protocols to US-CERT and FedRAMP PMO and to the mission owner as articulated in the SLA. In addition, the SLA may contain reporting requirements specific to each mission owner.

E-2.C.2. If the CSO is authorized through a DOD PA, the CSP will report for continuous monitoring and incident reporting via the terms of the DOD Authority to Operate (ATO) and mission owner SLAs.

E-3. CSP Cyber Event and Incident Procedures

E-3.A. Initial Cloud Activity Assessment

E-3.A.1. If initiated via incoming notification from an organization performing BCP or MCP, US-CERT, or via internal sensing and analysis, the CSP investigates for scope of impact to DOD and CSP.

E-3.A.2. Communicate findings to the impacted mission owner(s) in addition to other required reporting channels (e.g. US-CERT for FedRAMP-authorized CSOs).

E-3.A.3. Report updated situational awareness reports to mission owners.

E-3.B. Response to Unauthorized Access and Intrusion

E-3.B.1. CSP notifies all potentially impacted mission owners, who in turn notify the organizations providing MCP.

E-3.B.2. If event or incident occurred on a FedRAMP-authorized CSO, CSP reports event or incident to US-CERT.

E-3.B.3. CSP periodically reports remediation progress to potentially impacted mission owners until closure.

E-3.C. Response to Unsuccessful Activity Attempt

E-3.C.1. If the event is identified by the CSP, the CSP develops a situational awareness report and distributes it to the impacted mission owners.

E-3.D. Response to DoS

E-3.D.1. Execute CSP initial cloud activity assessment, Section E-3.A.

E-3.E. Response to Non-Compliance Activity

E-3.E.1. Execute CSP initial cloud activity assessment, Section E-3.A.

E-3.F. Response to Reconnaissance

E-3.F.1. If the event is identified by the CSP, the CSP develops a situational awareness report and distributes it to the impacted mission owners.

E-3.G. Response to Malicious Logic

E-3.G.1. Execute CSP initial cloud activity assessment, Section E-3.A.

E-3.H. Response to Explained Anomaly

E-3.H.1. Execute initial cloud activity assessment, Section E-3.A.

E-3.H.2. If possible, identify process or tool updates to reduce occurrence of explained anomaly and recommend or implement changes IAW specified contractual agreements.

E-3.I. Response to Spillage and Unauthorized Disclosure

E-3.I.1. Execute CSP initial cloud activity assessment, Section E-3.A.

E-3.I.2. Support investigation into spillage or unauthorized disclosure by mission owner and the organization proving MCP.

E-3.I.3. Support mission owner and the organization providing MCP in remediation effort.

E-3.I.4. If directed by mission owner, execute CSP data spill or unauthorized disclosure cleanup method as defined in CSO PA Assessment.

E-3.J. Performing Vulnerability Scans

E-3.J.1. CSP performs vulnerability scans within the cloud service authorization boundary.

E-3.J.2. CSP creates POA&M.

E-3.J.3. CSP reports results to FedRAMP PMO and all parties specified in the contractual agreement.

E-3.K. Performing Annual External Assessments

E-3.K.1. If the CSP provides some of the controls to the mission owner via the SLA, then:

a) CSP receives notice from the mission owner of an annual external assessment plan.

b) CSP coordinates resources to support mission owner’s annual external assessment (e.g., Pen Test, Red Team, etc.).

c) CSP delivers data packages to mission owner to complete its role in the annual external assessment.

E-3.L. Performing Configuration Management (CM) and Patching

Patching is a required routine activity. CSPs and mission owners can incorporate into their SLA that mission owners will utilize FedRAMP reports to satisfy CSP reporting responsibilities to the mission owner.

E-3.L.1. CSP receives a patch for systems and applications of the cloud service.

E-3.L.2. CSP follows reporting responsibilities to FedRAMP, US-CERT, and mission owner.

E-3.L.3. CSP follows defined patch process. If outage is required, CSP will follow Section E-3.M, performing planned outage procedures.

E-3.L.4. CSP reports restoration of service and success of patch deployment to the mission owner, FedRAMP PMO, and US-CERT.

E-3.M. Performing Planned Outage

E-3.M.1. If the planned outage is initiated by CSP

a) CSP plans outage.

b) CSP notifies mission owners.

c) If CSO operates under FedRAMP authorization, CSP notifies US-CERT and FedRAMP PMO.

d) At conclusion of planned outage, CSP notifies mission owners of restoration of service.

E-3.M.2. If the planned outage is initiated by DOD, the CSP will be notified of planned outage by mission owners.

E-3.N. Response to Unplanned Outage

E-3.N.1. CSP notifies mission owners.

E-3.N.2. If CSO operates under FedRAMP authorization, CSP notifies US-CERT and FedRAMP PMO.

E-3.N.3. At conclusion of unplanned outage, CSP notifies mission owners of restoration of service.

E-3.O. Performing Disaster Recovery

E-3.O.1. Assist mission owner upon request in executing disaster recovery procedures to restore cloud-hosted functionality.

E-3.P. Response to Training and Exercises

The following procedure pertains to incidents detected by the CSP that are determined to be associated to a training or exercise event.

E-3.P.1. Execute CSP Initial Cloud Activity Assessment, Section E-3.A.

ANNEX F: CLOUD CYBERSPACE PROTECTION COMMUNICATIONS MATRIX

The below table represents the means of communications typically available to organizations performing cybersecurity activities and DCO internal defensive measures to report or share data regarding events and incidents.

Table 3 - Cloud Cyberspace Protection Communications Matrix

Means of Communications	milCloud	CSP (CSO On-Premises)	CSP (CSO Off-Premises)	Mission Owner	Organization Providing MCP	Organization Providing BCP	JFHQ-DODIN	US-CERT
CSP (milCloud)								
JIMS					X			
Classified Communications (e.g. SIPRNet, STE, etc.)				X	X			
Unclassified Communications (e.g. NIPRNet, Phone, etc.)				X	X			
CSP (CSO On-Premises)								
US-CERT Incident Response System								X
DIB Cyber Incident Reporting tool				X	X			X
Unclassified Communications (e.g. Internet, Phone, etc.)				X	X			X
CSP (CSO Off-Premises)								
US-CERT Incident Response System								X
DIB Cyber Incident Reporting tool				X	X	X		X
Unclassified Communications (e.g. Internet, Phone, etc.)				X	X	X		X
Mission Owner								
DIBNET Incident Reporting Tool		X	X					
Classified Communications (e.g. SIPRNet, STE, etc.)	X				X			
Unclassified Communications (e.g. NIPRNet, Phone, etc.)	X	X	X		X			

Means of Communications	milCloud	CSP (CSO On-Premises)	CSP (CSO Off-Premises)	Mission Owner	Organization Providing MCP	Organization Providing BCP	JFHQ-DODIN	US-CERT
Organization Providing MCP								
JIMS					X	X	X	
DIBNET Incident Reporting Tool		X	X					
Classified Communications (e.g. SIPRNet, STE, etc.)	X			X	X	X	X	
Unclassified Communications (e.g. NIPRNet, Phone, etc.)	X	X	X	X	X	X	X	
Organization Providing BCP								
JIMS					X	X	X	
DIBNET Incident Reporting Tool			X					
Classified Communications (e.g. SIPRNet, STE, etc.)					X	X	X	
Unclassified Communications (e.g. NIPRNet, Phone, etc.)			X		X	X	X	
JFHQ-DODIN								
US-CERT Incident Response System								X
JIMS					X	X		
JWICS						X		X
Classified Communications (e.g. SIPRNet, STE, etc.)					X	X		
Unclassified Communications (e.g. NIPRNet, Phone, etc.)					X	X		X
US-CERT								
US-CERT Incident Response System	X	X	X				X	
Classified Communications (e.g. JWICS, SIPRNet, STE, etc.)							X	
DIBNET Incident Reporting Tool		X	X					
Unclassified Communications (e.g. Internet, Phone, etc.)	X	X	X				X	

ANNEX G: REFERENCES

(a) Joint Chiefs of Staff. (2012, July). Chairman of the Joint Chiefs of Staff Manual 6510.01B: Cyber Incident Handling Program. http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf

(b) DOD CIO. (2003, December). DOD O-8530.1-M: Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process Program Manual. https://whsddpubs.dtic.mil/corres/pdf/O853001M.pdf

(c) DOD CIO. (2016, March). DOD Instruction 8530.01: Cybersecurity Activities Support to DOD Information Network Operations. http://www.dtic.mil/whs/directives/corres/pdf/853001p.pdf

(d) Defense Information Systems Agency (DISA). (2016, March). DOD Cloud Computing SRG. http://iasecontent.disa.mil/cloud/SRG/index.html

(e) DISA. (2014, June). DISA's Strategy for Defensive Cyber Operations.

(f) DISN Connection Process Guide (CPG) Home Page. http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide

(g) FedRAMP Home Page. http://cloud.cio.gov/fedramp

(h) United States Code, Title 44.

(i) National Institute of Standards and Technology. (2011, September). NIST SP800-145: The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

(j) US-CERT Federal Incident Reporting Guidelines. https://www.us-cert.gov/government-users/reporting-requirements#tax

(k) DISA. (2015, June). Cloud Access Point (CAP) Security Functional Requirements Document (FRD).

(l) Joint Chiefs of Staff. (2011, February). Chairman of the Joint Chiefs of Staff Instruction 6510.01F: Information Assurance (IA) and Support to Computer Network Defense (CND). http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

(m) US-CERT. (2014, October). US-CERT Federal Incident Notification Guidelines. https://www.us-cert.gov/incident-notification-guidelines

(n) DOD CIO. (2013, August). DOD Instruction 8320.02: Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense. www.dtic.mil/whs/directives/corres/pdf/832002p.pdf

(o) DOD CIO. (2015, August). DOD Instruction 8320.07: Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense. www.dtic.mil/whs/directives/corres/pdf/832007p.pdf

(p) DOD CIO. (2013, March). DOD Manual 5200.01 Vol 3: DOD Information Security Program: Protection of Classified Information. http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

(q) DOD CIO. (2007, May). DOD 5400.11-R: DOD Privacy Program. http://dtic.mil/whs/directives/corres/pdf/540011r.pdf

ANNEX H: ABBREVIATIONS AND ACRONYMS

ACAS	Assured Compliance Assessment Solution
APT	advanced persistent threat
AS&W	attack sensing & warning
ATO	authority to operate
AV	anti-virus
BCAP	boundary cloud access point
BCP	boundary cyberspace protection
CAP	cloud access point
CCB	configuration control broad
CI	Counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
CM	configuration management
CMRS	Continuous Monitoring and Risk Scoring
COOP	Continuity of Operations
CPT	cyber protection team
CSO	cloud service offering
CSP	cloud service provider
CSSP	cybersecurity service provider
DCO	defensive cyberspace operations
DIBNET	Defense Industrial Base Network
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DOD	Department of Defense
DoS	denial of service
DODIN	Department of Defense Information Network

FedRAMP	Federal Risk and Authorization Management Program
HBSS	Host Based Security System
IaaS	Infrastructure as a Service
IAP	Internet Access Point
ICAP	internal cloud access point
ICF	Incident Collection Format
JAB	Joint Authorization Board
JCC	Joint Cyber Center
JFHQ-DODIN	Joint Force Headquarters DOD Information Network
JIE	Joint Information Environment
JIMS	Joint Incident Management System
LE	Law Enforcement
MCP	Mission Cyberspace Protection
NIST	National Institute of Standards and Technology
NCTOC	National Security Agency/Central Security Service Cyber Threat Operations Center
PaaS	Platform as a Service
PA	Provisional Authorization
POA&M	Plan of Action and Milestones
POND	Period of Non-Disruption
RTO	Recovery Time Objective
SaaS	Software as a Service
SA	Situational Awareness
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SRG	Security Requirements Guide
SQL	Structured Query Language

TIPR	Threat Intelligence Product Report
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network
XSS	Cross-Site Scripting

ANNEX I: CLOUD CYBERSPACE PROTECTION DEFINITIONS

Boundary Cloud Access Point (BCAP): DISN perimeter gateway that provides a barrier of protection between the DISN and the CSO.

Blue Team: As defined in CNSSI-4009, *"A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems."*

Breach: As defined in OMB M-17-12, *"the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for an other than authorized purpose."*

Classified Information: As defined in CNSSI-4009, *"Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."*

Cloud Service Provider (CSP): Commercial vendor or Federal organization offering or providing Cloud services (Includes DOD CSPs); the provider of CSOs.

Community Cloud: As defined in NIST SP800-145, *"The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises."*

Configuration Control Board (CCB): As defined in CNSSI-4009, *"A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational lifecycle of an information system."*

Continuous Monitoring: As defined in CNSSI-4009, *"The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise."*

Countermeasure: As defined in CNSSI-4009, *"Actions, devices, procedures, or techniques that meet or oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken."*

Cybersecurity Service Provider (CSSP): As defined in DOD Instruction 8530.01, *"DOD component or authorized external DOD Component service provider that provides one or more cybersecurity services to implement and protect the DODIN."*

Cyber Incident: As defined in CNSSI-4009, *"Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident."*

Denial of Service (DoS): As defined in CNSSI-4009, *"The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)"*

Defense Information Systems Network (DISN): As defined in JP 1-02, *"The integrated network, centrally managed and configured by the Defense Information Systems Agency to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services for all Department of Defense activities. Also called DISN. (JP 6-0)"*

DOD Information Network (DODIN): As defined in JP 1-02, *"The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called DODIN. (JP 6-0)"*

Event: As defined in CNSSI-4009, *"Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring."*

Gateway: As defined in CNSSI-4009, *"Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures."*

Incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Infrastructure as a Service (IaaS): As defined in NIST SP 800-145, *"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."*

Joint Authorization Board (JAB): The primary governance and decision-making body for the FedRAMP program.

Malware: From Evaluator Scoring Metrics, *"Malware refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, and/or availability of the victim's data, application, or information system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations."*

Penetration Testing: As defined in CNSSI-4009, *"A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system."*

Personally Identifiable Information (PII): As defined in OMB M-17-12, *"information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."*

Platform as a Service (PaaS): As defined in NIST SP 800-145, *"The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment."*

Private Cloud: As defined in NIST SP800-145, *"The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises."*

Red Team: As defined in CNSSI-4009, *"A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment."*

Scanning: As defined in CNSSI-4009, *"Sending packets or requests to another system to gain information to be used in a subsequent attack."*

Secure State: As defined in CNSSI-4009, *"Condition in which no subject can access any object in an unauthorized manner."*

Software as a Service (SaaS): As defined in NIST SP 800-145, *"The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual* *application capabilities, with the possible exception of limited user-specific application configuration settings."*

Spillage or Data Spill: an unauthorized transfer of classified information or Controlled Unclassified Information to an information system that is not accredited for the applicable security level of the data or information.

Threat: As defined in CNSSI-4009, *"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."*

Virtual Private Network (VPN): As defined in CNSSI-4009, *"Protected information system link utilizing tunneling, security controls (see Information Assurance), and endpoint address translation giving the impression of a dedicated line."*

Vulnerability: As defined in CNSSI-4009, *"Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."*

Vulnerability Assessment: As defined in CNSSI-4009, *"Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation."*