



1

2

3

**DEPARTMENT OF DEFENSE (DOD)
CLOUD CYBERSPACE PROTECTION GUIDE**

4

5

16 October 2017

Incorporating Change 1, 19 December 2017

6

7

8

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

9

Trademark Information

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

14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42

CLOUD CYBERSPACE PROTECTION GUIDE

TABLE OF CONTENTS

EXECUTIVE SUMMARY 5

CLOUD CYBERSPACE PROTECTION: BASE PLAN..... 6

1. Introduction..... 6

2. Background 7

3. Cyber Event and Incident Response Matrix 11

4. CSPs Reporting to US-CERT 16

ANNEX A: DOD COMPONENT RESPONSIBILITIES 17

ANNEX B: BOUNDARY CYBERSPACE PROTECTION (BCP) FUNCTIONS 18

B-1. BCP Introduction..... 18

B-2. Responsibilities of Organizations Providing BCP Functions..... 18

B-3. Organizations Providing BCP Cyber Incident and Event Procedures Responsibilities..... 19

ANNEX C: MISSION CYBERSPACE PROTECTION (MCP) FUNCTIONS..... 23

C-1. MCP Introduction 23

C-2. Responsibilities of Organizations Providing MCP Functions..... 23

C-3. Organizations Providing MCP Cyber Incident and Event Procedures Responsibilities 24

ANNEX D: MISSION OWNER 29

D-1. Mission Owner Introduction..... 29

D-2. Mission Owner Responsibilities..... 29

D-3. Mission Owner Cyber Event and Incident Procedures Responsibilities 31

ANNEX E: CSP..... 35

E-1. CSP Introduction 35

E-2. CSP Responsibilities 35

E-3. CSP Cyber Event and Incident Procedures 36

ANNEX F: CLOUD CYBERSPACE PROTECTION COMMUNICATIONS MATRIX..... 39

ANNEX G: REFERENCES 41

ANNEX H: ABBREVIATIONS AND ACRONYMS 43

ANNEX I: CLOUD CYBERSPACE PROTECTION DEFINITIONS..... 46

43 TABLE OF TABLES

44 **Table 1 – Cyber Event and Incident Response Matrix..... 11**

45 **Table 2 – Mapping US-CERT Categories to DOD Categories 16**

46 **Table 3 - Cloud Cyberspace Protection Communications Matrix 39**

47 TABLE OF FIGURES

48 **Figure 1 – Depiction of the Various Cloud Access Points 9**

49 **Figure 2 - DOD Cloud cyberspace protection information sharing model..... 10**

50 **EXECUTIVE SUMMARY**

51 The Cloud Cyberspace Protection guide defines a set of reporting and incident handling procedures for
52 the organizations that will protect the Department of Defense (DOD) Information Network (DODIN) in
53 the cloud, as specified in the DOD Cloud Computing Security Requirements Guide (SRG) section on
54 cyberspace protection and incident response. This guide defines how mission owners, organizations
55 providing mission cyberspace protection (MCP), boundary cyberspace protection (BCP), cloud service
56 providers¹ (CSPs), and Joint Force Headquarters DODIN (JFHQ-DODIN) will cooperate in response to
57 cyber incidents and events in accordance with DOD Cloud Computing (SRG) and DOD Instruction
58 (DODI) 8530.01.

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

- 62 1. BCP Function: Protects the Defense Information Systems Network (DISN) from an event or
63 incident that utilizes external cloud services.
- 64 2. MCP Function: Protects systems, applications, and data hosted within cloud services.

65 The guide provides additional guidance to the DOD Cloud Computing SRG and DOD Instruction (DODI)
66 8530.01 by defining reporting and data-sharing relationships between organizations providing protection.
67 The procedures described in each annex establish specific interactions between organizations conducting
68 BCP and MCP cybersecurity activities and DCO internal defensive measures, their interactions with
69 mission owners and CSPs, and the reporting requirements of cyber events and incidents to JFHQ-
70 DODIN. The procedures apply to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and
71 Software as a Service (SaaS) Cloud service offerings (CSOs) installed as: On-Premises CSO Level 2/4/5;
72 Off-Premises CSO Level 2; or Off-Premises CSO Level 4/5. This document does not apply to Level 6
73 CSOs.

74 The responsibilities and functions are elaborated in the annexes:

- 75 • Annex A – Responsibilities: DOD Component & JFHQ-DODIN
76 • Annex B – Boundary Cyberspace Protection Function
77 • Annex C – Mission Cyberspace Protection Function
78 • Annex D – Mission Owner
79 • Annex E – CSP
80

81 This document is expected to evolve as the procedures are put into practice and new best practices
82 emerge. As such it should be treated as a foundation upon which to improve in addition to providing
83 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

84 **CLOUD CYBERSPACE PROTECTION: BASE PLAN**

85 **1. Introduction**

86 1.A. General.

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

88 1.B. Boundary Cyberspace Protection (BCP) Function

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

93 1.C. Mission Cyberspace Protection (MCP) Function

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

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

108 1.D. Purpose and Audience.

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

113 1.E. Applicability.

114 This document:

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

117 b) Applies to .mil domains.

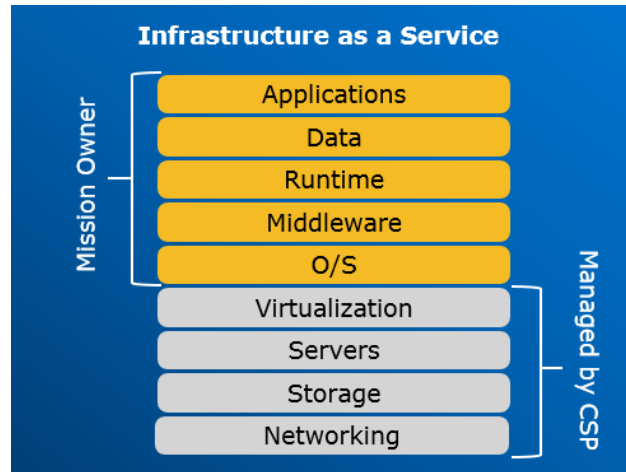
118 c) Does not apply to mission owners that typically operate networks that may not be part of the
119 DISN or .mil domain (e.g., commissaries; exchanges; Morale, Welfare and Recreation (MWR)
120 organizations; Non-Appropriated Fund (NAF) organizations; educational entities (e.g., National
121 Defense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

123 **2. Background**

124 2.A. Cloud Service Models

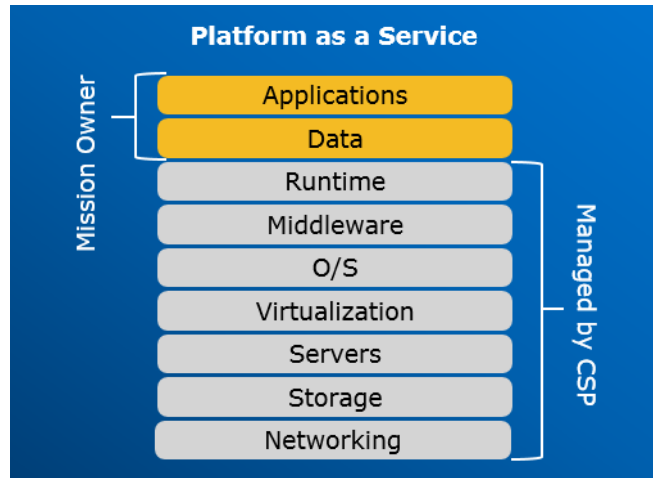
125 As applications and capabilities are moved to the cloud, mission owners will select CSOs offered by
126 CSPs. CSOs will be offered in three Service Models²:

- 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).

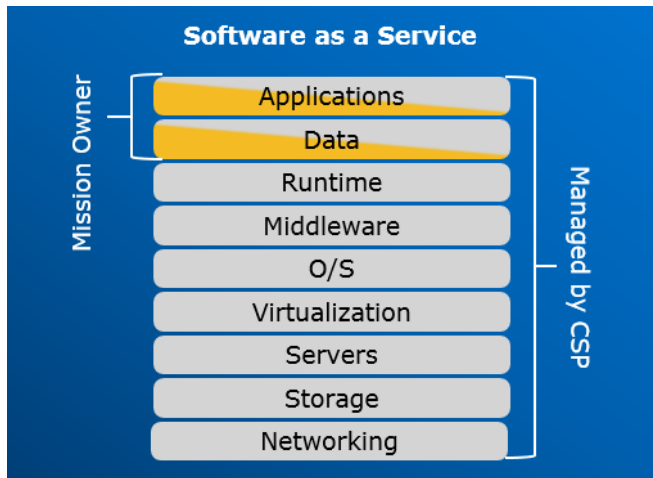


² Ref (i): Definitions from National Institute of Standards and Technology (NIST) SP 800-145: The NIST Definition of Cloud Computing

- 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.



127 2.B. CSO Connection Models

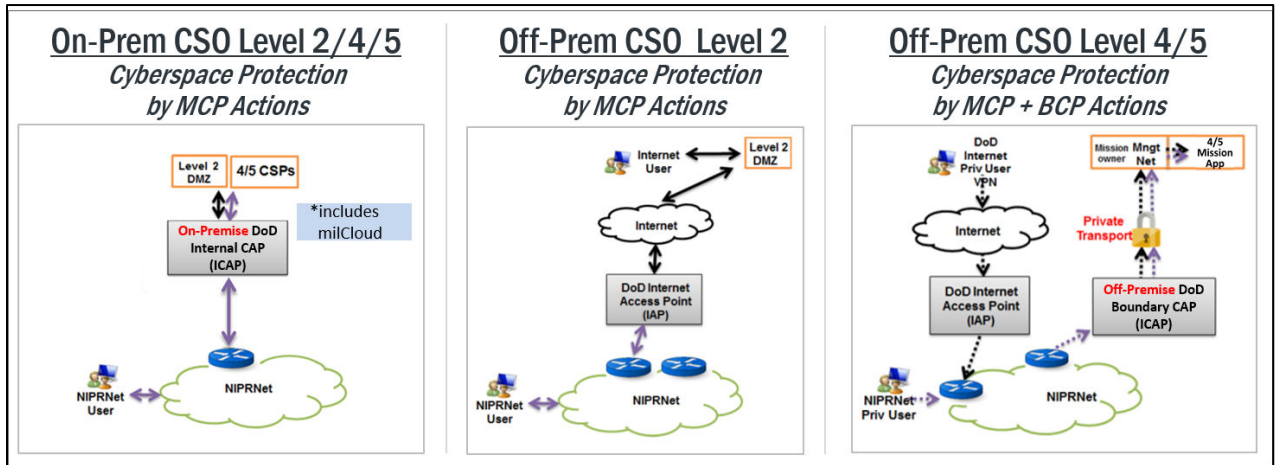
128 There are three CSO connection models that a mission owner can select to host their data. Off premises
129 connection models are dependent on the Information Impact Levels as defined in the DOD Cloud
130 Computing SRG. The connection models are On-Premises CSO Level 2/4/5 (including milCloud), Off-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

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

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

139 Off-Premises CSO Level 2: A mission Owner utilizing an off premises CSO requires support from
 140 an organization providing MCP (authorized CSSP) to protect systems, applications, and and/or data
 141 hosted in the cloud service model. For an Information Impact Level 2 CSO, the CSP off premises
 142 does not use a BCAP and does not require support from an organization providing BCP (see Figure
 143 1).

144 Off-Premises CSO Level 4/5: A mission owner utilizing an off premises CSO requires support from
 145 an organization providing MCP (authorized CSSP) to protect systems, applications, and/or data
 146 hosted in the Cloud. If the mission owner utilizes an off premises CSO for Information Impact Level
 147 4/5 (see Figure 1), they must establish a dedicated connection via a BCAP. The BCAP requires
 148 support from an organization providing BCP for all connections through that BCAP.



149
 150 **Figure 1 – Depiction of the Various Cloud Access Points³**

151 2.C. Cloud Cyberspace Protection Information Sharing Structure

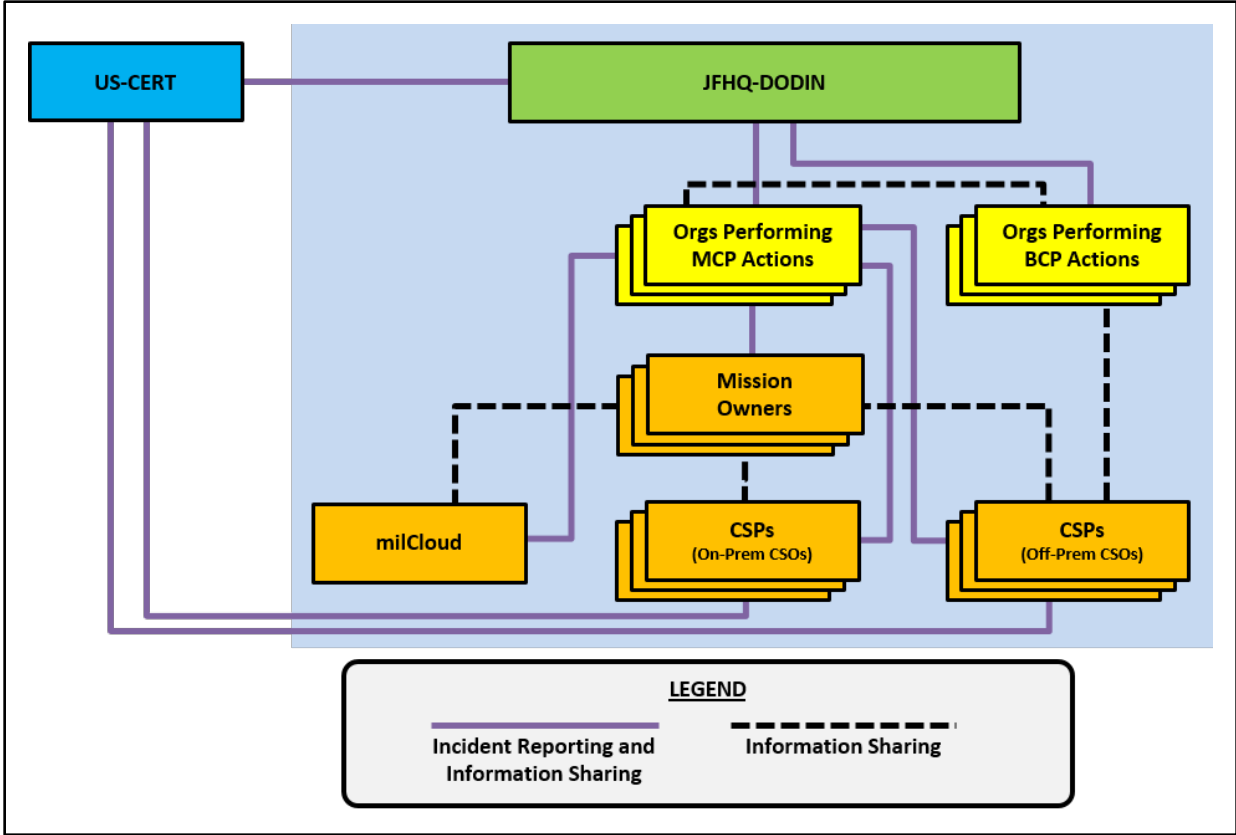
152 The DOD Cloud Computing SRG defines a reporting and communication function structure for cloud
 153 services. This structure supports the information flows that will be necessary to support global cyber
 154 situational awareness. The DOD Cloud Computing SRG defines the BCP and MCP actions. BCP actions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

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

³ Ref (k) extracted from CAP Security FRD

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

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



168

169 **Figure 2 - DOD Cloud cyberspace protection information sharing model**

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

176 2.D. Cyberspace Protection Methodology

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

184 **3. Cyber Event and Incident Response Matrix**

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

190

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”

191 3.A. Initial Cloud Activity Assessment

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

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

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

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

207 If the CSP submits a situational awareness report⁵, the recipient mission owner will post or distribute the
208 situational awareness report to the organization providing MCP. If a CSP detects a event or incident that
209 potentially affects DOD information confidentiality, integrity, or availability, information about the event
210 or incident should be made available to the mission owner via a situational awareness report, who will
211 post or distribute it to the organization providing MCP. Organizations providing MCP will share
212 situational awareness reports with peer organizations providing MCP and BCP, and the JFHQ-DODIN to
213 enable collaboration.

214 3.B. Response to Unauthorized Access and Intrusion

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

- 216 a) Cloud-hosted mission: An intrusion into the DOD mission applications, systems or data residing
217 on the cloud service.
- 218 b) DISN via BCAP: An intrusion that originates from outside the DISN and enters via the BCAP,
219 possibly from a cloud-hosted application, system, or data with persistent access into the DISN via
220 the BCAP.
- 221 c) CSO: An intrusion into the underlying cloud service management plane or infrastructure that
222 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.

UNCLASSIFIED

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

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

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

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

233 3.C. Response to Unsuccessful Activity Attempt

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

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

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

243 3.E. Response to Non-Compliance Activity

244 Execute initial cloud activity assessment, Section 3.A.

245 3.F. Response to Reconnaissance

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

253 3.G. Response to Malicious Logic

254 Malicious logic (aka malware) can reside on a cloud solution of any delivery model: IaaS, PaaS, and
255 SaaS. Malicious logic can infect operating systems, network devices, applications, or data files (e.g. PDF
256 or MS Word files). In addition to traditional malware impact analysis, analysts will monitor for malware

UNCLASSIFIED

UNCLASSIFIED

257 that specifically exploits the cloud infrastructure, software, or exploits the dedicated BCAP connections to
258 the DISN.

259 3.H. Response to Explained Anomaly

260 An explained anomaly is an event caused by non-malicious activity, such as malfunctions or false
261 alarms⁶. When it is determined by the detecting organization (whether by the organization providing
262 MCP or BCP, or CSP) that the explained anomaly events potentially affect DOD information
263 confidentiality, integrity, or accessibility, information about the events should be made available by the
264 detecting organization to the other organizations via a situational awareness report.

265 3.I. Response to Spillage or Unauthorized Disclosure

266 Although not defined as a incident or reportable event, reporting spillage or unauthorized disclosure is
267 still necessary for the maintenance of global cyber SA. Spillage⁷ is defined as “Contamination of lower
268 level networks with material of a higher classification.” The JFHQ-DODIN should be notified of any
269 spillage or unauthorized disclosure of controlled unclassified information (CUI), personally identifiable
270 information (PII), protected health information (PHI), or unclassified national security information (NSI)
271 with an evaluation of impact not only to DODIN but also to national security and personnel.

272 Unauthorized disclosure includes:

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

277 The mission owner retains accountability for spillage and unauthorized disclosure remediation, whether
278 the remediation process is executed by the mission owner or by the CSP. The steps taken depend on the
279 configuration of the mission owner applications and data, the service level agreements (SLAs) in place for
280 the cloud service, and the separations of authority for the systems on which the data resides. They will be
281 carried out via the CSP’s data spill/unauthorized disclosure cleanup methods in accordance with (IAW)
282 the Cloud Computing SRG⁸, and reported as a Category 5 incident via JIMS. In the case of spillage of
283 classified data, investigation, reporting, and remediation must be performed IAW the Cloud Computing
284 SRG and DOD Manual 5200.01 Vol 3⁹ or DOD 5400.11-R. In the case of spillage or unauthorized
285 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

UNCLASSIFIED

286 3.J. Performing Vulnerability Scans

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

292 3.K. Performing Annual External Assessments

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

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

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

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

313 3.M. Performing Planned Outage

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

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

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

326 3.N. Response to Unplanned Outage

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

330 3.O. Performing Disaster Recovery

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

333 3.P. Response to Training and Exercises

334 Execute initial cloud activity assessment, Section 3.A.

335 **4. CSPs Reporting to US-CERT**

336 CSPs that report events or incidents via the online DIB 10 Cyber ICF will characterize the event or
 337 incident IAW the US-CERT Federal Incident Notification Guidelines¹¹, which is reflected in Table 2.
 338 Impacted organizations providing MCP will relay the incident reported in the DIB Network (DIBNET)
 339 Incident Reporting Tool by the CSP to JFHQ-DODIN via JIMS. Table 2 reflects those DOD categories
 340 that directly map to US-CERT categories. The other DOD categories (categories 1, 2, 3, 9, and 0) are not
 341 listed on the table; however, they can be used by DOD to identify the incident or event.

342 **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.

343 **ANNEX A: DOD COMPONENT RESPONSIBILITIES**

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

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

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

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

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

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

359 **ANNEX B: BOUNDARY CYBERSPACE PROTECTION (BCP) FUNCTIONS**360 **B-1. BCP Introduction**

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

371 **B-2. Responsibilities of Organizations Providing BCP Functions**372 **B-2.A. CSSP**

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

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

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

377 a) Installing and maintaining sensors

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

380 c) Monitoring sensor and log feeds

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

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

383 B-2.B.2. Will monitor data in transit through the BCAP based on BCAP sensing capabilities¹².

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

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

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

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

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

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

UNCLASSIFIED

- 392 B-2.C.4. Generate and aggregate metric and trending data for the supported BCAP.
- 393 B-2.C.5. Provide aggregated metric and trending data for the supported BCAP to the JFHQ-
- 394 DODIN.
- 395 B-2.C.6. Combatant command and Joint Cyber Center (JCC) SA coordination.
- 396 B-2.D. Will establish communication plans.
- 397 B-2.E. Will maintain POC lists
- 398 B-2.E.1. Maintain current contact lists for POCs at the JFHQ-DODIN, organizations providing
- 399 BCP and MCP, mission owners, and CSPs for:
- 400 a) Cyber event and incident response reporting (see Figure 2), including: guidance, orders,
- 401 and reporting
- 402 b) Coordination (see Figure 2), including situational awareness reports distribution and
- 403 cyberspace protection data sharing
- 404 c) Distribution lists for situational awareness reports, plan of action and milestones
- 405 (POA&Ms), external assessments (plans, reports, findings), vulnerability scan schedules, and
- 406 outage notices
- 407 B-2.E.2. Maintain BCP organization POC list; distribute changes to POC list to the JFHQ-
- 408 DODIN, peer organizations providing BCP, relevant organizations providing MCP, mission
- 409 owners, and CSPs.

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

- 411 B-3.A. Initial Cloud Activity Assessment
- 412 B-3.A.1. Notify the JFHQ-DODIN if incidents are being reported with regard to multiple mission
- 413 owners or CSPs.
- 414 B-3.A.2. Document the incident in JIMS. If the boundary impact is unknown, the incident is
- 415 categorized as a CAT 8 “Investigating” incident.
- 416 B-3.A.3. Report incident to the JFHQ-DODIN for DOD CAT 1, 2, 4; CAT 3’s and 7’s as
- 417 required per Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01B¹³.
- 418 B-3.A.4. Consult and advise the JFHQ-DODIN to coordinate orders, as needed.
- 419 B-3.A.5. Notify impacted organizations providing MCP via situational awareness report.
- 420 B-3.A.6. Execute JFHQ-DODIN distributed TASKORDs.
- 421 B-3.A.7. Cooperate post intrusion, with the organizations providing BCP and MCP to support
- 422 return to normal operations. If for example a server is compromised and the cloud and network is
- 423 restored to a secure state¹⁴, the organization(s) providing BCP and MCP should be monitoring to
- 424 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.”

UNCLASSIFIED

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

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

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

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

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

431 c) Stop this procedure at this step.

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

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

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

438 c) Notify organization providing MCP via situational awareness report

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

441 B-3.C. Response to Unsuccessful Activity Attempt

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

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

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

448 B-3.D. Response to DoS

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

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

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

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

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

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

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

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

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

UNCLASSIFIED

- 462 B-3.F. Response to Reconnaissance
- 463 B-3.F.1. If signs of unauthorized access cannot be determined/validated by evaluating sources of
464 reconnaissance:
- 465 a) Investigate reported event or incident for DODIN boundary impact.
- 466 b) Develop a situational awareness report.
- 467 c) Distribute situational awareness report to the JFHQ-DODIN, peer organizations
468 performing BCP, and applicable organizations performing MCP and CSPs (within
469 classification constraints).
- 470 B-3.F.2. If the reconnaissance event is identified by the organization performing BCP, the
471 organization:
- 472 a) Develops a situational awareness report.
- 473 b) Distributes the situational awareness report to the JFHQ-DODIN, peer organizations
474 performing BCP, and applicable organizations performing MCP and CSPs (within
475 classification constraints).
- 476 B-3.F.3. Determine source or cause of reconnaissance for signs of unauthorized access or
477 malware.
- 478 a) If unauthorized access is detected, refer to the relevant procedure respective to
479 organizations providing BCP, MCP, or mission owner, Section 3.B: Response to
480 Unauthorized Access and Intrusion.
- 481 b) If malware is detected, refer to Section B-3.G: Response to Malicious Logic.
- 482 c) Update situational awareness report and resend.
- 483 B-3.F.4. Determine need, if any, for preventative countermeasures at the BCAP.
- 484 B-3.G. Response to Malicious Logic
- 485 B-3.G.1. Malware may be identified in the course of ongoing monitoring or in response to an
486 organization providing MCP. If the organization providing BCP identifies the malware, the
487 organization providing BCP notifies applicable organization providing MCP and the JFHQ-
488 DODIN. The organization providing MCP will open a CAT 7 JIMS ticket.
- 489 B-3.G.2. The JFHQ-DODIN may distribute TASKORD to organizations providing BCP and
490 MCP. All TASKORDs distributed by the JFHQ-DODIN will be executed by BCPs and MCPs.
- 491 B-3.H. Response to Explained Anomaly
- 492 B-3.H.1. Execute initial cloud activity assessment, Section B-3.A.
- 493 B-3.H.2. Implement process or tool update to reduce occurrence of explained anomaly, if
494 possible.
- 495 B-3.I. Response to Spillage or Unauthorized Disclosure
- 496 B-3.I.1. If the organization providing BCP identifies the spillage or unauthorized disclosure, the
497 organization providing BCP notifies organization providing MCP of impacted mission owner.
- 498 B-3.I.2. The organization providing BCP supports the organization providing MCP investigation
499 and response to spillage or unauthorized disclosure to closure.

UNCLASSIFIED

- 500 B-3.J. Performing Vulnerability Scans
- 501 B-3.J.1. Receive vulnerability scan schedule from the organization providing MCP.
- 502 B-3.J.2. Support mission owner during vulnerability scans (e.g. modify alert or response posture
- 503 during vulnerability scans period).
- 504 B-3.K. Performing Annual External Assessments.
- 505 B-3.K.1. Receive notification of external assessment type and period from organization providing
- 506 MCP.
- 507 B-3.K.2. Receive a full report of findings and recommendations from the organization providing
- 508 MCP after the assessment is complete.
- 509 B-3.L. Performing Configuration Management (CM) and Patching
- 510 B-3.L.1. Receive notice from organization providing MCP of patch schedule/outage.
- 511 B-3.L.2. Receive notice of restoration of service and success of patch deployment from
- 512 organization providing MCP.
- 513 B-3.L.3. Receive updated CM and patching documentation via the organization providing MCP.
- 514 B-3.M. Performing Planned Outage
- 515 B-3.M.1. Receive notice from organization providing MCP of outage schedule.
- 516 B-3.M.2. Receive notice from organization providing MCP after restoration of service.
- 517 B-3.N. Response to Unplanned Outage
- 518 B-3.N.1. Receive notice from organization providing MCP of outage and impact.
- 519 B-3.N.2. Track outages to closure.
- 520 B-3.O. Performing Disaster Recovery
- 521 B-3.O.1. Assist organization providing MCP and mission owner in executing disaster recovery
- 522 procedures to restore cloud-hosted functionality for off premises cloud services via BCAP.
- 523 B-3.P. Response to Training and Exercises
- 524 B-3.P.1. Execute initial cloud activity assessment, Section B-3.A.

UNCLASSIFIED

525 **ANNEX C: MISSION CYBERSPACE PROTECTION (MCP) FUNCTIONS**

526 **C-1. MCP Introduction**

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

535 **C-2. Responsibilities of Organizations Providing MCP Functions**

536 C-2.A. CSSP

537 C-2.A.1. Will be a DOD Component or authorized external DOD Component service provider
538 that provides one or more cybersecurity services to implement and protect the DODIN¹⁵.

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

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

541 a) Install and maintain sensors.

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

544 c) Monitor sensor and log feeds.

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

547 C-2.B. Perform analysis for cloud service incidents/events.

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

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

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

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

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

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

¹⁵ Ref (c) DOD Instruction 8530.01 Glossary

UNCLASSIFIED

- 557 C-2.F. Identify inconsistencies and inaccuracies in the results provided by CSP vulnerability
558 assessments and inform mission owners.
- 559 C-2.G. Will retain copy of the mission owner’s SLA with CSP; should ensure mission owner has
560 proper DOD-approved cloud service SLA.
- 561 C-2.G.1. Provide placement locations for sensors (if appropriate).
- 562 C-2.G.2. Assist with installation and feeds to systems providing MCP capabilities.
- 563 C-2.G.3. Perform and assist with external assessments.
- 564 C-2.G.4. Confirms setup of Host Based Security System (HBSS), ACAS, Continuous Monitoring
565 and Risk Scoring (CMRS), and any other security capabilities as applicable.

566 C-2.H. Will maintain POC lists

- 567 C-2.H.1. Maintain current contact lists for POCs at the JFHQ-DODIN, organizations performing
568 BCP, mission owner, and CSPs for:
- 569 a) Event and incident response reporting, including: guidance, orders and reporting
- 570 b) Coordination including situational awareness reports distribution and information sharing
- 571 c) Distribution lists for situational awareness reports, POA&Ms, external assessments (plans,
572 reports, findings), vulnerability scans schedules, and outage notices
- 573 C-2.H.2. Maintain POC list; distribute changes to POC list to the JFHQ-DODIN, relevant
574 organizations providing BCP actions, peer organizations providing MCP actions, mission owners,
575 and CSPs.

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

577 C-3.A. Initial Cloud Activity Assessment

- 578 C-3.A.1. Document the incident in JIMS. If mission owner impact is unknown, the incident is
579 categorized as a CAT 8 “Investigating” incident.
- 580 C-3.A.2. Notify organization providing BCP.
- 581 C-3.A.3. Execute JFHQ-DODIN distributed TASKORDs.

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

- 583 C-3.B.1. Execute initial cloud activity assessment, Section C-3.A.
- 584 C-3.B.2. If organization providing MCP finds no incident as a result of initial cloud activity
585 assessment:
- 586 a) Close out JIMS Cat 9/report no incident to the JFHQ-DODIN via situational awareness
587 report; share with organizations providing BCP.
- 588 b) Send update to mission owner.
- 589 c) Stop this procedure at this step.
- 590 C-3.B.3. If the organization providing MCP finds DOD impact as a result of initial cloud activity
591 assessment:
- 592 a) Update JIMS ticket to proper category (e.g. CAT 1; CAT 2).

UNCLASSIFIED

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

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

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

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

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

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

603 C-3.C. Response to Unsuccessful Activity Attempt

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

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

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

616 C-3.D. Response to DoS

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

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

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

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

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

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

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

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

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

630 C-3.F. Response to Reconnaissance

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

UNCLASSIFIED

UNCLASSIFIED

- 632 CSP, organization providing BCP, or other:
- 633 a) Investigate reported event or incident for mission owner impact.
- 634 b) Develop a situational awareness report and distribute to mission owner, the JFHQ-DODIN,
635 organization providing BCP, and CSP.
- 636 C-3.F.2. If the reconnaissance event is identified by the mission owner or organization providing
637 MCP:
- 638 a) Develop a situational awareness report.
- 639 b) Distribute situational awareness report to mission owner, the JFHQ-DODIN, organization
640 providing BCP, and CSP.
- 641 C-3.F.3. Determine source or cause of reconnaissance for signs of unauthorized access or
642 malware.
- 643 a) If unauthorized access or malware is discovered, refer to those procedures.
- 644 b) Update situational awareness report and resend.
- 645 C-3.F.4. Determine need, if any, for preventative countermeasures on the mission owner systems,
646 applications, cloud service, or connection configuration to the CSP, and direct changes by the
647 mission owner or request changes by the organization providing BCP or CSP.
- 648 C-3.G. Response to Malicious Logic
- 649 C-3.G.1. Malware may be identified in the course of ongoing monitoring or in response to an
650 organization providing BCP TIPR.
- 651 a) Notify CSP for awareness. If malware is detected, open JIMS ticket (CAT 7).
- 652 b) Investigate and report to JFHQ-DODIN with copies to organization providing BCP and
653 CSP, if MCP is notified of a malware impact assessment (e.g. by organization providing BCP
654 or triggered by identified malware on another mission owner system).
- 655 C-3.G.2. Support consolidating tickets at the direction of the JFHQ-DODIN, if the JFHQ-DODIN
656 determines multi-mission owner impact.
- 657 C-3.G.3. Execute JFHQ-DODIN distributed TASKORDs.
- 658 C-3.G.4. Close ticket, if MCP still owns the JIMS ticket.
- 659 C-3.H. Response to Explained Anomaly
- 660 C-3.H.1. Execute initial cloud activity assessment, Section C-3.A.
- 661 C-3.H.2. Implement process or tool update to reduce occurrence of Explained Anomaly, if
662 possible.
- 663 C-3.I. Response to Spillage or Unauthorized Disclosure
- 664 After organization providing MCP identifies or receives notice of a spillage/unauthorized
665 disclosure:
- 666 C-3.I.1. Report spillage or unauthorized disclosure via situational awareness report to the JFHQ-
667 DODIN; copy relevant organization providing BCP.
- 668 C-3.I.2. Support mission owner and CSP in the spillage or unauthorized disclosure investigation
669 and remediation.

UNCLASSIFIED

UNCLASSIFIED

670 C-3.I.3. Periodically update the JFHQ-DODIN and relevant organization providing BCP for SA.
671 C-3.I.4. Notify the JFHQ-DODIN and relevant organization providing BCP of completion via
672 updated situational awareness report when mission owner reports completion.

673 C-3.J. Performing Vulnerability Scans

674 C-3.J.1. Receive notice of vulnerability scans schedule from mission owner.
675 C-3.J.2. Share vulnerability scans schedule with the JFHQ-DODIN and organization providing
676 BCP.
677 C-3.J.3. Receive results and POA&M from mission owner after performance of vulnerability
678 scans.
679 C-3.J.4. Confirm reporting of compliance with USCYBERCOM per TASKORD.
680 C-3.J.5. Report POA&M to JFHQ-DODIN; share with organization providing BCP.

681 C-3.K. Performing Annual External Assessments

682 C-3.K.1. Coordinate mission owner request type (e.g. Red Team, Blue Team, Penetration
683 Testing, etc.).
684 a) Evaluate capabilities required to perform requested external assessment and compare
685 against current capability and capacity.
686 b) Share plan with organization providing BCP and the JFHQ-DODIN of type and period of
687 assessment.
688 c) Confirm notification to CSP via mission owner.
689 C-3.K.2. Conduct coordination for requested assessment, if capable and follow reporting
690 requirements per defined deconfliction process with the JFHQ-DODIN.
691 C-3.K.3. Send request to the JFHQ-DODIN, if the organization providing MCP cannot perform
692 requested assessment.
693 C-3.K.4. Perform the assessment, provide a full report of findings and recommendations to the
694 requesting mission owner and the JFHQ-DODIN; share report with organization providing BCP.
695 C-3.K.5. Receive remediation plan and POA&Ms from mission owner.

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

697 C-3.L.1. Receive notice from mission owner of patch schedule and outage.
698 C-3.L.2. Notify the JFHQ-DODIN and applicable organization providing BCP of patch schedule
699 and outage.
700 C-3.L.3. Ensure after CM and patching is complete, mission owner reports restoration of service
701 and success of patch deployment to organization providing MCP and the JFHQ-DODIN per
702 orders process.
703 C-3.L.4. Notify the JFHQ-DODIN and BCP of restoration of service.

704 C-3.M. Performing Planned Outage

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

UNCLASSIFIED

UNCLASSIFIED

- 707 C-3.M.2. Notify organization providing BCP of schedule updates or anomalies during execution.
- 708 C-3.M.3. Receive notice from mission owner after restoration of service.
- 709 a) Notify the JFHQ-DODIN of service restoration; share with organization providing BCP.
- 710 b) Provide updated CM and patching documentation to organization providing BCP.
- 711 C-3.N. Response to Unplanned Outage
- 712 C-3.N.1. Coordinate with mission owner to assess impact.
- 713 C-3.N.2. Report outage and impact to JFHQ-DODIN; share outage and impact information to
- 714 relevant organization providing BCP.
- 715 C-3.N.3. Track status with mission owner and CSP until closure or resolution.
- 716 C-3.N.4. Provide periodic updates to JFHQ-DODIN until closure/resolution; share with relevant
- 717 organization providing BCP.
- 718 C-3.O. Performing Disaster Recovery
- 719 C-3.O.1. Assist mission owner upon request in executing disaster recovery procedures to restore
- 720 cloud-hosted functionality.
- 721 C-3.P. Response to Training and Exercises
- 722 C-3.P.1. Execute initial cloud activity assessment, Section C-3.A.

UNCLASSIFIED

723 **ANNEX D: MISSION OWNER**

724 **D-1. Mission Owner Introduction**

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

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

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

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

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

750 **D-2. Mission Owner Responsibilities**

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

- 757 D-2.A. Will provide to the organization providing MCP:
- 758 D-2.A.1. Architecture drawings.
- 759 a) Physical and logical.
- 760 b) System descriptions (IP address, system name, description, operating system versions, list
- 761 of expected protocols, configurations, etc.).
- 762 D-2.A.2. Mission owner POCs' information to be used by the organization providing MCP to
- 763 request information or issue directives or orders.
- 764 D-2.A.3. Copies of SLA to the organization providing MCP.
- 765 D-2.B. Will Establish the Secure Logical Connection
- 766 D-2.B.1. For a dedicated connection to the CSO, request connection through a BCAP.
- 767 D-2.B.2. Provide CSP list of authorized connections.
- 768 D-2.B.3. Through CSP, confirm unauthorized attempts to connect to CSO are refused.
- 769 D-2.C. Will maintain a POC list.
- 770 D-2.C.1. Maintain current contact lists for POCs at organizations providing MCP and BCP , and
- 771 CSP for:
- 772 a) Event and incident response reporting, including guidance, orders, and reporting.
- 773 b) Cyberspace protection coordination, including situational awareness reports distribution
- 774 and information sharing.
- 775 c) Distribution lists for situational awareness reports, POA&Ms, external assessments (plans,
- 776 reports, and findings), vulnerability scan schedules, and outage notices.
- 777 D-2.C.2. Maintain mission owner POC list; distribute changes to POC list to organizations
- 778 providing MCP, and BCP, and the CSP.
- 779 D-2.C.3. The CSP will maintain a current CSP Technical POC list, which the mission owner will
- 780 provide to the relevant organizations providing MCP and BCP.
- 781 D-2.D. Will Establish Communication Plans
- 782 D-2.D.1. Add the organization providing MCP and BCP for off premises cloud services to
- 783 Trusted Disclosure list in SLA.
- 784 D-2.D.2. Notify the organization providing MCP and CSP of maintenance windows.
- 785 D-2.D.3. Notify the organization providing MCP and CSP of Periods of Non-Disruption
- 786 (PONDs)
- 787 D-2.D.4. In the case of a cloud service outage (planned or unplanned), the mission owner will
- 788 report the outage or plan for outage to the organization providing MCP.
- 789 D-2.D.5. Establish plan for providing updates to open vulnerability POA&M to the organization
- 790 providing MCP.
- 791 D-2.D.6. Incorporate situational awareness report communication requirements into SLA.

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

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

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

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

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

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

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

799 D-2.F. Incident Response Plan

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

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

802 a) Communication plans

803 b) Thresholds for reporting

804 c) Requirement to comply with designated organization providing MCP

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

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

807 D-3.A. Initial Cloud Activity Assessment

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

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

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

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

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

818 D-3.C. Response to Unsuccessful Activity Attempt

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

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

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

UNCLASSIFIED

826 D-3.D. Response to DoS

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

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

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

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

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

836 D-3.F. Response to Reconnaissance

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

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

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

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

846 D-3.G. Response to Malicious Logic

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

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

852 D-3.H. Response to Explained Anomaly

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

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

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

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

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

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

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

UNCLASSIFIED

- 862 D-3.J. Providing Vulnerability Scans
- 863 D-3.J.1. Mission owner provides vulnerability scans and is responsible for reporting compliance
864 to USCYBERCOM per TASKORD.
- 865 D-3.J.2. Mission owner creates POA&M.
- 866 D-3.J.3. Mission owner reports results compliance results, POA&Ms, open items to the
867 organization providing MCP.

868 D-3.K. Providing Annual External Assessments

- 869 D-3.K.1. Coordinate request type (e.g. Red Team, Blue Team, Penetration Testing, etc.) with the
870 organization providing MCP and the CSP.
- 871 D-3.K.2. Receive a full report of findings and recommendations from the organization that
872 provides the assessment.
- 873 D-3.K.3. Report to the organization providing MCP on remediation plans, including applicable
874 POA&Ms.

875 D-3.L. Providing CM and Patching

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

- 877 D-3.L.1. Mission owner receives requirement to patch systems/apps (is accountable for
878 compliance).
- 879 D-3.L.2. Mission owner acquires or develops patch.
- 880 D-3.L.3. Mission owner tests patch.
- 881 a) Mission owner follows configuration control board (CCB) process as defined by its
882 component to ensure that any patches implemented do not adversely affect the functionality
883 of the cloud-hosted systems and cloud service.
- 884 b) If outage is required, follow the planned outage for DOD to CSP and DOD authorized
885 service interruption (ASI) process.
- 886 c) Validate operations.
- 887 D-3.L.4. Mission owner notifies the organization providing MCP of patch schedule and outage.
- 888 D-3.L.5. Mission owner applies the patch.
- 889 D-3.L.6. Mission owner reports restoration of service and success of patch deployment to the
890 organization providing MCP and JFHQ-DODIN per orders process.
- 891 D-3.L.7. Mission owner provides updated CM and patching documentation to the organization
892 providing MCP.

893 D-3.M. Providing Planned Outage

- 894 D-3.M.1. If the planned outage is initiated by the DOD organization.
- 895 a) Mission owner plans outage.
- 896 b) Mission owner notifies CSP.
- 897 c) Mission owner notifies the organization providing MCP of planned outage, including if
898 COOP or devolution procedures are required.

UNCLASSIFIED

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

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

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

904 b) Mission owner notifies the organization providing MCP.

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

907 D-3.N. Response to Unplanned Outage

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

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

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

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

913 D-3.O. Providing Disaster Recovery

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

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

917 D-3.P. Response to Training and Exercises

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

919 **ANNEX E: CSP**

920 **E-1. CSP Introduction**

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

928 Per the DOD Cloud Computing SRG, all DOD information and data placed or created in a CSP's cloud
929 service is owned by the DOD mission owner and information owner unless otherwise stipulated in a
930 CSP's contract with the DOD organization¹⁶.

931 CSP reporting channels will be different for cloud services under FedRAMP vs. DOD PA. All Level
932 2/4/5 Commercial CSPs will report all incidents via the online DIB Cyber ICF¹⁷. These and additional
933 requirements for a CSP must be specified in the SLAs covering the relationships between a CSP and each
934 of the mission owners.

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

937 **E-2. CSP Responsibilities**

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

940 E-2.A. Provides to the mission owner

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

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

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

944 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"

945 E-2.B. Maintains a POC list

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

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

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

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

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

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

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

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

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

965 **E-3. CSP Cyber Event and Incident Procedures**

966 E-3.A. Initial Cloud Activity Assessment

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

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

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

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

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

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

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

980 E-3.C. Response to Unsuccessful Activity Attempt

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

UNCLASSIFIED

- 983 E-3.D. Response to DoS
- 984 E-3.D.1. Execute CSP initial cloud activity assessment, Section E-3.A.
- 985 E-3.E. Response to Non-Compliance Activity
- 986 E-3.E.1. Execute CSP initial cloud activity assessment, Section E-3.A.
- 987 E-3.F. Response to Reconnaissance
- 988 E-3.F.1. If the event is identified by the CSP, the CSP develops a situational awareness report and
- 989 distributes it to the impacted mission owners.
- 990 E-3.G. Response to Malicious Logic
- 991 E-3.G.1. Execute CSP initial cloud activity assessment, Section E-3.A.
- 992 E-3.H. Response to Explained Anomaly
- 993 E-3.H.1. Execute initial cloud activity assessment, Section E-3.A.
- 994 E-3.H.2. If possible, identify process or tool updates to reduce occurrence of explained anomaly
- 995 and recommend or implement changes IAW specified contractual agreements.
- 996 E-3.I. Response to Spillage and Unauthorized Disclosure
- 997 E-3.I.1. Execute CSP initial cloud activity assessment, Section E-3.A.
- 998 E-3.I.2. Support investigation into spillage or unauthorized disclosure by mission owner and the
- 999 organization proving MCP.
- 1000 E-3.I.3. Support mission owner and the organization providing MCP in remediation effort.
- 1001 E-3.I.4. If directed by mission owner, execute CSP data spill or unauthorized disclosure cleanup
- 1002 method as defined in CSO PA Assessment.
- 1003 E-3.J. Performing Vulnerability Scans
- 1004 E-3.J.1. CSP performs vulnerability scans within the cloud service authorization boundary.
- 1005 E-3.J.2. CSP creates POA&M.
- 1006 E-3.J.3. CSP reports results to FedRAMP PMO and all parties specified in the contractual
- 1007 agreement.
- 1008 E-3.K. Performing Annual External Assessments
- 1009 E-3.K.1. If the CSP provides some of the controls to the mission owner via the SLA, then:
- 1010 a) CSP receives notice from the mission owner of an annual external assessment plan.
- 1011 b) CSP coordinates resources to support mission owner's annual external assessment (e.g.,
- 1012 Pen Test, Red Team, etc.).
- 1013 c) CSP delivers data packages to mission owner to complete its role in the annual external
- 1014 assessment.

UNCLASSIFIED

UNCLASSIFIED

- 1015 E-3.L. Performing Configuration Management (CM) and Patching
1016 Patching is a required routine activity. CSPs and mission owners can incorporate into their SLA that
1017 mission owners will utilize FedRAMP reports to satisfy CSP reporting responsibilities to the mission
1018 owner.
- 1019 E-3.L.1. CSP receives a patch for systems and applications of the cloud service.
1020 E-3.L.2. CSP follows reporting responsibilities to FedRAMP, US-CERT, and mission owner.
1021 E-3.L.3. CSP follows defined patch process. If outage is required, CSP will follow Section E-
1022 3.M, performing planned outage procedures.
1023 E-3.L.4. CSP reports restoration of service and success of patch deployment to the mission
1024 owner, FedRAMP PMO, and US-CERT.
- 1025 E-3.M. Performing Planned Outage
1026 E-3.M.1. If the planned outage is initiated by CSP
1027 a) CSP plans outage.
1028 b) CSP notifies mission owners.
1029 c) If CSO operates under FedRAMP authorization, CSP notifies US-CERT and FedRAMP
1030 PMO.
1031 d) At conclusion of planned outage, CSP notifies mission owners of restoration of service.
1032 E-3.M.2. If the planned outage is initiated by DOD, the CSP will be notified of planned outage by
1033 mission owners.
- 1034 E-3.N. Response to Unplanned Outage
1035 E-3.N.1. CSP notifies mission owners.
1036 E-3.N.2. If CSO operates under FedRAMP authorization, CSP notifies US-CERT and FedRAMP
1037 PMO.
1038 E-3.N.3. At conclusion of unplanned outage, CSP notifies mission owners of restoration of
1039 service.
- 1040 E-3.O. Performing Disaster Recovery
1041 E-3.O.1. Assist mission owner upon request in executing disaster recovery procedures to restore
1042 cloud-hosted functionality.
- 1043 E-3.P. Response to Training and Exercises
1044 The following procedure pertains to incidents detected by the CSP that are determined to be
1045 associated to a training or exercise event.
- 1046 E-3.P.1. Execute CSP Initial Cloud Activity Assessment, Section E-3.A.

1047 **ANNEX F: CLOUD CYBERSPACE PROTECTION COMMUNICATIONS MATRIX**

1048 The below table represents the means of communications typically available to organizations performing
 1049 cybersecurity activities and DCO internal defensive measures to report or share data regarding events and
 1050 incidents.

1051 **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			

UNCLASSIFIED

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	

UNCLASSIFIED

1053 ANNEX G: REFERENCES

- 1054 (a) Joint Chiefs of Staff. (2012, July). Chairman of the Joint Chiefs of Staff Manual 6510.01B: Cyber
1055 Incident Handling Program. http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf
- 1056 (b) DOD CIO. (2003, December). DOD O-8530.1-M: Department of Defense Computer Network
1057 Defense (CND) Service Provider Certification and Accreditation Process Program Manual.
1058 <https://whsddpubs.dtic.mil/corres/pdf/O853001M.pdf>
- 1059 (c) DOD CIO. (2016, March). DOD Instruction 8530.01: Cybersecurity Activities Support to DOD
1060 Information Network Operations. <http://www.dtic.mil/whs/directives/corres/pdf/853001p.pdf>
- 1061 (d) Defense Information Systems Agency (DISA). (2016, March). DOD Cloud Computing SRG.
1062 <http://iasecontent.disa.mil/cloud/SRG/index.html>
- 1063 (e) DISA. (2014, June). DISA's Strategy for Defensive Cyber Operations.
- 1064 (f) DISN Connection Process Guide (CPG) Home Page. <http://www.disa.mil/Services/Network->
1065 [Services/Enterprise-Connections/Connection-Process-Guide](http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide)
- 1066 (g) FedRAMP Home Page. <http://cloud.cio.gov/fedramp>
- 1067 (h) United States Code, Title 44.
- 1068 (i) National Institute of Standards and Technology. (2011, September). NIST SP800-145: The NIST
1069 Definition of Cloud Computing. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- 1070 (j) US-CERT Federal Incident Reporting Guidelines. [https://www.us-cert.gov/government-](https://www.us-cert.gov/government-users/reporting-requirements#tax)
1071 [users/reporting-requirements#tax](https://www.us-cert.gov/government-users/reporting-requirements#tax)
- 1072 (k) DISA. (2015, June). Cloud Access Point (CAP) Security Functional Requirements Document
1073 (FRD).
- 1074 (l) Joint Chiefs of Staff. (2011, February). Chairman of the Joint Chiefs of Staff Instruction
1075 6510.01F: Information Assurance (IA) and Support to Computer Network Defense (CND).
1076 http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
- 1077 (m) US-CERT. (2014, October). US-CERT Federal Incident Notification Guidelines. [https://www.us-](https://www.us-cert.gov/incident-notification-guidelines)
1078 [cert.gov/incident-notification-guidelines](https://www.us-cert.gov/incident-notification-guidelines)
- 1079 (n) DOD CIO. (2013, August). DOD Instruction 8320.02: Sharing Data, Information, and
1080 Information Technology (IT) Services in the Department of Defense.
1081 www.dtic.mil/whs/directives/corres/pdf/832002p.pdf
- 1082 (o) DOD CIO. (2015, August). DOD Instruction 8320.07: Implementing the Sharing of Data,
1083 Information, and Information Technology (IT) Services in the Department of Defense.
1084 www.dtic.mil/whs/directives/corres/pdf/832007p.pdf

UNCLASSIFIED

UNCLASSIFIED

- 1085 (p) DOD CIO. (2013, March). DOD Manual 5200.01 Vol 3: DOD Information Security Program:
1086 Protection of Classified Information. http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf
- 1087 (q) DOD CIO. (2007, May). DOD 5400.11-R: DOD Privacy Program.
1088 <http://dtic.mil/whs/directives/corres/pdf/540011r.pdf>

UNCLASSIFIED

1089 **ANNEX H: ABBREVIATIONS AND ACRONYMS**

1090	ACAS	Assured Compliance Assessment Solution
1091	APT	advanced persistent threat
1092	AS&W	attack sensing & warning
1093	ATO	authority to operate
1094	AV	anti-virus
1095	BCAP	boundary cloud access point
1096	BCP	boundary cyberspace protection
1097	CAP	cloud access point
1098	CCB	configuration control board
1099	CI	Counterintelligence
1100	CJCS	Chairman of the Joint Chiefs of Staff
1101	CM	configuration management
1102	CMRS	Continuous Monitoring and Risk Scoring
1103	COOP	Continuity of Operations
1104	CPT	cyber protection team
1105	CSO	cloud service offering
1106	CSP	cloud service provider
1107	CSSP	cybersecurity service provider
1108	DCO	defensive cyberspace operations
1109	DIBNET	Defense Industrial Base Network
1110	DISA	Defense Information Systems Agency
1111	DISN	Defense Information Systems Network
1112	DOD	Department of Defense
1113	DoS	denial of service
1114	DODIN	Department of Defense Information Network

UNCLASSIFIED

1115	FedRAMP	Federal Risk and Authorization Management Program
1116	HBSS	Host Based Security System
1117	IaaS	Infrastructure as a Service
1118	IAP	Internet Access Point
1119	ICAP	internal cloud access point
1120	ICF	Incident Collection Format
1121	JAB	Joint Authorization Board
1122	JCC	Joint Cyber Center
1123	JFHQ-DODIN	Joint Force Headquarters DOD Information Network
1124	JIE	Joint Information Environment
1125	JIMS	Joint Incident Management System
1126	LE	Law Enforcement
1127	MCP	Mission Cyberspace Protection
1128	NIST	National Institute of Standards and Technology
1129	NCTOC	National Security Agency/Central Security Service Cyber Threat Operations Center
1130	PaaS	Platform as a Service
1131	PA	Provisional Authorization
1132	POA&M	Plan of Action and Milestones
1133	POND	Period of Non-Disruption
1134	RTO	Recovery Time Objective
1135	SaaS	Software as a Service
1136	SA	Situational Awareness
1137	SIEM	Security Information and Event Management
1138	SLA	Service Level Agreement
1139	SRG	Security Requirements Guide
1140	SQL	Structured Query Language

UNCLASSIFIED

UNCLASSIFIED

- 1141 TIPR Threat Intelligence Product Report
- 1142 US-CERT United States Computer Emergency Readiness Team
- 1143 VPN Virtual Private Network
- 1144 XSS Cross-Site Scripting

1145 **ANNEX I: CLOUD CYBERSPACE PROTECTION DEFINITIONS**

1146 **Boundary Cloud Access Point (BCAP):** DISN perimeter gateway that provides a barrier of protection
1147 between the DISN and the CSO.

1148 **Blue Team:** As defined in CNSSI-4009, “A group of individuals that conduct operational network
1149 vulnerability evaluations and provide mitigation techniques to customers who have a need for an
1150 independent technical review of their network security posture. The Blue Team identifies security threats
1151 and risks in the operating environment, and in cooperation with the customer, analyzes the network
1152 environment and its current state of security readiness. Based on the Blue Team findings and expertise,
1153 they provide recommendations that integrate into an overall community security solution to increase the
1154 customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a
1155 Red Team employment to ensure that the customer's networks are as secure as possible before having the
1156 Red Team test the systems.”

1157 **Breach:** As defined in OMB M-17-12, “the loss of control, compromise, unauthorized disclosure,
1158 unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user
1159 accesses or potentially accesses personally identifiable information or (2) an authorized user accesses
1160 personally identifiable information for an other than authorized purpose.”

1161 **Classified Information:** As defined in CNSSI-4009, “Information that has been determined pursuant to
1162 Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure
1163 and is marked to indicate its classified status when in documentary form.”

1164 **Cloud Service Provider (CSP):** Commercial vendor or Federal organization offering or providing Cloud
1165 services (Includes DOD CSPs); the provider of CSOs.

1166 **Community Cloud:** As defined in NIST SP800-145, “The cloud infrastructure is provisioned for
1167 exclusive use by a specific community of consumers from organizations that have shared concerns (e.g.,
1168 mission, security requirements, policy, and compliance considerations). It may be owned, managed, and
1169 operated by one or more of the organizations in the community, a third party, or some combination of
1170 them, and it may exist on or off premises.”

1171 **Configuration Control Board (CCB):** As defined in CNSSI-4009, “A group of qualified people with
1172 responsibility for the process of regulating and approving changes to hardware, firmware, software, and
1173 documentation throughout the development and operational lifecycle of an information system.”

1174 **Continuous Monitoring:** As defined in CNSSI-4009, “The process implemented to maintain a current
1175 security status for one or more information systems or for the entire suite of information systems on which
1176 the operational mission of the enterprise depends. The process includes: 1) The development of a
1177 strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant
1178 events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA
1179 controls, or changes that affect IA risks, and 4) Publishing the current security status to enable
1180 information sharing decisions involving the enterprise.”

UNCLASSIFIED

1181 **Countermeasure:** As defined in CNSSI-4009, “Actions, devices, procedures, or techniques that meet or
1182 oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing
1183 the harm it can cause, or by discovering and reporting it so that corrective action can be taken.”

1184 **Cybersecurity Service Provider (CSSP):** As defined in DOD Instruction 8530.01, “DOD component or
1185 authorized external DOD Component service provider that provides one or more cybersecurity services
1186 to implement and protect the DODIN.”

1187 **Cyber Incident:** As defined in CNSSI-4009, “Actions taken through the use of computer networks that
1188 result in an actual or potentially adverse effect on an information system and/or the information residing
1189 therein. See incident.”

1190 **Denial of Service (DoS):** As defined in CNSSI-4009, “The prevention of authorized access to resources
1191 or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours,
1192 depending upon the service provided.)”

1193 **Defense Information Systems Network (DISN):** As defined in JP 1-02, “The integrated network,
1194 centrally managed and configured by the Defense Information Systems Agency to provide dedicated
1195 point-to-point, switched voice and data, imagery, and video teleconferencing services for all
1196 Department of Defense activities. Also called DISN. (JP 6-0)”

1197 **DOD Information Network (DODIN):** As defined in JP 1-02, “The set of information capabilities, and
1198 associated processes for collecting, processing, storing, disseminating, and managing information on-
1199 demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone,
1200 including owned and leased communications and computing systems and services, software (including
1201 applications), data, security services, other associated services, and national security systems. Also
1202 called DODIN. (JP 6-0)”

1203

1204 **Event:** As defined in CNSSI-4009, “Any observable occurrence in a system and/or network. Events
1205 sometimes provide indication that an incident is occurring.”

1206 **Gateway:** As defined in CNSSI-4009, “Interface providing compatibility between networks by
1207 converting transmission speeds, protocols, codes, or security measures.”

1208 **Incident:** An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or
1209 availability of an information system; or the information the system processes, stores, or transmits; or that
1210 constitutes a violation or imminent threat of violation of security policies, security procedures, or
1211 acceptable use policies.

1212 **Infrastructure as a Service (IaaS):** As defined in NIST SP 800-145, “The capability provided to the
1213 consumer is to provision processing, storage, networks, and other fundamental computing resources
1214 where the consumer is able to deploy and run arbitrary software, which can include operating systems
1215 and applications. The consumer does not manage or control the underlying Cloud infrastructure but has
1216 control over operating systems, storage, and deployed applications; and possibly limited control of select
1217 networking components (e.g., host firewalls).”

UNCLASSIFIED

UNCLASSIFIED

- 1218 **Joint Authorization Board (JAB):** The primary governance and decision-making body for the
1219 FedRAMP program.
- 1220 **Malware:** From Evaluator Scoring Metrics, “*Malware refers to a program that is covertly inserted into*
1221 *another program with the intent to destroy data, run destructive or intrusive programs, or otherwise*
1222 *compromise the confidentiality, integrity, and/or availability of the victim’s data, application, or*
1223 *information system. Malware is the most common external threat to most hosts, causing widespread*
1224 *damage and disruption and necessitating extensive recovery efforts within most organizations.”*
- 1225 **Penetration Testing:** As defined in CNSSI-4009, “*A test methodology in which assessors, typically*
1226 *working under specific constraints, attempt to circumvent or defeat the security features of an information*
1227 *system.”*
- 1228 **Personally Identifiable Information (PII):** As defined in OMB M-17-12, “*information that can be used*
1229 *to distinguish or trace an individual’s identity, either alone or when combined with other information that*
1230 *is linked or linkable to a specific individual.”*
- 1231 **Platform as a Service (PaaS):** As defined in NIST SP 800-145, “*The capability provided to the*
1232 *consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created*
1233 *using programming languages, libraries, services, and tools supported by the provider. The consumer*
1234 *does not manage or control the underlying Cloud infrastructure including network, servers, operating*
1235 *systems, or storage, but has control over the deployed applications and possibly configuration settings for*
1236 *the application-hosting environment.”*
- 1237 **Private Cloud:** As defined in NIST SP800-145, “*The cloud infrastructure is provisioned for exclusive*
1238 *use by a single organization comprising multiple consumers (e.g., business units). It may be owned,*
1239 *managed, and operated by the organization, a third party, or some combination of them, and it may exist*
1240 *on or off premises.”*
- 1241 **Red Team:** As defined in CNSSI-4009, “*A group of people authorized and organized to emulate a*
1242 *potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red*
1243 *Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of*
1244 *successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an*
1245 *operational environment.”*
- 1246 **Scanning:** As defined in CNSSI-4009, “*Sending packets or requests to another system to gain*
1247 *information to be used in a subsequent attack.”*
- 1248 **Secure State:** As defined in CNSSI-4009, “*Condition in which no subject can access any object in an*
1249 *unauthorized manner.”*
- 1250 **Software as a Service (SaaS):** As defined in NIST SP 800-145, “*The capability provided to the*
1251 *consumer is to use the provider’s applications running on a Cloud infrastructure. The applications are*
1252 *accessible from various client devices through either a thin client interface, such as a web browser (e.g.,*
1253 *web-based email), or a program interface. The consumer does not manage or control the underlying*
1254 *Cloud infrastructure including network, servers, operating systems, storage, or even individual*

UNCLASSIFIED

UNCLASSIFIED

1255 *application capabilities, with the possible exception of limited user-specific application configuration*
1256 *settings.”*

1257 **Spillage or Data Spill:** an unauthorized transfer of classified information or Controlled Unclassified
1258 Information to an information system that is not accredited for the applicable security level of the data or
1259 information.

1260 **Threat:** As defined in CNSSI-4009, “*Any circumstance or event with the potential to adversely impact*
1261 *organizational operations (including mission, functions, image, or reputation), organizational assets,*
1262 *individuals, other organizations, or the Nation through an information system via unauthorized access,*
1263 *destruction, disclosure, modification of information, and/or denial of service.”*

1264 **Virtual Private Network (VPN):** As defined in CNSSI-4009, “*Protected information system link*
1265 *utilizing tunneling, security controls (see Information Assurance), and endpoint address translation*
1266 *giving the impression of a dedicated line.”*

1267 **Vulnerability:** As defined in CNSSI-4009, “*Weakness in an information system, system security*
1268 *procedures, internal controls, or implementation that could be exploited by a threat source.”*

1269 **Vulnerability Assessment:** As defined in CNSSI-4009, “*Systematic examination of an information*
1270 *system or product to determine the adequacy of security measures, identify security deficiencies, provide*
1271 *data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of*
1272 *such measures after implementation.”*

UNCLASSIFIED