



1

2

3

4

**DEPARTMENT OF DEFENSE (DoD)
CONCEPT OF OPERATIONS (CONOPS) FOR
CLOUD COMPUTER NETWORK DEFENSE (CND)**

5

DRAFT v1

6

21 Sep 2015

7

8

9

10

**Developed by the
Defense Information Systems Agency (DISA)
for the
Department of Defense (DoD)**

11

Trademark Information

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

DRAFT

17
18
19
20
21

CONCEPT OF OPERATIONS FOR CLOUD CND

22

TABLE OF CONTENTS

23 **EXECUTIVE SUMMARY 5**

24 **CONCEPT OF OPERATIONS FOR CLOUD CND: BASE PLAN 7**

25 **1. Introduction..... 7**

26 **2. Background 8**

27 **3. Cyber Event and Incident Response Matrix 12**

28 **ANNEX A: DODIN CND 19**

29 **A-1. DoDIN CND Introduction..... 19**

30 **A-2. DoDIN CND Responsibilities..... 19**

31 **A-3. DoDIN CND Cyber Incident and Event Procedures..... 20**

32 **ANNEX B: BCND 25**

33 **B-1. BCND Introduction 25**

34 **B-2. BCND Responsibilities..... 25**

35 **B-3. BCND Cyber Incident and Event Procedures..... 26**

36 **ANNEX C: MCND..... 31**

37 **C-1. MCND Introduction 31**

38 **C-2. MCND Responsibilities 31**

39 **C-3. MCND Cyber Incident and Event Procedures 32**

40 **ANNEX D: MISSION OWNER 37**

41 **D-1. Mission Owner Introduction..... 37**

42 **D-2. Mission Owner Responsibilities..... 37**

43 **D-3. Mission Owner Cyber Incident and Event Procedures..... 39**

44 **ANNEX E: JFHQ-DODIN 43**

45 **E-1. JFHQ-DoDIN Introduction..... 43**

46 **E-2. JFHQ-DoDIN Responsibilities..... 43**

47 **E-3. JFHQ-DoDIN Cyber Incident and Event Procedures..... 44**

48 **ANNEX F: CSP 47**

49 **F-1. CSP Introduction 47**

50 **F-2. CSP Responsibilities..... 47**

51 **F-3. CSP Cyber Incident and Event Procedures..... 48**

52 **ANNEX G: CLOUD CND COMMUNICATIONS MATRIX 52**

53 **ANNEX H: REFERENCES 55**

54 **ANNEX I: ABBREVIATIONS AND ACRONYMS..... 57**

55 **ANNEX J: CLOUD CND DEFINITIONS..... 60**

56 **TABLE OF TABLES**

57 **Table 1 – Cyber Event and Incident Response Matrix..... 13**

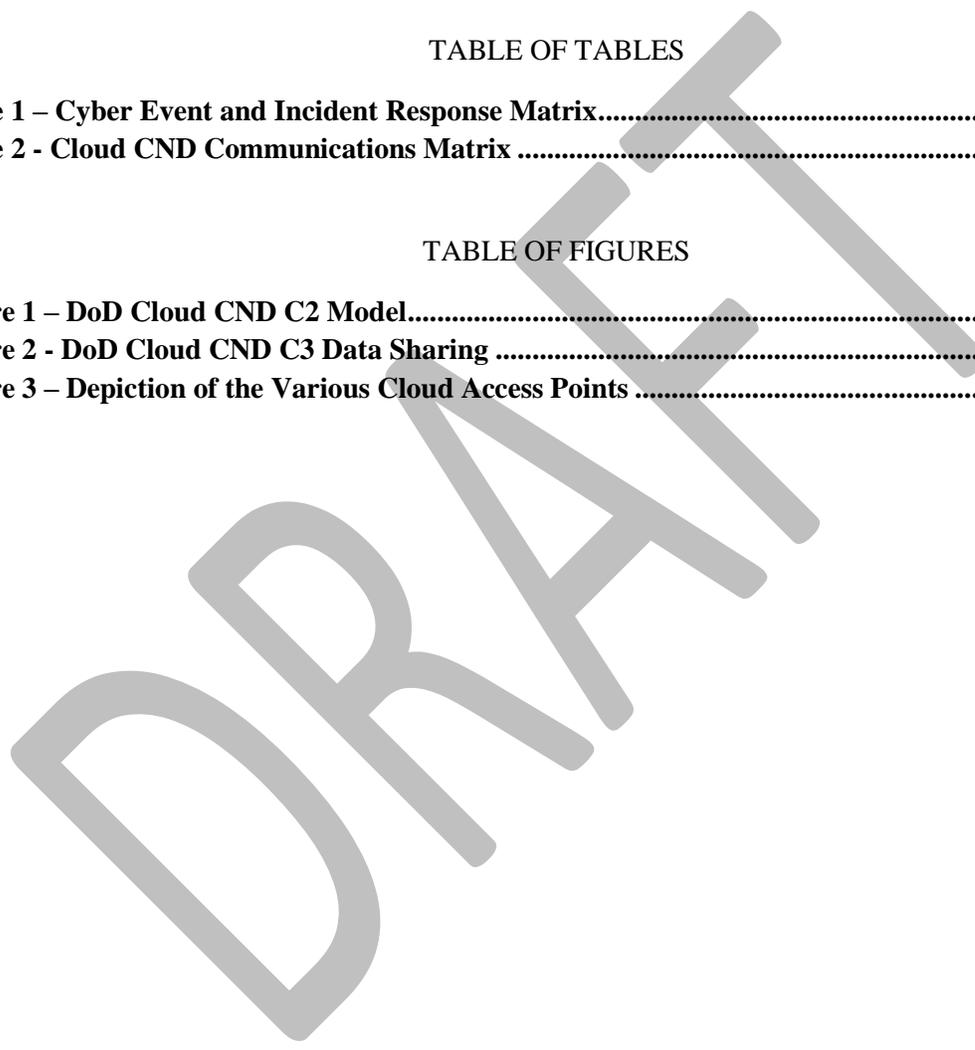
58 **Table 2 - Cloud CND Communications Matrix 52**

59 **TABLE OF FIGURES**

60 **Figure 1 – DoD Cloud CND C2 Model..... 10**

61 **Figure 2 - DoD Cloud CND C3 Data Sharing 11**

62 **Figure 3 – Depiction of the Various Cloud Access Points 12**



63 **EXECUTIVE SUMMARY**

64 The Cloud Computer Network Defense (CND) CONOPS defines a set of reporting and incident handling
65 procedures for the organizations that will defend the Department of Defense (DoD) Information Network
66 (DoDIN) in the cloud, as specified in the Cloud Computing Security Requirements Guide (SRG) section
67 on CND and Incident Response. This CONOPS defines how Mission Owners, Mission CND (MCND),
68 Boundary CND (BCND), DoDIN CND, Cloud Service Providers¹ (CSPs), and Joint Force Headquarters
69 DoDIN (JFHQ-DoDIN) shall cooperate in response to cyber incidents and events in accordance with
70 Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B.

71 This document introduces the supporting organizations and reference procedures for achieving the two
72 objectives for CND of the DoDIN with regards to the cloud:

- 73 1. BCND: Defend the Defense Information Systems Network (DISN) from an attack utilizing the
74 external Cloud.
- 75 2. MCND: Defend systems, applications, and/or data hosted within the Cloud.

76 The quantity of combinations of cloud solutions expands to hundreds of potential combinations of service
77 models, delivery models, DoD CSP Process, which encompasses the Federal Risk and Authorization
78 Management Program (FedRAMP) v. Agency Authority to Operate (ATO), connection methods (e.g. On-
79 Premise v. Off-Premise), Information Impact Levels, and other parameters.

80 This document expands on the SRG with the introduction of the Cloud CND Command and Control (C2)
81 model and the Cloud CND Command, Control, and Communications (C3) Data Sharing model, defining
82 reporting and data-sharing relationships between the CND and Cloud organizations. DoDIN CND will
83 also aggregate MCND reporting and perform cross-CSP correlation to identify incidents and events that
84 span multiple Missions hosted in the Cloud.

85 Lastly, it introduces the Cyber Event and Incident Response Matrix for each role identified below. This
86 matrix assigns procedures to be performed in response to incidents and events as categorized by DoD.
87 The procedures are introduced and expanded with role-specific workflows in the annexes.

88 The annexes provide detailed responsibilities and procedures for the major roles specified in the DoD
89 Cloud Computing SRG. The procedures are written in the most comprehensive form, for an externally
90 hosted commercial Infrastructure as a Service (IaaS) Cloud Service Offering (CSO), with annotations for
91 recommended tailoring and considerations for Platform as a Service (PaaS) or Software as a Service
92 (SaaS), for On-Premise hosting, and/or for DoD hosting. This document does not outline procedures or
93 processes for deploying/implementing CND services in the cloud.

94 The roles that are elaborated in the annexes are:

¹ Mission Owner, MCND, BCND, and CSPs are defined in Section 6.3 “CND Roles and Responsibilities” of reference (d), the DoD Cloud Computing SRG

UNCLASSIFIED

- 95 • Annex A – DoDIN CND
- 96 • Annex B – BCND
- 97 • Annex C – MCND
- 98 • Annex D – Mission Owner
- 99 • Annex E – JFHQ-DoDIN
- 100 • Annex F – CSP

101

102 This document is expected to evolve as the procedures are put into practice and new best practices
103 emerge. It will track changes in the Cloud Computing SRG, CJCSM 6510.01B, and Joint Information
104 Environment (JIE) implementation strategies. As such it should be treated as a foundation upon which to
105 improve in addition to providing uniformity and efficient cooperation in Cloud CND.

DRAFT

106
107
108

109

110

111 **CONCEPT OF OPERATIONS FOR CLOUD CND: BASE PLAN**

112 **1. Introduction**

113 1.A. General.

114 This document extends the Department of Defense (DoD) Cloud Computing Security Requirements
115 Guide (SRG) with reference procedures for Cloud Computer Network Defense (CND). The DoD Cloud
116 Computing SRG defined a CND Command and Control (C2)² structure with Mission CND (MCND) and
117 Boundary CND (BCND) as unique elements with separate missions. It establishes expectations for two
118 CND objectives supporting defense of the DoD Information Network (DoDIN) with regard to the cloud:

- 119 1. BCND: The primary objective of the BCND is to protect the Defense Information Systems
120 Network (DISN) from attacks utilizing public, private, hybrid, or community clouds, through
121 approved Cloud Service Providers (CSPs) that can impact the DISN through a dedicated
122 connection via a Boundary Cloud Access Point (BCAP). The BCND furthermore supports the
123 MCNDs in their objectives of defending their systems, applications, and data hosted in the
124 Cloud. In that capacity, the BCND builds a broad Cyber Situational Awareness (SA) picture
125 across Missions, Cloud Service Offerings (CSOs), and CSPs and can identify broader patterns
126 of incidents or events.
- 127 2. MCND: The primary objective of the MCND is to defend systems, applications, and and/or
128 data hosted in the Cloud. The MCND defends all connections to the CSO, whether via BCAP,
129 Internal Cloud Access Point (ICAP), Virtual Private Network (VPN), direct internet access to
130 public servers, or other. The MCND monitors activities committed with privileged
131 connections (e.g. Cloud management or Mission application administration) and monitors for
132 attacks against the Mission applications (e.g. Structured Query Language (SQL) injection).
133 The MCND supports BCND efforts to identify correlations between related incidents or events
134 impacting multiple Missions, CSOs, or CSPs.

135 The reference procedures defined in this document establish specific interactions between the BCND,
136 MCND, Mission Owner, Joint Force Headquarters DoDIN (JFHQ-DoDIN)/DoDIN CND, and the CSP to
137 execute the CND mission. These interactions are defined in a way to support the full range of cloud

² Section 6.3 of reference (d): DoD Cloud Computing SRG

138 solutions that DoD may utilize and to support the transition to the Joint Information Environment (JIE) by
139 establishing CND C2 and Command, Control, and Communications (C3) models for global Cyber SA.

140 1.B. Purpose and Audience.

141 The purpose of this document is to establish workflows and expectations between the DoDIN CND,
142 BCND, MCNDs, Mission Owners, JFHQ-DoDIN, and the CSPs who together will defend the
143 applications, data and systems on DoD and non-DoD cloud solutions. This document does not replace
144 existing reporting requirements.

145 1.C. Scope and Applicability.

146 This document applies to all DoDIN CND, MCND, BCND, Mission Owner, and JFHQ-DoDIN activities
147 as they relate to Cloud CND.

148 **2. Background**

149 Cloud expands the scope of the DoDIN defensible surface while potentially reducing the direct authority
150 to sense or defend the DoDIN through traditional touch points, such as in the cases of Platform as a
151 Service (PaaS) and Software as a Service (SaaS). In addition, as new capability delivery models are
152 created in the commercial arena, DoD will likewise evolve its approach to Cloud CND for the DoDIN.

153 2.A. Moving to the Cloud

154 As applications and capability are moved to the Cloud, Mission Owners will select CSOs offered by
155 CSPs. CSOs will be offered in three Service Models³:

- 156 • Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision
157 processing, storage, networks, and other fundamental computing resources where the consumer is
158 able to deploy and run arbitrary software, which can include operating systems and applications.
159 The consumer does not manage or control the underlying cloud infrastructure but has control over
160 operating systems, storage, and deployed applications; and possibly limited control of select
161 networking components (e.g., host firewalls).
162
- 163 • Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud
164 infrastructure consumer-created or acquired applications created using programming languages,
165 libraries, services, and tools supported by the provider. (This capability does not necessarily
166 preclude the use of compatible programming languages, libraries, services, and tools from other
167 sources.) The consumer does not manage or control the underlying cloud infrastructure including
168 network, servers, operating systems, or storage, but has control over the deployed applications
169 and possibly configuration settings for the application-hosting environment.
170

³ Ref (i): Definitions from National Institute of Standards and Technology (NIST) SP 800-145: The NIST Definition of Cloud Computing

171 • Software as a Service (SaaS): The capability provided to the consumer is to use the provider's
 172 applications running on a cloud infrastructure. (A cloud infrastructure is the collection of
 173 hardware and software that enables the five essential characteristics of cloud computing. The
 174 cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer.
 175 The physical layer consists of the hardware resources that are necessary to support the cloud
 176 services being provided, and typically includes server, storage and network components. The
 177 abstraction layer consists of the software deployed across the physical layer, which manifests the
 178 essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.)
 179 The applications are accessible from various client devices through either a thin client interface,
 180 such as a web browser (e.g., web-based email), or a program interface. The consumer does not
 181 manage or control the underlying cloud infrastructure including network, servers, operating
 182 systems, storage, or even individual application capabilities, with the possible exception of
 183 limited user-specific application configuration settings.

184 With three Service Models (IaaS, PaaS, and SaaS)⁴, four Deployment Models (Public, Community,
 185 Private, and Hybrid)⁴, multiple Provisional Authorization (PA) types (e.g. Federal Risk and Authorization
 186 Management Program (FedRAMP) Joint Authorization Board (JAB) PA and DoD FedRAMP+ PA)⁵, four
 187 DoD Data Impact Levels (2, 4, 5, and 6)⁵, and at least three connection models (BCAP, ICAP, and public
 188 internet)⁶, if treated separately a complete exploration of the permutations could consider hundreds of
 189 variations.

190 This document, therefore, approaches this variability from the perspective of cyber event or incident
 191 types. As defined in the section titled Cyber Incident and Reportable Cyber Event Categorization of the
 192 Cyber Incident Handling Program⁷, DoD recognizes ten distinct categories of cyber incidents and
 193 reportable events. For each incident or event category, a reference procedure is described with conditional
 194 steps based on the Service Model, Delivery Model, etc., of the Mission Applications and Systems and the
 195 CSOs on which they reside. An overview of each procedure is described in Section 3 of this Base Plan,
 196 with workflows specified within this document's Annexes.

197 2.B. Cloud CND C2 Model and C3 Data Sharing Structure

198 The DoD Cloud Computing SRG defines a CND reporting and communication structure for cloud. This
 199 structure supports the information flows that will be necessary to support global cyber situational
 200 awareness and the JIE. The Cloud Computing SRG introduced the separation of CND responsibilities
 201 between the BCND and MCND. The BCND will monitor and defend the DISN perimeter where BCAP
 202 connections to CSPs are supported. The MCNDs will monitor and defend the systems, applications, and
 203 data that are remotely hosted on the CSO on behalf of their Mission Owners. Each Mission Owner will
 204 identify a certified CND Service Provider (CNDSP) to perform the MCND role for its systems,

⁴ Ref (i): NIST SP800-145 "The NIST Definition of Cloud Computing"

⁵ Ref (d): DoD Cloud Computing SRG

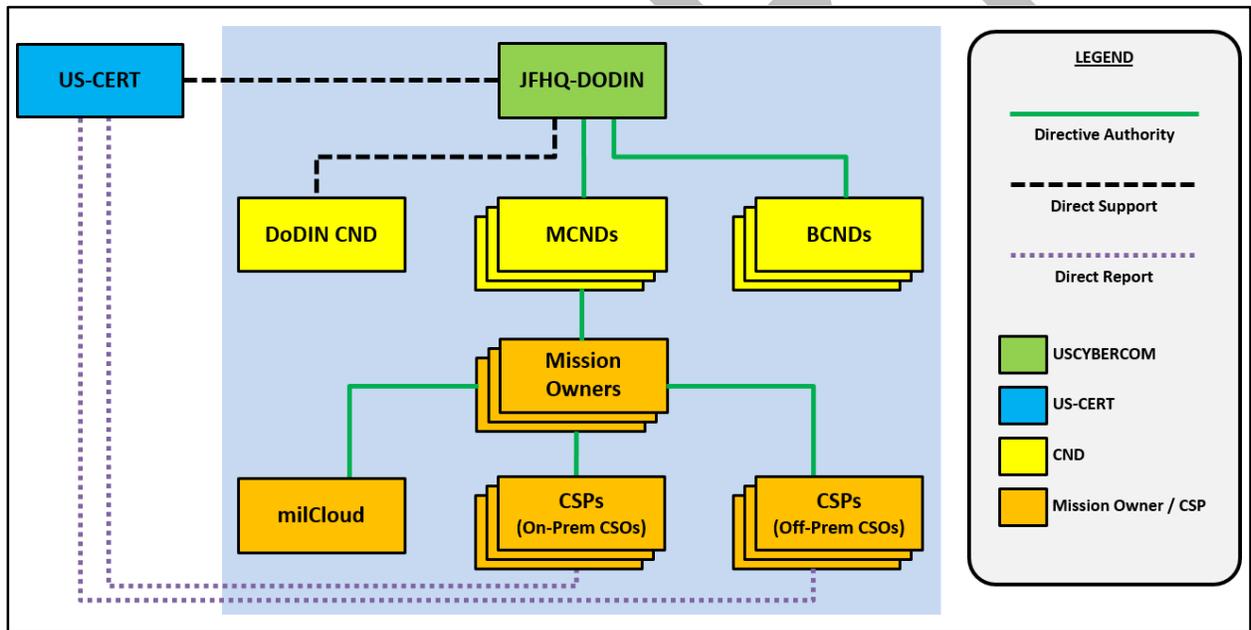
⁶ Ref (k): Cloud Access Point (CAP) Security Functional Requirements Document (FRD)

⁷ Ref (a): CJCSM 6510.01B "Cyber Incident Handling Program"

205 applications, and data. Each BCAP will have a certified CNDSP to perform the BCND role for that
206 BCAP.

207 The scope of CND responsibility for the MCND and the CSP will depend on the features of the CSO. In
208 the case of oOff-Premise SaaS CSOs, for example, the CSP may perform the majority of 24x7 incident
209 and event detection. The Mission Owner is still responsible for complying with CYBERCOM and JFHQ
210 DoDIN Directives and Tasks (e.g. CYBERCON). The MCND would still assist with implementation or
211 elevate concerns on behalf of their customers to JFHQ DoDIN or CYBERCOM. The MCND will always
212 retain the responsibility of reporting to JFHQ-DODIN and responding to JFHQ-DODIN TASKORDs, as
213 well as sharing CND data to peer MCNDs, BCNDs, and DoDIN CND to enable CND collaboration.

214 Figure 1 depicts the Cloud CND C2 model. JFHQ-DoDIN has direct tasking authority over DoDIN CND,
215 BCNDs, and MCNDs. JFHQ-DoDIN, as part of USCYBERCOM, has legal authority to collaborate with
216 entities external of DoD, such as the United States Computer Emergency Readiness Team (US-CERT).
217 The Mission Owners, as the CSO subscribers to the CSPs, are the default C2 relationship to the CSPs.
218 Mission Owners can optionally expand CND-relevant reporting to their selected MCNDs and BCNDs by
219 including such language in their Service Level Agreements (SLAs).

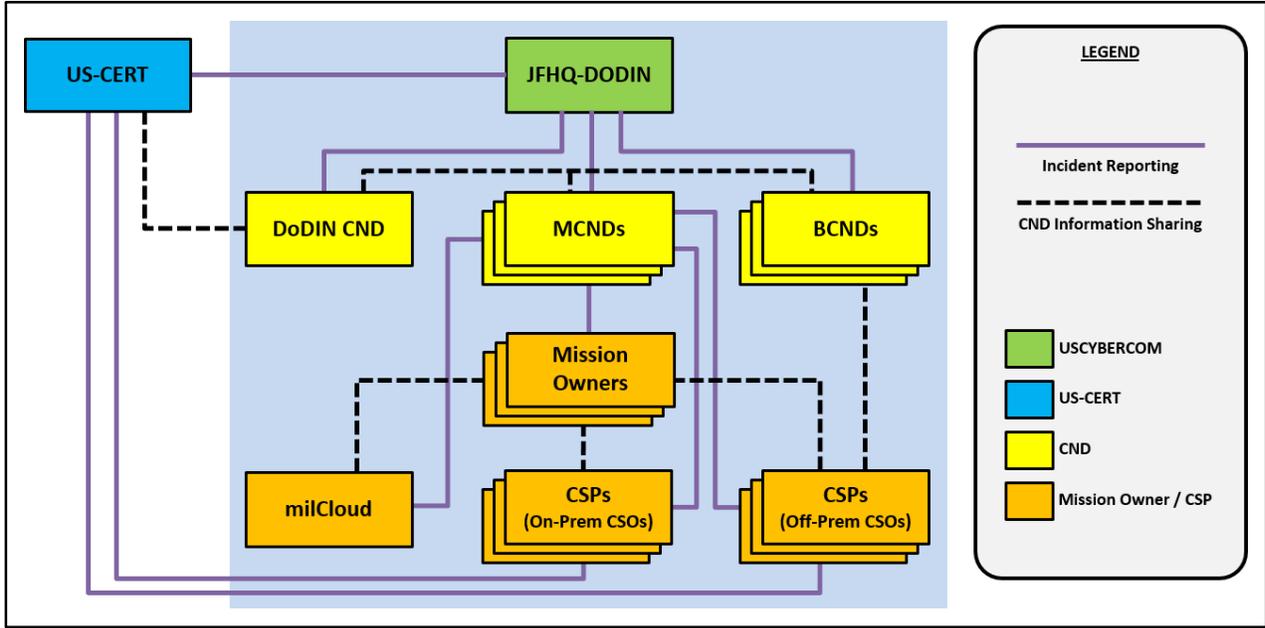


220

221

Figure 1 – DoD Cloud CND C2 Model

222 To support JFHQ-DoDIN, DoDIN CND performs Cross-Cloud Analysis (XCA) to enable “populate once
223 and reuse many”, enabled by the CND Data Sharing (see Figure 2). Given that a single CSP may provide
224 multiple and simultaneous service offerings for different Mission Owners, for each CSP, DoDIN-CND
225 will analyze potential impacts across the multiple missions, CSOs, and CSPs based on information
226 coming from the MCNDs.



227

228

Figure 2 - DoD Cloud CND C3 Data Sharing

229 **ANNEX A: The Cloud CND C3 data sharing structure builds a comprehensive cyber SA picture**
 230 **across the MCNDs, BCNDs, DoDIN CND, JFHQ-DoDIN and the CSPs. Incident and event data is**
 231 **correlated at the DoDIN CND and JFHQ-DoDIN to minimize duplication of effort, minimize**
 232 **miscommunication (e.g. different descriptions for “same” incident spanning multiple CSOs),**
 233 **improve responsiveness and enable greater proactive defense for the Mission Owners across all of**
 234 **the CSOs. ANNEX H: CLOUD CND COMMUNICATIONS MATRIX**

235 The below table represents the means of communications available to be used by CND Organization to
 236 report or share data regarding CDN incidents and events. atrix shows the means of communication used
 237 between the organizations shown on Figure 2. New or modified information exchanges will be
 238 implemented in accordance with DoD Instruction (DoDI) 8320.02 and DoDI 8320.07.

239 **2.C. CSOs**

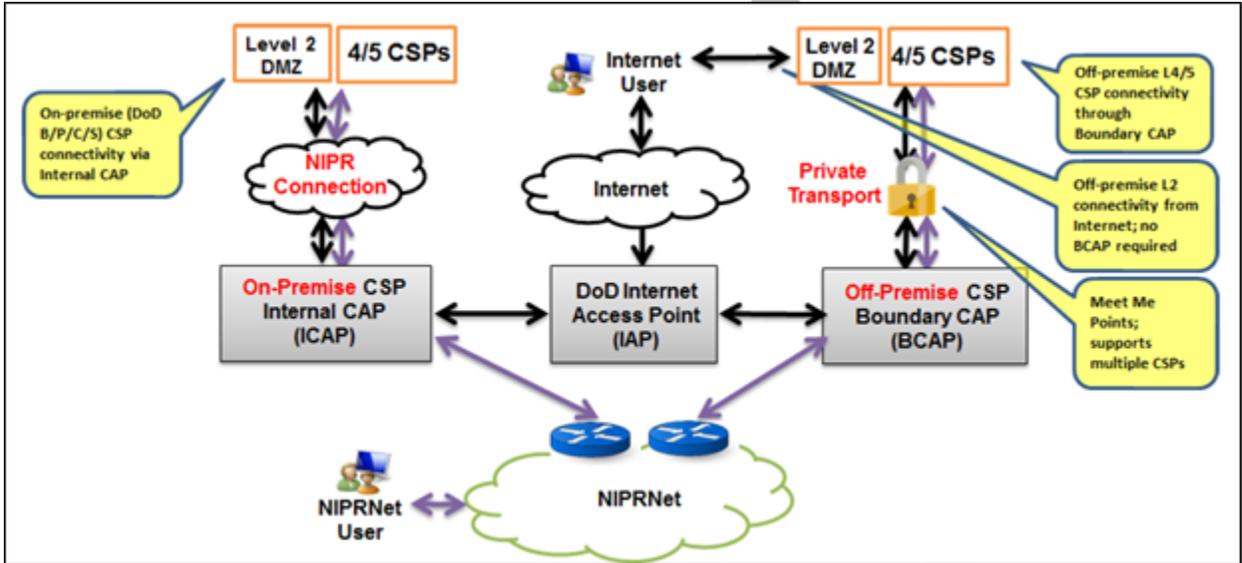
240 There are three CSOs that a Mission Owner can select to host their data. The CSOs are milCloud, CSP
 241 On-Premise, CSP Off-Premise. Below is an explanation of the CND requirements for each offering:

242 milCloud: A Mission Owner utilizing milCloud must align to a MCND (accredited CNDSP) to
 243 defend systems, applications, and/or data hosted in the Cloud. It does not establish a dedicated
 244 connection via the BCAP (see Figure 3) or align to a BCND, because access to the CSO is provided
 245 through the ICAP. Monitoring and protection from external attacks is accomplished at the IAP.

246 On-Premise CSO: A Mission Owner utilizing a CSP On-Premise CSO must align to a MCND
 247 (accredited CNDSP) to defend systems, applications, and and/or data hosted in the Cloud. It does not
 248 establish a dedicated connection via the BCAP (see Figure 3) or align to a BCND, because access to

249 the CSO is provided through the ICAP. Monitoring and protection from external attacks is
 250 accomplished at the IAP.

251 Off-Premise CSO: A Mission Owner utilizing a CSP Off-Premise CSO must align to a MCND
 252 (accredited CNDSP) to defend systems, applications, and and/or data hosted in the Cloud. If the
 253 Mission Owner utilizes a CSP Off-Premise CSO for Information Impact Level 4/5 (see Figure 3),
 254 they must establish a dedicated connection via a BCAP. The Mission Owner, in this case, is assigned
 255 the BCND from their connection to the BCAP. For an Information Impact Level 2 CSO, the CSP Off-
 256 Premise does not have to use a BCAP and is not associated to a BCND.



257
 258 **Figure 3 – Depiction of the Various Cloud Access Points⁸**

259 **2.D. CND Methodology**

260 The desire for a consistent CND methodology to conduct analysis may require collaboration between the
 261 BCND and MCNDs for some incidents and events. For example, Advanced Persistent Threats (APTs)
 262 could attempt to target data hosted On-Premise, or use the applications and virtual servers hosted on Off-
 263 Premise CSOs to attempt to access the DISN via the BCAP. In such instances, the BCND and MCNDs
 264 would each hold part of the Cyber SA picture that through collaboration would provide richer Cyber SA
 265 and further enable an information-driven defense.

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

267 Table 1 lists the DoD cyber incidents and events and their associated CND Use Procedures. In addition,
 268 additional events of relevance for CND (e.g. Spillage/Unauthorized Disclosure, Annual Assessment) are
 269 listed with their CND user procedures. The subparagraphs that follow in this annex will introduce each of
 270 these Use Procedures from Table 1, describing the event in a Cloud context and providing an overview of

⁸ Ref (k) from CAP Security Functional Requirements, Figure 1

271 the procedure. See Section 3 of subsequent annexes for role-specific Use Procedures as listed in Table 1.
 272 For example, the BCND response to a CAT 7 incident is defined in Annex B at Section B-3.G, “Response
 273 to Malicious Logic”.

274 **Table 1 – Cyber Event and Incident Response Matrix**

DoD Category ⁹	CND Function	Use Procedure
CAT 1 - Root Access CAT 2 - User Access	Respond	B - Response to Unauthorized Access / Intrusion
CAT 3 - Unsuccessful Activity Attempt	Respond	C - Response to Unsuccessful Activity Attempt
CAT 4 - Denial of Service (DoS)	Respond	D - Response to DoS
CAT 5 - Non-Compliance Activity	Respond	E - Response to Non-Compliance Activity
CAT 6 – Reconnaissance	Respond	F - Response to Reconnaissance
CAT 7 - Malicious Logic	Respond	G - Response to Malicious Logic
CAT 8 – Investigating	Respond	A - Initial Cloud Activity Assessment
CAT 9 - Explained Anomaly	Respond	H - Response to Explained Anomaly
CAT 0 - Training and Exercises	Respond	P – Response to Training and Exercises
Spillage/Unauthorized Disclosure	Respond	I - Response to Spillage/Unauthorized Disclosure
Vulnerability Scans (VS)	Protect	J - Performing VS
Annual Assessments	Protect	K - Performing Annual External Assessments
Configuration Management (CM)/Patching	Protect	L - Performing CM/Patching
Planned Outage	Protect	M - Performing Planned Outage
Unplanned Outage	Respond	N - Response to Unplanned Outage
Disaster Recovery	Respond	O - Performing Disaster Recovery

275
 276 CSPs that report cyber events or incidents via US-CERT or the Defense Industrial Base Network
 277 (DIBNet) should characterize the cyber event or incident IAW the US-CERT Federal Incident
 278 Notification Guidelines¹⁰. Impacted MCNDs will map the CSP-reported events and incidents to DoD
 279 categories per Table 1 when reporting the cyber events and incidents to JFHQ-DoDIN.

280 **3.A. Initial Cloud Activity Assessment**

281 The Initial Cloud Activity Assessment is invoked by procedures that are part of the initial investigation of
 282 a cyber event or incident. The purpose of this procedure is to determine the extent of a cyber event or
 283 incident, survey the impact, communicate findings to relevant CND organizations, and if needed initiate a
 284 response from the right level IAW Figure 1.

⁹ Reference (a): CJCSM 6510.01B “Cyber Incident Handling Program”

¹⁰ 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 aligns with NIST SP 800-61 Rev 2.

285 The Initial Cloud Activity Assessment is a self-standing response for DoD CAT 8 “Investigating”
286 incidents. Initial notification must be established to provide initial SA to all CND organizations (and, if
287 appropriate, US-CERT) and log the incident in the Joint Incident Management System (JIMS) in
288 accordance with the Cyber Incident Handling Program.

289 Other procedures may first invoke an investigation phase by referencing the use of the Initial Cloud
290 Activity Assessment as the first of many steps. For those procedures, the findings from the Initial Cloud
291 Activity Assessment may be used to determine correct next steps. In such cases the procedures will
292 branch based on findings.

293 If the incident or event impacts multiple Missions, BCNDs, and/or CSOs, the DoDIN CND will monitor
294 the CSP response across the Missions and report to JFHQ-DODIN for SA.

295 JFHQ-DoDIN distributes TASKORDs to DoDIN CND, BCNDs, and MCNDs. All TASKORDs will be
296 followed and executed according to the directives described in the order. The Cloud CND C3 structure
297 (Figure 2) is provided to illustrate the Incident Reporting and CND Information Sharing requirements of
298 the CND organizations and CSPs.

299 If the Initial Cloud Activity Assessment requires Situational Awareness Reports¹¹ (SARs) from the CSPs,
300 the recipient Mission Owners will post or distribute those SARs to their MCNDs. If a CSP detects a cyber
301 event or incident that potentially affects DoD information confidentiality, integrity, or accessibility,
302 information about the cyber event or incident should be made available to the Mission Owner via a SAR,
303 who will post or distribute it to their MCND. The MCNDs will share SARs to peer MCNDs, BCNDs, and
304 DoDIN CND to enable CND collaboration.

305 3.B. Response to Unauthorized Access / Intrusion

306 Three points of entry for unauthorized access / intrusion are of interest in a Cloud context.

- 307 a) Cloud-hosted mission: an intrusion into the DoD mission applications, systems or data residing
308 on the CSO
- 309 b) DISN via BCAP: an intrusion that originates from outside the DISN and enters via the BCAP,
310 possibly from a cloud-hosted mission with persistent access into the DISN via the BCAP
- 311 c) CSO: an intrusion into the underlying CSO that may threaten the cloud-hosted mission (DoD
312 mission applications, systems or data residing on the CSO)

313 Nominally the MCND will detect, investigate, and respond in the case of (a), the BCND in the case of (b),
314 and the CSP in the case of (c). However, it is possible that some incidents will require a collaboration and
315 coordination amongst the DoDIN CND, BCND, MCND, and/or CSP.

¹¹ SAR is defined in Quick Reference Guide (QRG) S11.2 *Situational Awareness Report*, and TTP 310-240-07-C1
Cyber Incident Handling

316 Unauthorized access or intrusion becomes relevant to the CSP if the cyber incident or event occurs within
317 the CSO. Examples include:

- 318 • Below-hypervisor access or intrusion to an IaaS CSO hosting DoD missions
- 319 • Mission Cloud access or intrusion to services software that formulates the PaaS
- 320 • Web server intrusion to a SaaS CSO hosting DoD missions, such as Cross-Site Scripting (XSS) and
321 SQL injections

322 In such instances the CSP shall report the incident to the Mission Owner's MCND to initiate an
323 investigation for possible DoD impact.

324 3.C. Response to Unsuccessful Activity Attempt

325 Unsuccessful activity attempts are cyber events but not cyber incidents, per the Cyber Incident Handling
326 Program. They can be reported via JIMS, although it is not required. Information about the cyber event
327 should be made available to the relevant CND groups via a SAR.

328 3.D. Response to DoS

329 The primary factor in determining the appropriate response is to identify the Recovery Time Objective
330 (RTO) of the impacted systems. The response will be different in the case of a DoS against an application
331 with a RTO of 5 days (for example) vs. an application with an RTO of 1 hour. In addition, if multiple
332 mission applications are impacted by a coordinated attack then JFHQ-DoDIN may coordinate the
333 response across the BCND and MCNDs.

334 3.E. Response to Non-Compliance Activity

335 Execute Initial Cloud Activity Assessment, Section 3.A.

336 3.F. Response to Reconnaissance

337 Identified reconnaissance are cyber events but not cyber incidents, per the Cyber Incident Handling
338 Program, and therefore do not in themselves trigger JIMS reporting. Reconnaissance can occur against the
339 BCAP, externally-hosted CSOs, or other targets. However, when it is determined by the detecting
340 organization that reconnaissance events potentially affect DoD information confidentiality, integrity, or
341 accessibility (whether by MCND, BCND, or CSP) information about the cyber events should be made
342 available to the relevant CND groups via a SAR.

343 3.G. Response to Malicious Logic

344 Malicious logic (aka malware) can reside on a cloud solution of any delivery model: IaaS, PaaS, and
345 SaaS. Malicious logic can infect OSES, network devices, applications, or data files (e.g. PDF or MS Word
346 files). In addition to traditional malware impact analysis, CND analysts shall monitor for malware that
347 specifically exploits the cloud infrastructure to impact other missions or exploits the dedicated BCAP
348 connections to impact the DISN.

349 3.H. Response to Explained Anomaly

350 An explained anomaly is a cyber event caused by non-malicious activity, such as malfunctions or false
 351 alarms¹². The proper response to an explained anomaly is to execute the Initial Cloud Activity
 352 Assessment (paragraph **Error! Reference source not found.**). However, when it is determined by the
 353 detecting organization that the Explained Anomaly events potentially affect DoD information
 354 confidentiality, integrity, or accessibility (whether by MCND, BCND, or CSP) information about the
 355 cyber events should be made available to the relevant CND groups via a SAR.

356 3.I. Response to Spillage/Unauthorized Disclosure

357 Although not defined as a cyber incident or cyber reportable event, reporting spillage/unauthorized
 358 disclosure is still necessary for the maintenance of global cyber situational awareness. Spillage¹³ is
 359 defined as “Contamination of lower level networks with material of a higher classification.” JFHQ-
 360 DoDIN should be notified of any spillage/unauthorized disclosure of CUI, personally identifiable
 361 information (PII)/protected health information (PHI), or unclassified NSS with an evaluation of impact
 362 not only to DoDIN but also to national security and/or personnel.

363 Spillage/unauthorized disclosure in the Cloud includes:

- 364 • Transfer of information at a higher Information Impact Level than the CSO is approved to (e.g.
 365 Impact Level 4 data on an Impact Level 2 CSO).
- 366 • Posting of information to an Impact Level 2 CSO that has not been approved for public or
 367 unclassified private release (e.g. ITAR, PII, etc.).

368 Mission Owner / Mission Administrator retain accountability for spillage/unauthorized disclosure
 369 remediation, whether the remediation process is executed by the Mission Owner / Mission Administrator
 370 or by the CSP. The steps taken depend on the configuration of the Mission applications and data, the
 371 SLAs in place for the CSO, and the separations of authority for the systems on which the data resides.
 372 They will be carried out via the CSP’s data spill/unauthorized disclosure cleanup methods IAW the Cloud
 373 Computing SRG¹⁴. In the case of spillage of classified data, investigation, reporting, and remediation
 374 must be performed IAW the Cloud Computing SRG and DoD Manual (DoDM) 5200.01 Vol 3¹⁵.

375 3.J. Performing VS

376 In all instances, the CSP retains responsibility for vulnerability scans for the CSO. The extent of Mission
 377 Owner VS responsibility varies with the type of service offering. In the instances of IaaS solutions, the
 378 Mission Owner retains responsibility for VS for mission systems and mission applications on the CSO. It
 379 is possible for the Mission Owner to automate VS, for example, utilizing Assured Compliance

¹² Ref (a): Cyber Incident Handling Program, Section 2: Categories

¹³ Ref (l): CJCSI 6510.01F, Enclosure C, Section 29: Spillage of Classified Information

¹⁴ 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.”

¹⁵ Ref (p): DoDM 5200.01 Vol 3 Enclosure 7 Section 5 on Classified Data Spills

380 Assessment Solution (ACAS) feeds into a central repository. For PaaS and SaaS solutions, the Mission
381 Owner retains responsibility to confirm results of continuous monitoring, which should be enforced
382 through the SLA.

383 3.K. Performing Annual External Assessments

384 Requirements for annual external assessments (e.g. Red Team, Blue Team, Penetration Testing, etc.)
385 extend to systems/applications/data hosted on CSOs. This includes IaaS, PaaS, and SaaS service delivery
386 models. While the CSPs (both commercial and DoD) are responsible for continuous monitoring and
387 regular assessment of their CSOs, Mission Owners (and their Mission Administrators) are separately
388 assessed on the proper configuration and use of those service offerings.

389 In the case of a SaaS or PaaS CSO, the Mission Owner may elect to inherit a portion of their CND
390 controls from the CSP. Such an agreement should be negotiated during CSO acquisition and reflected in
391 the SLA. In such a case, the Mission Owner shall coordinate the external assessment with the CSP.

392 3.L. Performing CM/Patching

393 If the service offering is an IaaS solution, then the Mission Owner retains responsibility for CM/patching
394 of all systems in their virtual data center (e.g. virtual servers, virtual networks, applications, etc.). For
395 PaaS and SaaS solutions, the Mission Owner retains responsibility to confirm CSP results of continuous
396 monitoring. Although the Mission Owner is responsible for performing or confirming CM/Patching, the
397 MCND and BCND must maintain awareness of CM/Patching operations. Depending on the features of
398 the CSOs it may be possible for the Mission Owner to automate CM/patching validation with, for
399 example, ACAS feeds into a central repository which would alter/simplify this procedure (e.g. Cloud-
400 hosted DoDIN utility services). The Mission Owner shall maintain up-to-date CM/Patching
401 documentation and share to MCND so that MCND can detect malicious changes to network/system
402 configurations and settings.

403 3.M. Performing Planned Outage

404 An outage can be planned by the CSP or by the Mission Owner. The CSP may plan an outage for
405 scheduled maintenance or upgrades. The CSP notifies the Mission Owner of the planned outage. As the
406 Mission Owner evaluates downtime impact to the mission, the Mission Owner is simultaneously
407 encouraged to review the SLA to monitor the performance of the CSP against SLA commitments.

408 DoD planned outages can originate from multiple organizations. The obvious case is a Mission Owner-
409 directed outage to upgrade systems. In the case of a Mission Owner, this pertains primarily to IaaS and
410 possibly to PaaS (in the instance of custom software upgrades, for example). The planned outage,
411 however, can be in response to a TASKORD or a need to perform maintenance on the BCAP. In all
412 instances the Mission Owner (or Mission Administrator) notifies the CSP and MCND of the planned
413 outage.

414 3.N. Response to Unplanned Outage

415 The response procedures assume communication from a CSP of an unplanned service outage, or the
416 discovery thereof. The response to an Unplanned Outage is similar to the response to a DoS.

- 417 3.O. Performing Disaster Recovery
- 418 Execute established disaster recovery procedures to restore Cloud-hosted functionality.
- 419 3.P. Response to Training and Exercises
- 420 Execute Initial Cloud Activity Assessment, Section 3.A.

DRAFT

424 **ANNEX B: DODIN CND**

425 **B-1. DoDIN CND Introduction**

426 The primary objective of the DoDIN CND is to monitor for DoDIN-wide attacks. DoDIN CND builds a
427 broad Cyber SA picture across Missions, MCNDs, BCNDs, CSOs, and CSPs. With this broad view, the
428 DoDIN CND can identify broader patterns of incidents or events. In the instances that incidents or events
429 span multiple BCNDs the DoDIN CND performs a coordination support function for JFHQ-DoDIN. The
430 DoDIN CND can help consolidate related incident tickets, recommend mitigations, and assist JFHQ-
431 DoDIN with assigning Cyber Protection Teams (CPTs) to focus efforts on a specific threat or adversary.
432 The C3 structure and workflows broadly aggregate MCND reporting and correlation at the DoDIN CND
433 to minimize duplication of effort, minimize miscommunication (e.g. different descriptions for “same”
434 incident spanning multiple CSOs), improve responsiveness and enable greater proactive defense across
435 the MCNDs and, by extension, the service offerings and CSPs (see Section 2.B).

436 **B-2. DoDIN CND Responsibilities**

- 437 B-2.A. Shall monitor CND incident databases (JIMS and DIBNet) for reported incidents.
 - 438 B-2.A.1. Where an incident spans multiple MCNDs or BCNDs, consolidate JIMS tickets
 - 439 B-2.A.2. Adjudicate conflicting reporting
 - 440 B-2.A.3. Recommend a lead for the activity (e.g. MCND, BCND, or CCMD, etc.) to JFHQ-
441 DoDIN
- 442 B-2.B. Shall coordinate with MCNDs and BCNDs on JFHQ-DODIN orders/tasks status.
- 443 B-2.C. Pass Indications & Warnings (I&W) to BCND.
- 444 B-2.D. Assist JFHQ-DoDIN w/ effective orders.
- 445 B-2.E. Maintain JFHQ-DoDIN and BCND POC lists.
- 446 B-2.F. Disseminate Threat Intelligence Product Reports (TIPRs) from Intel sources.
- 447 B-2.G. Provide aggregated data to JFHQ-DODIN.
 - 448 B-2.G.1. Perform delta of Vulnerability Assessments of CSO-hosted systems, networks, and data.
 - 449 B-2.G.2. Provide trending data to JFHQ-DODIN.
- 450 B-2.H. JFHQ-DoDIN recommendations on CPT activation.
- 451 B-2.I. Shall establish communication plans.
- 452 B-2.J. Shall maintain a CSP POC list.

- 453 B-2.K. Maintain JFHQ-DODIN contact list.
- 454 B-2.L. Provide POC information to JFHQ-DoDIN.
- 455 B-2.M. Provide POC information to Combatant Command/Joint Cyber Center (CCMD/JCC).
- 456 B-2.N. Shall maintain POC lists.
- 457 B-2.N.1. Maintain current contact lists for POCs at JFHQ-DoDIN, BCNDs, MCNDs, Mission
458 Owners, and CSPs for:
- 459 a) Cyber event and incident response reporting (see Figure 1 – DoD Cloud CND C2 Model),
460 including: guidance/orders and reporting
- 461 b) CND coordination (see Figure 2 - DoD Cloud CND C3 Data Sharing), including: SARs
462 distribution and CND data sharing
- 463 c) Distribution lists for: SARs, Plan of Action and Milestones (POA&Ms), external
464 assessments (plans, reports, findings), VS schedules, and outage notices
- 465 B-2.N.2. Maintain DoDIN CND POC list; distribute changes to POC list to JFHQ-DoDIN,
466 BCNDs, MCNDs, Mission Owners, and CSPs.

467 **B-3. DoDIN CND Cyber Incident and Event Procedures**

- 468 B-3.A. Initial Cloud Activity Assessment
- 469 B-3.A.1. If incidents are being reported with regard to multiple Missions and/or CSOs, perform
470 XCA to search for correlation; if possible, consolidate incident reports.
- 471 B-3.A.2. Document the incident in JIMS. If the boundary impact is unknown, the incident is
472 categorized as a CAT 8 “Investigating” incident.
- 473 B-3.A.3. DoDIN CND reports incident to JFHQ-DoDIN for DOD CAT 1, 2, 4; CAT 3’s and 7’s
474 as required per CJCSM 6510.01B¹⁶.
- 475 B-3.A.4. Share to impacted MCNDs and BCNDs via SAR.
- 476 B-3.A.5. As needed, consult and advise JFHQ-DoDIN to coordinate orders.
- 477 B-3.A.6. Share updated information to impacted MCNDs and BCNDs via SAR.
- 478 B-3.A.7. JFHQ-DoDIN may distribute TASKORD. All TASKORD distributed by JFHQ-DoDIN
479 will be executed.
- 480 B-3.A.8. Post intrusion, support JFHQ-DoDIN, MCND, and BCND return to normal operations.
481 If for example a server is compromised and the cloud/network is restored to a secure state¹⁷, the
482 BCND and/or MCND should be monitoring to ensure that responses to eliminated adversaries
483 were effective.

¹⁶ Ref (a): Cyber Incident Handling Program

¹⁷ Per CNSSI-4009, Secure State is the “condition in which no subject can access any object in an unauthorized manner.”

- 484 B-3.B. Response to Unauthorized Access / Intrusion
- 485 B-3.B.1. Execute DoDIN CND Initial Cloud Activity Assessment, Section B-3.A.
- 486 B-3.B.2. If DoDIN CND finds no incident as a result of Initial Cloud Activity Assessment:
- 487 a) Close out JIMS Cat 8/report no incident to T1.
- 488 b) Update SAR; report it to JFHQ-DoDIN; share to applicable MCNDs and BCNDs.
- 489 c) Stop this procedure at this step.
- 490 B-3.B.3. If DoDIN CND discovers Unauthorized Access/Intrusion:
- 491 a) Identify and document if access attempted misuse of DoD PKI certificates, DoD privileged
- 492 credentials, CSO or application management plane privileged credentials, or other privileges.
- 493 b) Identify and document if incident originated from DoDIN, external internet, or the Cloud.
- 494 c) Report to JFHQ-DoDIN; share to applicable MCND or BCND via SAR.
- 495 d) Transfer JIMS ticket MCND/BCND and confirm update to category (e.g. CAT 1, CAT 2,
- 496 etc.).
- 497 B-3.C. Response to Unsuccessful Activity Attempt
- 498 B-3.C.1. If the event is identified by the CSP, Mission Owner, MCND, or BCND then receive
- 499 SAR from MCND or BCND.
- 500 B-3.C.2. If the event is identified by the DoDIN CND, then develop SAR and distribute to
- 501 applicable MCNDs and BCNDs.
- 502 B-3.C.3. As needed, consult and advise JFHQ-DoDIN to coordinate orders.
- 503 B-3.D. Response to DoS
- 504 B-3.D.1. Execute Initial Cloud Activity Assessment, Section B-3.A.
- 505 B-3.D.2. Notify JFHQ-DoDIN via SAR; share to relevant MCNDs and BCNDs.
- 506 B-3.D.3. As needed, consult and advise JFHQ-DoDIN to coordinate orders.
- 507 B-3.D.4. JFHQ-DoDIN may distribute TASKORD per Initial Cloud Activity Assessment,
- 508 Section B-3.A. All TASKORD will be distributed by JFHQ-DoDIN and executed by DoDIN
- 509 CND, BCNDs and MCNDs.
- 510 B-3.E. Response to Non-Compliance Activity
- 511 B-3.E.1. Execute Initial Cloud Activity Assessment, Section B-3.A.
- 512 B-3.F. Response to Reconnaissance
- 513 B-3.F.1. If signs of unauthorized access cannot be determined/validated by evaluating sources of
- 514 reconnaissance:

- 515 a) Investigate reported event or incident for DoDIN boundary impact.
- 516 b) Develop a SAR and distribute to JFHQ-DoDIN, BCNDs, the applicable MCNDs, and
517 CSPs (within classification constraints)
- 518 B-3.F.2. If the reconnaissance event is identified by DoDIN CND:
- 519 a) Develop a SAR.
- 520 b) Distribute the SAR to JFHQ-DoDIN, BCNDs, the applicable MCNDs, and CSPs (within
521 classification constraints).
- 522 B-3.F.3. Determine source or cause of reconnaissance for signs of unauthorized access or
523 malware.
- 524 B-3.F.4. If unauthorized access is detected, refer to the relevant Use Procedure respective to
525 BCND, MCND, or Mission Owner. Section [C-3.A.7](#): Post intrusion, the BCND and MCND
526 should be cooperating to support return to normal operations. If for example a server is
527 compromised and the cloud/network is restored to a secure state, the BCND and/or MCND
528 should be monitoring to ensure that responses to eliminated adversaries were effective.
- 529 a) Response to Unauthorized Access / Intrusion.
- 530 b) If malware is detected, refer to [C-3.G](#) Response to Malicious Logic.
- 531 c) Update SAR and resend.
- 532 B-3.F.5. Determine need, if any, for preventative countermeasures at the BCAPs (via BCNDs) or
533 Internet Access Point (IAP) to defend the DoDIN.
- 534 **B-3.G. Response to Malicious Logic**
- 535 B-3.G.1. Malware may be identified in the course of ongoing monitoring or in response to a
536 MCND notice. If DoDIN CND identifies the malware, DoDIN CND notifies applicable MCND
537 or BCND. Applicable MCND or BCND will open a CAT 7 JIMS ticket.
- 538 B-3.G.2. DoDIN CND investigates across all Missions for similar reports to ascertain scope of
539 impact. If impact is seen across multiple Missions, then the DoDIN CND:
- 540 a) Is responsible for CAT 7 incident response.
- 541 b) Consolidates all related CAT 7 tickets to a DoDIN CND-owned ticket
- 542 c) Coordinates guidance/action with JFHQ-DoDIN; evaluate recommending
543 USCYBERCOM CPT activation.
- 544 B-3.G.3. JFHQ-DoDIN may distribute TASKORD to DoDIN CND, BCND, and MCNDs. All
545 TASKORD will be distributed by JFHQ-DoDIN and executed by DoDIN CND, BCND, and
546 MCNDs.
- 547 B-3.G.4. Close JIMS Tickets that are assigned to the DoDIN CND.
- 548 **B-3.H. Response to Explained Anomaly**
- 549 B-3.H.1. Execute Initial Cloud Activity Assessment, Section B-3.A.
- 550 B-3.H.2. If possible, implement process, signature, or tool update to reduce occurrence of
551 Explained Anomaly.

- 552 B-3.I. Response to Spillage/Unauthorized Disclosure
- 553 B-3.I.1. If the DoDIN CND identifies the spillage/unauthorized disclosure, DoDIN CND notifies
554 MCND and BCND (if applicable) of impacted Mission Owner
- 555 B-3.I.2. Support MCND/BCND investigation and track the spillage/unauthorized disclosure JIMS
556 ticket** to closure. (**Until creation of Spillage/Unauthorized Disclosure category, submit via
557 SAR to JFHQ-DoDIN).
- 558 B-3.J. Performing VS
- 559 B-3.J.1. Receive VS POA&M from MCND (see Section D-3.J.5).
- 560 B-3.J.2. Compare POA&M vulnerabilities to Intel reports.
- 561 B-3.J.3. Evaluate results for the Hosting CSP.
- 562 B-3.J.4. Develop scorecard and deliver to JFHQ-DoDIN for entire CSP mission space with
563 recommendations on mitigations, if applicable.
- 564 B-3.K. Performing Annual External Assessments.
- 565 B-3.K.1. DoDIN CND receives notification of external assessment type and period from MCND
566 (see Section D-3.K.1).
- 567 B-3.K.2. If MCND performs the assessment, then receive a full report of findings and
568 recommendations from the MCND after the assessment is complete (see Section D-3.K.4).
- 569 B-3.K.3. If JFHQ-DoDIN requests support to plan and perform the external assessment, support
570 JFHQ-DoDIN.
- 571 B-3.L. Performing CM/Patching
- 572 B-3.L.1. Receive notice from MCND of patch schedule/outage.
- 573 B-3.L.2. Receive notice of restoration of service and success of patch deployment from MCND.
- 574 B-3.L.3. Receive updated CM/Patching documentation via MCND.
- 575 B-3.M. Performing Planned Outage
- 576 B-3.M.1. Receive notice from MCND of outage schedule (see Section D-3.M.1.a).
- 577 B-3.M.2. If schedule anomalies are reported by MCND, perform XCA to assess if there is a
578 pattern of anomalies across the CSO or CSP. If so, notify JFHQ-DoDIN of the updates or
579 anomalies.
- 580 B-3.M.3. Receive notice from MCND after restoration of service.
- 581 B-3.N. Response to Unplanned Outage
- 582 B-3.N.1. Receive notice from MCND of outage and impact.
- 583 B-3.N.2. Confirm awareness at JFHQ-DoDIN of outage and impact.
- 584 B-3.N.3. Perform XCA to assess if outage and impact spans Missions, CSOs, and/or CSPs.
- 585 B-3.N.4. If outage impact spans multiple Missions, CSOs, and/or CPS, report aggregate impacts
586 of impacted missions to JFHQ-DoDIN.
- 587 B-3.N.5. Track outages to closure.

- 588 B-3.O. Performing Disaster Recovery
- 589 B-3.O.1. Maintain SA of the MCND and Mission Owner efforts to execute disaster recovery
- 590 procedures to restore Cloud-hosted functionality.

- 591 B-3.P. Response to Training and Exercises
- 592 B-3.P.1. Execute DoDIN CND Initial Cloud Activity Assessment, Section B-3.A.

DRAFT

593
594
595RME, DEFENSE INFORMATION SYSTEMS AGENCY
CHAMBERSBURG, PENNSYLVANIA 17201
21 Sep 2015596 **ANNEX C: BCND**597 **C-1. BCND Introduction**

598 The primary objective of the BCND is to protect the DISN from attacks utilizing Public, Community,
599 Private, and Hybrid clouds, through approved CSPs, that can impact the DISN through a dedicated
600 connection via a BCAP. The BCND furthermore supports the MCNDs in their objectives of defending
601 their systems, applications, and data hosted in the Cloud. In that capacity, the BCND builds a broad Cyber
602 SA picture across Missions, CSOs, and CSPs and can identify broader patterns of incidents or events. In
603 the instances that incidents or events span multiple Missions, CSOs, or CSPs the BCND performs a CND
604 coordination support function for JFHQ-DoDIN. The BCND can help consolidate related incident tickets,
605 recommend mitigations, and confirm technical aspect of TASKORD compliance by MCNDs that is
606 verifiable from the Boundary. Lastly, the BCND supports the DoDIN CND by providing reports and
607 information for incidents and events for further aggregation to ensure that the incidents are not DoDIN-
608 wide or are isolated to a particular BCAP. Each BCAP will align to an accredited CNDSP to perform as
609 the BCND for that BCAP.

610 **C-2. BCND Responsibilities**

611 C-2.A.1. B-2.A. Assist in Connecting MCND Systems Shall maintain a CNDSP accreditation.

612 C-2.A.2. Shall be the performing CNDSP for the BCAP

613 C-2.A.3. Shall assist with enabling CND at the BCAP, to include:

614 a) Installing and maintaining CND sensors

615 b) Connecting MCND systems, such as a Security Information and Event Management
616 (SIEM) solution, to logs from Mission Owner and/or CSO systems

617 c) Monitoring sensor and log feeds

618 C-2.A.4. Shall protect the DoDIN at the boundary BCAP.

619 C-2.A.5. Shall monitor data in transit through the BCAP based on BCAP sensing capabilities¹⁸.

620 C-2.A.6. Shall monitor for unauthorized connections (attempted and actual).

621 **C-2.B. Shall coordinate with MCNDs on JFHQ-DoDIN orders/tasks status**

622 C-2.B.1. Pass I&W to MCND, other BCNDs, and DoDIN CND.

623 C-2.B.2. Maintain JFHQ-DoDIN, DoDIN CND, and MCND POC lists.

¹⁸ Ref (k) *Cloud Access Point Functional Requirements Document (CAP FRD)* defines the sensing capabilities at the CAP

- 624 C-2.B.3. Disseminate TIPRs from Intel sources.
- 625 C-2.B.4. Provide aggregated data to DoDIN CND.
- 626 C-2.B.5. Provide BCAP trending data to DoDIN CND.
- 627 C-2.B.6. CCMD/JCC SA coordination.
- 628 C-2.C. Shall establish communication plans.
- 629 C-2.D. Shall maintain POC lists
- 630 C-2.D.1. Maintain current contact lists for POCs at JFHQ-DoDIN, DoDIN CND, BCND,
631 MCND, Mission Owner, and CSPs for:
- 632 a) Cyber event and incident response reporting (see Figure 1 – DoD Cloud CND C2 Model),
633 including: guidance/orders and reporting
- 634 b) CND coordination (see Figure 2 - DoD Cloud CND C3 Data Sharing), including: SARs
635 distribution and CND data sharing
- 636 c) Distribution lists for: SARs, POA&Ms, external assessments (plans, reports, findings), VS
637 schedules, and outage notices
- 638 C-2.D.2. Maintain BCND POC list; distribute changes to POC list to JFHQ-DoDIN, DoDIN
639 CND, peer BCNDs, relevant MCNDs, relevant Mission Owners, and relevant CSPs

640 **C-3. BCND Cyber Incident and Event Procedures**

- 641 C-3.A. Initial Cloud Activity Assessment
- 642 C-3.A.1. If incidents are being reported with regard to multiple Missions and/or CSOs, BCND
643 notifies DoDIN CND for XCA.
- 644 C-3.A.2. BCND documents the incident in JIMS. If the boundary impact is unknown, the incident
645 is categorized as a CAT 8 “Investigating” incident.
- 646 C-3.A.3. BCND reports incident to DoDIN CND and JFHQ-DoDIN for DOD CAT 1, 2, 4; CAT
647 3’s and 7’s as required per CJCSM 6510.01B¹⁹.
- 648 C-3.A.4. As needed, the BCND consults and advises DoDIN CND and/or JFHQ-DoDIN to
649 coordinate orders.
- 650 C-3.A.5. BCND notifies impacted MCNDs via SAR.
- 651 C-3.A.6. JFHQ-DoDIN may distribute TASKORD. All TASKORD distributed by JFHQ-DoDIN
652 will be executed.
- 653 C-3.A.7. Post intrusion, the BCND and MCND should be cooperating to support return to normal
654 operations. If for example a server is compromised and the cloud/network is restored to a secure

¹⁹ Ref (a): Cyber Incident Handling Program

655 state²⁰, the BCND and/or MCND should be monitoring to ensure that responses to eliminated
656 adversaries were effective.

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

658 C-3.B.1. Execute BCND Initial Cloud Activity Assessment, Section 26C-3.A.

659 C-3.B.2. If BCND finds no incident as a result of Initial Cloud Activity Assessment:

660 a) Close out JIMS Cat 8/report no incident to T1.

661 b) Update SAR and send it to MCND

662 c) Stop this procedure at this step.

663 C-3.B.3. If BCND discovers Unauthorized Access/Intrusion:

664 a) Identify and document if access attempted misuse of DoD PKI certificates, DoD privileged
665 credentials, CSO or application management plane privileged credentials, or other privileges.

666 b) Identify and document if incident originated from DoDIN, external internet, or the Cloud.

667 c) Notify MCND via SAR

668 d) Transfer JIMS ticket MCND and confirm update to category (e.g. CAT 1, CAT 2, etc.).

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

670 C-3.C.1. If the event is identified by the CSP, Mission Owner, MCND then the BCND will
671 receive SAR from MCND.

672 C-3.C.2. If the event is identified by the BCND, then develop the SAR and distribute to
673 applicable MCNDs.

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

675 C-3.D. Response to DoS

676 C-3.D.1. Execute Initial Cloud Activity Assessment, Section 26C-3.A.

677 C-3.D.2. If DoS attack impacts DoDIN via BCAP, document the incident in JIMS.

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

679 C-3.D.4. Notify impacted MCNDs, JFHQ-DoDIN via SAR.

680 C-3.D.5. JFHQ-DoDIN may distribute TASKORD to BCND and MCNDs per Initial Cloud
681 Activity Assessment. All TASKORD will be distributed by JFHQ-DoDIN and executed by
682 BCND and MCNDs.

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

684 C-3.E.1. Execute Initial Cloud Activity Assessment.

²⁰ Per CNSSI-4009, Secure State is the "condition in which no subject can access any object in an unauthorized manner."

UNCLASSIFIED

- 685 C-3.E.2. Notify relevant MCNDs of non-compliance activity.
- 686 C-3.E.3. If impact to Mission, notify MCND via SAR. If appropriate, document in JIMS ticket;
- 687 track to resolution.
- 688 C-3.F. Response to Reconnaissance
- 689 C-3.F.1. If signs of unauthorized access cannot be determined/validated by evaluating sources of
- 690 reconnaissance:
- 691 a) Investigate reported event or incident for DoDIN boundary impact.
- 692 b) Develop a SAR and distribute to JFHQ-DoDIN, DoDIN CND, the applicable MCNDs, and
- 693 CSPs (within classification constraints).
- 694 C-3.F.2. If the reconnaissance event is identified by the BCND:
- 695 a) The BCND develops a SAR.
- 696 b) The BCND distributes the SAR to JFHQ-DoDIN, DoDIN CND, the applicable MCNDs,
- 697 and CSPs (within classification constraints).
- 698 C-3.F.3. Determine source or cause of reconnaissance for signs of unauthorized access or
- 699 malware.
- 700 C-3.F.4. If unauthorized access is detected, refer to the relevant Use Procedure respective to
- 701 BCND, MCND, or Mission Owner. Section C-3.A.7: Post intrusion, the BCND and MCND
- 702 should be cooperating to support return to normal operations. If for example a server is
- 703 compromised and the cloud/network is restored to a secure state, the BCND and/or MCND
- 704 should be monitoring to ensure that responses to eliminated adversaries were effective.
- 705 a) Response to Unauthorized Access / Intrusion.
- 706 b) If malware is detected, refer to Section C-3.G: Response to Malicious Logic.
- 707 c) Update SAR and resend.
- 708 C-3.F.5. Determine need, if any, for preventative countermeasures at the BCAP.
- 709 C-3.G. Response to Malicious Logic
- 710 C-3.G.1. Malware may be identified in the course of ongoing monitoring or in response to a
- 711 MCND notice. If BCND identifies the malware, BCND notifies applicable MCND. MCND will
- 712 open a CAT 7 JIMS ticket.
- 713 C-3.G.2. BCND requests impact assessments across all Missions to ascertain scope of impact. If
- 714 impact is seen across multiple Missions, then the BCND:
- 715 a) Is responsible for CAT 7 incident response.
- 716 b) Consolidates all related CAT 7 tickets to a BCND-owned ticket
- 717 c) Coordinates guidance/action with JFHQ-DoDIN; evaluate recommending
- 718 USCYBERCOM CPT activation.
- 719 C-3.G.3. JFHQ-DoDIN may distribute TASKORD to BCND and MCNDs. All TASKORD will
- 720 be distributed by JFHQ-DoDIN and executed by BCND and MCNDs.
- 721 C-3.G.4. Close JIMS Tickets that are assigned to the BCND.

UNCLASSIFIED

UNCLASSIFIED

- 722 C-3.H. Response to Explained Anomaly
- 723 C-3.H.1. Execute Initial Cloud Activity Assessment, Section 26C-3.A.
- 724 C-3.H.2. If possible, implement process or tool update to reduce occurrence of Explained
- 725 Anomaly.
- 726 C-3.I. Response to Spillage/Unauthorized Disclosure
- 727 C-3.I.1. If the BCND identifies the spillage/unauthorized disclosure, BCND notifies MCND of
- 728 impacted Mission Owner
- 729 C-3.I.2. BCND supports MCND investigation and tracks the MCND's Spillage/Unauthorized
- 730 Disclosure JIMS ticket** to closure. (**Until creation of Spillage/Unauthorized Disclosure
- 731 category, submit via SAR to JFHQ-DoDIN).
- 732 C-3.J. Performing VS
- 733 C-3.J.1. Receive VS schedule from MCND.
- 734 C-3.J.2. Support Mission Owner during VS (e.g. modify alert or response posture during VS
- 735 period).
- 736 C-3.K. Performing Annual External Assessments.
- 737 C-3.K.1. BCND receives notification of external assessment type and period from MCND.
- 738 C-3.K.2. If MCND performs the assessment, then BCND receives a full report of findings and
- 739 recommendations from the MCND after the assessment is complete.
- 740 C-3.K.3. If MCND cannot perform requested assessment, then:
- 741 a) Coordinate required assessment with JFHQ-DoDIN (could be activation of a
- 742 USCYBERCOM CPT).
- 743 b) Follow Reporting Requirements per defined Deconfliction Process with JFHQ-DoDIN.
- 744 c) Provide a full report of findings and recommendations to the requesting Mission Owner,
- 745 Mission Administrator, and MCND.
- 746 C-3.K.4. Notify JFHQ-DoDIN that assessment is complete.
- 747 C-3.K.5. Notify JFHQ-DoDIN and all MCNDs that the Lessons Learned are posted.
- 748 C-3.K.6. Deconfliction issues will be addressed between JFHQ-DoDIN and US-CERT
- 749 C-3.L. Performing CM/Patching
- 750 C-3.L.1. Receive notice from MCND of patch schedule/outage.
- 751 C-3.L.2. Receive notice of restoration of service and success of patch deployment from MCND.
- 752 C-3.L.3. Receive updated CM/Patching documentation via MCND.
- 753 C-3.M. Performing Planned Outage
- 754 C-3.M.1. Receive notice from MCND of outage schedule.
- 755 C-3.M.2. Receive notice from MCND after restoration of service.
- 756 C-3.N. Response to Unplanned Outage

UNCLASSIFIED

757 C-3.N.1. Receive notice from MCND of outage and impact.

758 C-3.N.2. Track outages to closure.

759 C-3.O. Performing Disaster Recovery

760 C-3.O.1. Maintain SA of the MCND and Mission Owner efforts to execute disaster recovery
761 procedures to restore Cloud-hosted functionality for On-Premise CSOs and milCloud.

762 C-3.O.2. Assist MCND and Mission Owner in executing disaster recovery procedures to restore
763 Cloud-hosted functionality for Off-Premise CSOs via BCAP.

764 C-3.P. Response to Training and Exercises

765 C-3.P.1. Execute BCND Initial Cloud Activity Assessment, Section 26C-3.A.

766

DRAFT

767
768
769

RME, DEFENSE INFORMATION SYSTEMS AGENCY
CHAMBERSBURG, PENNSYLVANIA 17201
21 Sep 2015

770 **ANNEX D: MCND**

771 **D-1. MCND Introduction**

772 The primary objective of the MCND is to defend systems, applications, and and/or data hosted in the
773 Cloud. The MCND defends all connections to the Mission Owner's resources on the CSO, whether via
774 BCAP, VPN, direct internet access to public servers, or other. The MCND monitors activities committed
775 with privileged connections (e.g. Cloud management or Mission application administration) and monitors
776 for attacks against the Mission applications (e.g. SQL injection). The MCND supports BCND efforts to
777 identify correlations between related incidents or events impacting multiple Missions, CSOs, or CSPs.
778 Mission Owners will align with an accredited CNDSP to perform as MCND for Cloud-hosted systems.

779 **D-2. MCND Responsibilities**

780 D-2.A. CNDSP

781 D-2.A.1. Shall maintain a CNDSP accreditation.

782 D-2.A.2. Shall be the performing CNDSP for the Mission Owner

783 D-2.A.3. Shall assist Mission Owners with enabling CND, to include:

784 a) Installing and maintaining CND sensors

785 b) Connecting MCND systems (e.g. SIEM) to logs from Mission Owner and/or CSO systems

786 c) Monitoring sensor and log feeds

787 d) Monitor for CSP communications via DIBNet (for commercial CSPs)

788 D-2.B. Perform analysis for CSO incidents/events.

789 D-2.B.1. Shall detect CSO events, analyze CSP incidents.

790 D-2.B.2. Shall map events reported by CSPs via US-CERT guidelines or DIBNet to DoD cyber
791 event and incident categories (see Table 1)

792 D-2.C. Distribute SAR to JFHQ-DoDIN, DoDIN CND, and BCNDs for Attack Sensing & Warning
793 (AS&W)/SAR.

794 D-2.D. Distribute guidance/orders (patch management)to Mission Owners

795 D-2.E. Report cyber events and incidents via JIMS.

796 D-2.F. Perform delta of Vulnerability Assessments of CSO-hosted systems, networks, and data.

797 D-2.G. Shall assist Mission Owners with enabling CND.

798 D-2.H. Shall Retain copy of SLA from Mission Owners; ensure they have proper DoD-approved
799 cloud SLA.

800 D-2.H.1. Provide placement locations for sensors (if appropriate).

801 D-2.H.2. Assist with CND installation/feeds to MCND.

802 D-2.H.3. Perform/assist with external assessments.

803 D-2.H.4. Setup Host Based Security System (HBSS), ACAS, Continuous Monitoring and Risk
804 Scoring (CMRS), and any other security capabilities as applicable.

805 D-2.I. Shall establish executive communication plans.

806 D-2.J. Shall maintain POC lists

807 D-2.J.1. Maintain current contact lists for POCs at JFHQ-DoDIN, DoDIN CND, BCND, Mission
808 Owner, and CSPs for:

809 a) Cyber event and incident response reporting (see Figure 1 – DoD Cloud CND C2 Model),
810 including: guidance/orders and reporting

811 b) CND coordination (see Figure 2 - DoD Cloud CND C3 Data Sharing), including: SARs
812 distribution and CND data sharing

813 c) Distribution lists for: SARs, POA&Ms, external assessments (plans, reports, findings), VS
814 schedules, and outage notices

815 D-2.J.2. Maintain MCND POC list; distribute changes to POC list to JFHQ-DoDIN, DoDIN
816 CND, relevant BCNDs, peer MCNDs, relevant Mission Owners, and relevant CSPs

817 **D-3. MCND Cyber Incident and Event Procedures**

818 D-3.A. Initial Cloud Activity Assessment

819 D-3.A.1. MCND documents the incident in JIMS. If the Mission impact is unknown, the incident
820 is categorized as a CAT 8 “Investigating” incident.

821 D-3.A.2. MCND notifies BCND.

822 D-3.A.3. If JFHQ-DoDIN distributes TASKORD to MCNDs, they will be executed by BCND
823 and MCNDs.

824 D-3.B. Response to Unauthorized Access / Intrusion

825 D-3.B.1. Execute MCND Initial Cloud Activity Assessment, Section D-3.A.

826 D-3.B.2. If MCND finds no incident as a result of Initial Cloud Activity Assessment:

827 a) Close out JIMS Cat 8/report no incident to JFHQ-DoDIN via SAR; share to DoDIN CND,
828 and BCNDs.

829 b) Send update to Mission Administrator / Mission Owner.

830 c) Stop this procedure at this step.

831 D-3.B.3. If MCND finds DoD impact as a result of Initial Cloud Activity Assessment:

- 832 a) Update JIMS ticket to proper category (e.g. CAT 1; CAT 2).
833 b) Note if access attempted misuse of DoD PKI certificates, DoD privileged credentials, CSO
834 or application management plane privileged credentials, or other privileges.
835 c) Note if incident originated from DoDIN, external internet, or the Cloud.
836 d) Notify JFHQ-DoDIN via SAR; share to DoDIN CND and BCNDs.
837 e) Notify Mission Owner and Mission Administrator via SAR. If appropriate, notify CSP.

838 D-3.B.4. If JFHQ-DoDIN distributes TASKORD, they are executed by MCNDs.

839 D-3.B.5. MCND sends update to Mission Owner and Mission Administrator via SAR. If
840 appropriate, notify CSP.

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

842 D-3.C.1. A SAR will be provided to the MCND if the event is identified by the BCND or CSP.
843 The MCND will distribute the respective SAR to the Mission Owners. If the CSO is a PaaS or
844 SaaS offering, the notice may come from the Mission Administrators. If so, MCND requests logs
845 from Mission Administrators (who may, depending on SLAs, acquire them from the CSP).

846 D-3.C.2. If the event is identified by the Mission team (e.g. Mission Owner, Mission
847 Administrator, or MCND) then the MCND distributes a SAR and directs changes by Mission
848 Owners or requests changes by BCND or CSP.

849 D-3.C.3. MCND will determine need, if any, for preventative countermeasures on the mission
850 data, service offering, or connection configuration to the CSP, and direct changes by the Mission
851 Administrators or request changes by the BCND or CSP.

852 D-3.D. Response to DoS

853 D-3.D.1. Execute Initial Cloud Activity Assessment, Section D-3.A.

854 D-3.D.2. If DoS attack impacts Mission, document the incident in JIMS.

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

857 D-3.D.4. Notify BCND via SAR.

858 D-3.D.5. JFHQ-DoDIN may distribute orders to MCND per Initial Cloud Activity Assessment,
859 Section D-3.A. All TASKORD will be distributed by JFHQ-DoDIN and executed by BCND and
860 MCNDs. The MCND reports status to BCND who in turn reports status to JFHQ-DoDIN.

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

862 D-3.E.1. Execute Initial Cloud Activity Assessment, Section D-3.A.

863 D-3.E.2. Notify Mission Owners and Mission Administrators of non-compliance activity; share to
864 DoDIN CND, relevant BCND,

865 D-3.E.3. If impact to Boundary, notify BCND via SAR. If appropriate, document in JIMS ticket;
866 track to resolution.

867 D-3.F. Response to Reconnaissance

868 D-3.F.1. If the MCND is notified of a Reconnaissance event or incident by CSP, BCND, or other:

- 869 a) Investigate reported event or incident for Mission impact.
- 870 b) Develop a SAR and distribute to JFHQ-DoDIN, Mission Owner, Mission Administrator,
871 DoDIN CND, BCND, and CSP.
- 872 D-3.F.2. If the reconnaissance event is identified by the Mission team (Mission Owner, Mission
873 Administrator, or MCND):
- 874 a) The MCND develops a SAR.
- 875 b) The MCND distributes SAR to JFHQ-DoDIN, Mission Administrator, Mission Owner,
876 DoDIN CND, BCND, and CSP.
- 877 D-3.F.3. Determine source or cause of reconnaissance for signs of unauthorized access or
878 malware.
- 879 a) If unauthorized access or malware is discovered, refer to those procedures.
- 880 b) Update SAR and resend.
- 881 D-3.F.4. MCND will determine need, if any, for preventative countermeasures on the Mission
882 systems, applications, CSO, or connection configuration to the CSP, and direct changes by the
883 Mission Administrators or request changes by the BCND or CSP.
- 884 D-3.G. Response to Malicious Logic
- 885 D-3.G.1. Malware may be identified in the course of ongoing monitoring or in response to a
886 BCND TIPR.
- 887 a) If malware is detected by MCND, open JIMS ticket (CAT 7), notifies CSP for awareness.
- 888 b) If MCND is notified of a malware impact assessment (e.g. by BCND or triggered by
889 identified malware on another Mission), MCND investigates and reports to JFHQ-DoDIN,
890 copies DoDIN CND, BCND, and CSP.
- 891 c) Open JIMS ticket (CAT 7).
- 892 D-3.G.2. If DoDIN CND determines multi-Mission impact (see Section [Error! Reference
893 source not found.](#)) then MCND supports consolidating tickets at DoDIN CND.
- 894 D-3.G.3. JFHQ-DoDIN may distribute TASKORD to MCND. All TASKORD will be distributed
895 by JFHQ-DoDIN and executed by BCND and MCND.
- 896 D-3.G.4. If MCND still owns the JIMS ticket, close the ticket.
- 897 D-3.H. Response to Explained Anomaly
- 898 D-3.H.1. Execute Initial Cloud Activity Assessment, Section D-3.A.
- 899 D-3.H.2. If possible, implement process or tool update to reduce occurrence of Explained
900 Anomaly.
- 901 D-3.I. Response to Spillage/Unauthorized Disclosure
- 902 After MCND identifies or receives notice of a spillage/unauthorized disclosure:
- 903 D-3.I.1. Open spillage/unauthorized disclosure JIMS ticket (**until creation of
904 Spillage/Unauthorized Disclosure category, submit via SAR to BCND and JFHQ-DoDIN).

UNCLASSIFIED

- 905 D-3.I.2. Support Mission Owner and CSP in the spillage/unauthorized disclosure investigation
906 and remediation.
- 907 D-3.I.3. Periodically update JFHQ-DoDIN, DoDIN CND, and relevant BCND for SA
- 908 D-3.I.4. When Mission Owner reports completion, MCND notifies JFHQ-DoDIN, DoDIN CND,
909 and relevant BCND of completion (via closing JIMS ticket or delivering updated SAR, IAW
910 method used to send initial notice).
- 911 D-3.J. Performing VS
- 912 D-3.J.1. MCND receives notice of VS schedule from Mission Owner.
- 913 D-3.J.2. MCND shares VS schedule to JFHQ-DoDIN, DoDIN CND, and BCND.
- 914 D-3.J.3. MCND receives results and POA&M from Mission Owner after performance of VS.
- 915 D-3.J.4. Confirm reporting of compliance with USCYBERCOM per Cyber Task Order (CTO).
- 916 D-3.J.5. Report POA&M to JFHQ-DoDIN; share to DoDIN CND and BCND.
- 917 D-3.K. Performing Annual External Assessments
- 918 D-3.K.1. Mission owner coordinates request type (e.g. Red Team, Blue Team, Penetration
919 Testing, etc.) with the MCND.
- 920 a) Evaluate capabilities required to perform requested external assessment and compare
921 against current MCND Capability and capacity.
- 922 b) MCND shares plan to BCND and DoDIN CND of type and period of assessment.
- 923 c) Confirm notification to CSP via Mission Owner / Mission Administrator.
- 924 D-3.K.2. If MCND can perform requested assessment, follow Reporting Requirements per
925 defined Deconfliction Process with JFHQ-DoDIN.
- 926 D-3.K.3. If MCND cannot perform requested assessment, then send request to JFHQ-DoDIN.
- 927 D-3.K.4. If MCND performs the assessment, provide a full report of findings and
928 recommendations to the requesting Mission Owner, Mission Administrator and JFHQ-DoDIN;
929 share to DoDIN CND and BCND.
- 930 D-3.K.5. Receive remediation plan and POA&Ms from Mission Owner (see Section E-3.K.3).
- 931 D-3.L. Performing CM/Patching
- 932 D-3.L.1. Receive notice from Mission Owner of patch schedule/outage.
- 933 D-3.L.2. Notify JFHQ-DoDIN of patch schedule/outage; share to DoDIN CND and applicable
934 BCND.
- 935 D-3.L.3. After CM/Patching is complete, Mission Owner reports restoration of service and
936 success of patch deployment to MCND and JFHQ-DoDIN per CTO/Information Assurance
937 Vulnerability Management (IAVM) Process.
- 938 D-3.L.4. MCND notifies DoDIN CND and BCND of restoration of service.
- 939 D-3.M. Performing Planned Outage
- 940 D-3.M.1. MCND receives notice from Mission Owner of outage schedule.

UNCLASSIFIED

941 a) Notify JFHQ-DoDIN of outage schedule; share to DoDIN CND and applicable BCND.

942 D-3.M.2. Notify BCND of schedule updates or anomalies during execution.

943 D-3.M.3. MCND receives notice from Mission Owner after restoration of service.

944 a) Notify JFHQ-DoDIN of service restoration; share to DoDIN CND and BCND.

945 b) Provide updated CM/Patching documentation to BCND.

946 D-3.N. Response to Unplanned Outage

947 D-3.N.1. Coordinate with Mission Owner / Mission Administrator to assess impact.

948 D-3.N.2. Report outage and impact to JFHQ-DoDIN; share outage and impact information to
949 DoDIN CND and relevant BCND.

950 D-3.N.3. Track status with Mission Owner and CSP until closure/resolution.

951 D-3.N.4. Provide periodic updates to JFHQ-DoDIN until closure/resolution; share to DoDIN
952 CND and relevant BCND.

953 D-3.O. Performing Disaster Recovery

954 D-3.O.1. Assist Mission Owner upon request in executing disaster recovery procedures to restore
955 Cloud-hosted functionality.

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

957 D-3.P.1. Execute MCND Initial Cloud Activity Assessment, Section D-3.A.

958
959
960RME, DEFENSE INFORMATION SYSTEMS AGENCY
CHAMBERSBURG, PENNSYLVANIA 17201
21 Sep 2015961 **ANNEX E: MISSION OWNER**962 **E-1. Mission Owner Introduction**

963 The Mission Owner operates, and maintains the mission systems, applications, and/or data (depending on
964 CSO service model, e.g. IaaS, PaaS, or SaaS). In that capacity, the Mission Owner is a DoD entity that
965 acquires cloud services and dedicated connections in support of its mission. Per the DoD Cloud
966 Computing SRG, the Mission Owner aligns to an accredited CNDSP for MCND and serves as the CND
967 Tier 3 for the mission systems, applications, and/or data.

968 The Cloud Computing SRG defines as separate roles the Mission Administrators and the Mission
969 Owners. Per the Cloud Computing SRG, Mission Owners are individuals/organizations responsible for
970 the overall mission environment, ensuring that the functional requirements of the system are being met.
971 Mission Owners are minimally responsible for:

- 972 • Engaging and funding the services of a MCND to provide for the defense of the Mission Owner's
973 systems, applications, and virtual networks in any CSP's IaaS/PaaS infrastructure (whether DoD
974 operated or operated by a commercial/non-DoD entity).
- 975 • Negotiating the terms and requirements with the CSP for incident reporting and incident
976 response, in coordination with the BCND and their MCND provider.
- 977 • Coordinating access for MCND and BCND for all actions required.

978 Mission Administrators are the administrators of Mission Owner's cloud-based systems, applications, and
979 virtual networks. They are Tier 3 entities consuming CNDSP services, minimally responsible for:

- 980 • Following JFHQ-DoDIN and MCND directions
- 981 • For IaaS, maintaining and patching the cloud-based mission systems, applications, and virtual
982 networks
- 983 • For PaaS, maintaining and patching cloud-based mission applications
- 984 • Installing and maintaining protective measures for the cloud-based mission systems, applications,
985 and virtual networks

986 **E-2. Mission Owner Responsibilities**

987 The Mission Owner designates a Mission Administrator, a person or group with technical responsibility
988 for the configuration of the CSO, commensurate with the cloud service model being used. The Mission
989 Owner aligns with an accredited CNDSP for MCND and integrates into the CNDSP provider architecture.

990 To enable the designated MCND, Mission Owners:

- 991 E-2.A. Shall Provide to MCND
- 992 E-2.A.1. Architecture drawings.
- 993 a) Physical and logical.
- 994 b) System descriptions (IP address, system name, description, OS versions, list of expected
- 995 protocols, configurations, etc.).
- 996 E-2.A.2. Mission Owner (and Mission Administrator) POC information to be used by MCND to
- 997 request information or issue CND directives
- 998 E-2.A.3. Copies of SLA to MCND.
- 999 E-2.B. Shall Establish the Secure Logical Connection
- 1000 E-2.B.1. For a dedicated virtual circuit (IPSec tunnel) to the CSO, request connection through a
- 1001 BCAP. For example, DISA BCAP request process is defined in the DISA Cloud Connection
- 1002 Process Guide (CCPG).
- 1003 E-2.B.2. Provide CSP list of authorized connections.
- 1004 E-2.B.3. Through CSP, confirm unauthorized attempts to connect to CSO are refused.
- 1005 E-2.C. Shall maintain a POC list.
- 1006 E-2.C.1. Maintain current contact lists for POCs at MCND, BCND, DoDIN CND, and CSP for:
- 1007 a) Cyber event and incident response reporting (see Figure 1 – DoD Cloud CND C2 Model),
- 1008 including: guidance/orders and reporting
- 1009 b) CND coordination (see Figure 2 - DoD Cloud CND C3 Data Sharing), including: SARs
- 1010 distribution and CND data sharing
- 1011 c) Distribution lists for: SARs, POA&Ms, external assessments (plans, reports, findings), VS
- 1012 schedules, and outage notices
- 1013 E-2.C.2. Maintain Mission Owner POC list; distribute changes to POC list to MCND, BCND,
- 1014 DoDIN CND, and CSP.
- 1015 E-2.D. Shall Establish Communication Plans
- 1016 E-2.D.1. Add MCND (and BCND for Off-Premise CSOs) to Trusted Disclosure list in SLA.
- 1017 E-2.D.2. Notify MCND and CSP of maintenance windows.
- 1018 E-2.D.3. Notify MCND and CSP of Periods of Non-Disruption (PONDs)
- 1019 E-2.D.4. In the case of a CSO outage (planned or unplanned), the Mission Owner shall report the
- 1020 outage or plan for outage to the MCND.
- 1021 E-2.D.5. The CSP shall maintain a current CSP Technical POC list which the Mission Owner
- 1022 shall provide to the relevant MCNDs, BCNDs, and DoDIN CNDs.
- 1023 E-2.D.6. Maintain current contact lists for MCND, BCND, and DoDIN CND.
- 1024 E-2.D.7. Establish plan for providing updates to open vulnerability POA&M to MCND.
- 1025 E-2.D.8. Incorporate SAR communication requirements into SLA.

- 1026 E-2.E. Shall Prepare Mission Data for CND
- 1027 E-2.E.1. Ensure coordination of scan results with CSP is incorporated into SLA
- 1028 E-2.E.2. Ensure proper O&M for App.
- 1029 E-2.E.3. Ensure compliance with STIGs.
- 1030 E-2.E.4. Comply with placement of sensors from MCND.
- 1031 E-2.E.5. Ensure feeds of Host CND Tools to MCND.
- 1032 E-2.E.6. Install Host CND Tools (e.g. HBSS, ACAS).
- 1033 E-2.F. Incident Response Plan
- 1034 E-2.F.1. Ensure CSP data spill cleanup method is incorporated into SLA
- 1035 E-2.F.2. Ensure CSP incident response plan is incorporated into SLA, including:
- 1036 a) Communication plans
- 1037 b) Thresholds for reporting
- 1038 c) Requirement to comply with designated MCND
- 1039 E-2.G. Review SLA every six months for potential updates (e.g. POCs, etc.)
- 1040 **E-3. Mission Owner Cyber Incident and Event Procedures**
- 1041 E-3.A. Initial Cloud Activity Assessment
- 1042 E-3.A.1. Mission Owner notifies the MCND of the suspected cyber incident or event.
- 1043 E-3.A.2. The Mission Owner shall support any assessments requested by the MCND. This may
- 1044 be in relation to a TASKORD issued by JFHQ-DoDIN to the MCND.
- 1045 E-3.B. Response to Unauthorized Access / Intrusion
- 1046 E-3.B.1. Execute Mission Owner Initial Cloud Activity Assessment, Section E-3.A.
- 1047 E-3.B.2. The MCND shall support remediation activities as directed by the MCND in support of
- 1048 JFHQ-DODIN TASKORDs or MCND identified unauthorized accesses/intrusions.
- 1049 E-3.C. Response to Unsuccessful Activity Attempt
- 1050 E-3.C.1. If the event is identified by the Mission Owner, the Mission Owner notifies the MCND.
- 1051 E-3.C.2. Support MCND development of SAR.
- 1052 E-3.C.3. The MCND shall support preventative activities as directed by the MCND in support of
- 1053 the JFHQ-DoDIN TASKORDs or MCND identified unsuccessful activity attempt.
- 1054 E-3.D. Response to DoS
- 1055 E-3.D.1. Execute Mission Owner Initial Cloud Activity Assessment, Section E-3.A. In
- 1056 notification to MCND, note extent of Mission impact (if any).
- 1057 E-3.D.2. The Mission Owner shall support DoS courses of action as directed by the MCND in
- 1058 support of either JFHQ-DoDIN TASKORDs or MCND identified DoS activity.

1059 E-3.E. Response to Non-Compliance Activity

1060 E-3.E.1. Execute Mission Owner Initial Cloud Activity Assessment, Section E-3.A. In
1061 notification to MCND, note extent of Mission impact (if any).

1062 E-3.E.2. The Mission Owner shall implement Non-Compliance Activity courses of action as
1063 directed by the MCND in support of JFHQ-DoDIN TASKORDs or MCND identified Non-
1064 Compliance Activity.

1065 E-3.F. Response to Reconnaissance

1066 E-3.F.1. Notify MCND.

1067 E-3.F.2. Support the development of a SAR by the MCND.

1068 E-3.F.3. Support MCND effort to determine source or cause of reconnaissance for signs of
1069 unauthorized access or malware.

1070 E-3.F.4. MCND will determine need, if any, for preventative countermeasures on the Mission
1071 systems, applications, CSO, or connection configuration to the CSP. Mission Owner shall comply
1072 with prescribed preventative countermeasures.

1073 E-3.G. Response to Malicious Logic

1074 E-3.G.1. Execute Mission Owner Initial Cloud Activity Assessment, Section E-3.A. In
1075 notification to MCND, note extent of Mission impact (if any).

1076 E-3.G.2. The Mission Owner shall support malicious logic courses of action as directed by the
1077 MCND in support of JFHQ-DoDIN TASKORDs or MCND identified malicious logic.

1078 E-3.H. Response to Explained Anomaly

1079 E-3.H.1. Execute Initial Cloud Activity Assessment, Section E-3.A.

1080 E-3.H.2. If possible, implement process or tool update to reduce occurrence of Explained
1081 Anomaly.

1082 E-3.I. Response to Spillage/Unauthorized Disclosure

1083 E-3.I.1. Notify MCND of spillage/unauthorized disclosure.

1084 E-3.I.2. Investigate scope of spillage/unauthorized disclosure, to include copies propagated to
1085 other storage media and/or backups. Request support as needed from relevant MCND and/or
1086 BCND.

1087 E-3.I.3. Remediate spillage/unauthorized disclosure in coordination with MCND and BCND.
1088 Where necessary, direct CSP to conduct data spill cleanup IAW procedures defined in CSO PA
1089 Assessment.

1090 E-3.I.4. When complete, report closure to MCND.

1091 E-3.J. Performing VS

1092 E-3.J.1. Mission Owner performs VS (who is responsible for reporting compliance to
1093 USCYBERCOM per CTO).

1094 E-3.J.2. Mission Owner creates POA&M.

1095 E-3.J.3. Mission Owner reports results compliance results, POA&Ms, open items to MCND.

- 1096 E-3.K. Performing Annual External Assessments
- 1097 E-3.K.1. Coordinate request type (e.g. Red Team, Blue Team, Penetration Testing, etc.) with the
1098 MCND.
- 1099 E-3.K.2. Receive a full report of findings and recommendations from the CND that performs the
1100 assessment.
- 1101 E-3.K.3. Report to MCND on remediation plans, including applicable POA&Ms.
- 1102 E-3.L. Performing CM/Patching
- 1103 The following steps pertain to Mission Owners utilizing an IaaS CSO. There may be applicable cases
1104 for Mission Owners utilizing PaaS CSOs as well if they allow the inclusion of Mission-Owner
1105 provided software packages or libraries.
- 1106 E-3.L.1. Mission Owner receives requirement to patch systems/apps (is accountable for
1107 compliance).
- 1108 E-3.L.2. Mission Owner acquires or develops patch.
- 1109 E-3.L.3. Mission Owner tests patch.
- 1110 a) Mission Owner follows Configuration Control Broad (CCB) process as defined by its
1111 Component to ensure that any patches implemented do not adversely affect the functionality
1112 of the Cloud-hosted systems and CSO.
- 1113 b) If outage is required, follow the Planned Outage for DoD to CSP and DoD Authorized
1114 Service Interruption (ASI) process.
- 1115 c) Validate operations.
- 1116 E-3.L.4. Mission Owner notifies MCND of patch schedule/outage.
- 1117 E-3.L.5. Mission Owner applies the patch.
- 1118 E-3.L.6. Mission Owner reports restoration of service and success of patch deployment to MCND
1119 and JFHQ-DoDIN per CTO/IAVM Process.
- 1120 E-3.L.7. Mission Owner provides updated CM/Patching documentation to MCND.
- 1121 E-3.M. Performing Planned Outage
- 1122 E-3.M.1. If the Planned Outage is initiated by DOD.
- 1123 a) Mission Owner plans outage.
- 1124 b) Mission Owner notifies CSP.
- 1125 c) Mission Owner notifies MCND.
- 1126 d) At conclusion of Planned Outage, Mission Owner notifies CSP of restoration of service.
- 1127 E-3.M.2. If the Planned Outage is initiated by the CSP
- 1128 a) Mission Owner will be notified of planned outage by the CSP.
- 1129 b) Mission Owner notifies MCND
- 1130 E-3.N. Response to Unplanned Outage

- 1131 E-3.N.1. Mission Owner supports MCND impact assessment.
- 1132 E-3.N.2. Mission Owner statuses CSP until closure/resolution; tracks status.
- 1133 E-3.O. Performing Disaster Recovery
- 1134 E-3.O.1. Execute disaster recovery procedures to restore Cloud-hosted functionality.
- 1135 E-3.P. Response to Training and Exercises
- 1136 E-3.P.1. Execute Mission Owner Initial Cloud Activity Assessment, Section E-3.A.
- 1137

DRAFT

1138
1139
11401141 **ANNEX F: JFHQ-DoDIN**1142 **F-1. JFHQ-DoDIN Introduction**

1143 JFHQ-DoDIN provides operational C2 for CND under USCYBERCOM. JFHQ-DoDIN can issue
1144 TASKORDs against CNDSPs – including the DoDIN CND, BCND, and MCNDs. As part of
1145 USCYBERCOM it can acquire and disseminate DoDIN Intel to the CND community and coordinate
1146 external interactions. As the nexus of CND reporting, JFHQ-DoDIN can perform trending analysis,
1147 correlate cyber incidents and events, and construct a broad and cohesive cyber SA picture. JFHQ-DoDIN
1148 is envisioned working in close collaboration with the DoDIN CND for coordinating data aggregation for
1149 cyber incidents or events that span multiple Mission Owners, BCAPs, or multiple CSPs in order to
1150 enhance comprehension and decision-making. If more than one organization is affected, or if a significant
1151 risk to the DoDIN exists, JFHQ-DoDIN may release TASKORDs and evaluate DoDIN CPT deployments
1152 to components without organic teams.

1153 **F-2. JFHQ-DoDIN Responsibilities**1154 **F-2.A. CND**

- 1155 F-2.A.1. Disseminate CND policies and DoDIN-wide CND requirements to CNDs.
- 1156 F-2.A.2. Acquire and disseminate DoDIN Intel.
- 1157 F-2.A.3. Provide Orders/Tasks in coordination with BCND.
- 1158 F-2.A.4. Deconflict external assessments.
- 1159 F-2.A.5. Require aggregation by BCND.
- 1160 F-2.A.6. Task MCNDs and require reporting through BCND.
- 1161 F-2.A.7. Receive and retain trending and reports from BCND.
- 1162 F-2.A.8. Perform trending across DoDIN.

1163 **F-2.B. Coordinate with:**

- 1164 F-2.B.1. Law Enforcement (LE)
- 1165 F-2.B.2. Intelligence Community
- 1166 F-2.B.3. Counterintelligence (CI)
- 1167 F-2.B.4. National Security Agency/Central Security Service Threat Operations Center (NTOC)
- 1168 F-2.B.5. US-CERT
- 1169 F-2.B.6. Combatant Command/Service/Agency/Field Activity (CC/S/A/FA)
- 1170 F-2.B.7. Information/Intel Sharing with CNDSPs

1171 F-2.C. Shall maintain a POC list.

1172 F-2.C.1. Maintain current contact lists for POCs at DoDIN CND, BCNDs, MCNDs, Mission
1173 Owners, CSPs, JCCs, LE agencies, Intelligence agencies, CI, NTOC, and US-CERT, and JCCs
1174 for:

1175 a) Cyber event and incident response reporting (see Figure 1 – DoD Cloud CND C2 Model),
1176 including: guidance/orders and reporting

1177 b) CND coordination (see Figure 2 - DoD Cloud CND C3 Data Sharing), including: SARs
1178 distribution and CND data sharing

1179 c) Distribution lists for: SARs, POA&Ms, external assessments (plans, reports, findings), VS
1180 schedules, and outage notices

1181 F-2.C.2. Maintain JFHQ-DoDIN POC list; distribute changes to POC list to DoDIN CND,
1182 BCNDs, MCNDs, Mission Owners, and CSPs

1183 **F-3. JFHQ-DoDIN Cyber Incident and Event Procedures**

1184 F-3.A. Initial Cloud Activity Assessment

1185 F-3.A.1. If initiated by JFHQ-DoDIN (e.g. in response to NTOC report, sensor log analysis, etc.),
1186 via incoming notification from external (e.g. US-CERT), or from internal reporting via JIMS
1187 then:

1188 a) JFHQ-DoDIN analyses the cyber event or incident to determine breadth and severity of
1189 impact.

1190 b) As needed, notifies DoDIN CND, BCNDs, and/or MCNDs.

1191 F-3.A.2. JFHQ-DoDIN, with coordination and support from DoDIN CND, analyzes and
1192 determines whether to release TASKORDs; disseminates to DoDIN CND, BCNDs, and/or
1193 MCNDs.

1194 F-3.A.3. JFHQ-DoDIN evaluates DoDIN CPT activation.

1195 F-3.A.4. JFHQ-DoDIN receives TASKORD updates from DoDIN CND, BCNDs, and/or
1196 MCNDs; monitors to closure.

1197 F-3.B. Response to Unauthorized Access / Intrusion

1198 F-3.B.1. If BCND or MCND finds no DoD impact as a result of their Initial Cloud Activity
1199 Assessments:

1200 a) If the CSO does not have a FedRAMP PA, stop this procedure at this step.

1201 b) If the CSO does have a FedRAMP PA, JFHQ-DoDIN notifies US-CERT.

1202 c) Stop this procedure at this step.

1203 F-3.B.2. If BCND or MCND finds DoD impact as a result of their Initial Cloud Activity
1204 Assessments:

UNCLASSIFIED

- 1205 a) JFHQ-DoDIN, with coordination and support from BCND, authors TASKORDs;
1206 disseminates to BCND and MCNDs.
- 1207 b) JFHQ-DoDIN evaluates DoDIN CPT activation.
- 1208 c) JFHQ-DoDIN receives TASKORD updates from BCND; monitors to closure.

1209 F-3.C. Response to Unsuccessful Activity Attempt

1210 F-3.C.1. If JFHQ-DoDIN receives notice from BCND of a sustained wave of unsuccessful
1211 activity attempts:

- 1212 a) JFHQ-DoDIN, with coordination and support from BCND, authors TASKORDs;
1213 disseminates to BCND and MCNDs.
- 1214 b) JFHQ-DoDIN evaluates DoDIN CPT activation.
- 1215 c) JFHQ-DoDIN receives TASKORD updates from BCND; monitors to closure.

1216 F-3.D. Response to DoS

1217 F-3.D.1. Execute JFHQ-DoDIN Initial Cloud Activity Assessment, Section F-3.A.

1218 F-3.E. Response to Non-Compliance Activity.

1219 F-3.E.1. Execute JFHQ-DoDIN Initial Cloud Activity Assessment, Section F-3.A.

1220 F-3.F. Response to Reconnaissance

1221 F-3.F.1. If JFHQ-DoDIN receives notice from BCND or MCNDs of a sustained wave of
1222 reconnaissance activities:

- 1223 a) JFHQ-DoDIN, with coordination and support from DoDIN CND, authors TASKORDs;
1224 disseminates to DoDIN CND, BCNDs, and MCNDs with request for DoDIN CND on copy
1225 on TASKORD updates.
- 1226 b) JFHQ-DoDIN evaluates DoDIN CPT activation.
- 1227 c) JFHQ-DoDIN updates any involved external notifiers.
- 1228 d) JFHQ-DoDIN receives TASKORD updates; monitors to closure.

1229 F-3.G. Response to Malicious Logic

1230 F-3.G.1. If JFHQ-DoDIN receive from BCND or MCNDs of a sustained wave of malicious logic
1231 activities:

- 1232 a) JFHQ-DoDIN, with coordination and support from BCND, authors TASKORDs;
1233 disseminates to BCND and MCNDs.
- 1234 b) JFHQ-DoDIN evaluates DoDIN CPT activation.
- 1235 c) JFHQ-DoDIN receives TASKORD updates from BCND; monitors to closure.

1236 F-3.H. Response to Explained Anomaly

1237 F-3.H.1. Execute JFHQ-DoDIN Initial Cloud Activity Assessment, Section F-3.A.

UNCLASSIFIED

UNCLASSIFIED

- 1238 F-3.H.2. If possible, implement process or tool update to reduce occurrence of Explained
1239 Anomaly.
- 1240 F-3.I. Response to Spillage/Unauthorized Disclosure
- 1241 F-3.I.1. Execute JFHQ-DoDIN Initial Cloud Activity Assessment, Section F-3.A.
- 1242 F-3.J. Performing VS
- 1243 F-3.J.1. JFHQ-DoDIN updates VS trending data for the Missions.
- 1244 F-3.J.2. JFHQ-DoDIN updates VS trending data for the CSPs.
- 1245 F-3.K. Performing Annual External Assessments
- 1246 F-3.K.1. External assessments do not require JFHQ DoDIN direction or involvement.
- 1247 F-3.L. Performing CM/Patching
- 1248 F-3.L.1. JFHQ-DoDIN receives reports of Mission Owner patch deployments per CTO/IAVM
1249 Process.
- 1250 F-3.L.2. JFHQ-DoDIN receives reports of CSP patch deployments (via US-CERT for FedRAMP-
1251 authorized CSOs).
- 1252 F-3.M. Performing Planned Outage
- 1253 F-3.M.1. If a planned outage is scheduled, JFHQ-DODIN will be notified of planned outage by
1254 the relevant MCND, regardless of who initiated the outage.
- 1255 F-3.N. Response to Unplanned Outage
- 1256 F-3.N.1. JFHQ-DoDIN receives report of CSP outage and Mission impact from MCND.
- 1257 F-3.N.2. JFHQ-DoDIN receives report of aggregate impact (if multiple Missions are impacted)
1258 from BCND.
- 1259 F-3.O. Performing Disaster Recovery
- 1260 F-3.O.1. Maintain SA of the MCND and Mission Owner efforts to execute disaster recovery
1261 procedures to restore Cloud-hosted functionality.
- 1262 F-3.P. Response to Training and Exercises
- 1263 F-3.P.1. Execute JFHQ-DoDIN Initial Cloud Activity Assessment, Section F-3.A.

UNCLASSIFIED

1264
1265
1266

1267 **ANNEX G: CSP**

1268 **G-1. CSP Introduction**

1269 The CSP is responsible for the maintenance and operation of the CSO that are procured and used by
1270 Mission Owners. The CSP can be a commercial vendor or a Federal organization that provides CSOs for
1271 Mission use. The scope of CND responsibility of the CSP for the Mission Applications and Mission Data
1272 depends on the service delivery model used (IaaS, PaaS, or SaaS). The CSP provides CNDSP services for
1273 their infrastructure and service offerings. This complements to the MCND services for the Mission
1274 Applications and Mission data using the CSP infrastructure and service offerings.

1275 Per the Cloud Computing SRG, all DoD information/data placed or created in a CSP's CSO is owned by
1276 the DoD and the Mission Owner and/or their Information Owner unless otherwise stipulated in the CSP's
1277 contract with the DoD²¹.

1278 The CSP reporting channels will be different for CSOs offered under FedRAMP vs. DoD PA, such as a
1279 FedRAMP+. These and additional requirements for the CSP must be specified in the SLAs covering the
1280 relationships between the CSP and each of the Mission Owners. In time it is expected that CSP reporting
1281 requirements will be met through automated means.

1282 Per the C2 model in Figure 1, the CSP is under the directive authority of their subscriber Mission Owners.
1283 Via that relationship, the CSP is expected to support and comply with efforts to resolve issues under the
1284 direction of their Mission Owners.

1285 **G-2. CSP Responsibilities**

1286 CSP responsibilities shall be documented in the appropriate SLA and include:

1287 G-2.A. Shall Provide to Mission Owner

1288 G-2.A.1. CSP maintain a copy of the SLA with the Mission Owner.

1289 G-2.A.2. Assist on developing future automated capabilities that could increase efficiencies.

²¹ Reference (d): Cloud Computing SRG Section 5.5.2 states, "All DoD information/data placed or created in a CSP's CSO is owned by the DoD and the Mission Owner and/or their Information Owner unless otherwise stipulated in the CSP's contract with the DoD. The CSP has no rights to the DoD's information/data. DoD information/data includes logs and monitoring data created within a Mission Owner's system/application implemented in IaaS/PaaS CSOs. CSPs seeking a DoD PA must agree that DoD remains the owner of all DoD data in a CSO. 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)."

- 1290 G-2.A.3. Maintain a current CSP Technical POC list with the Mission Owner.
- 1291 G-2.A.4. Provide open CSO vulnerability POA&M to Mission Owner.
- 1292 G-2.B. Shall maintain a POC list
- 1293 G-2.B.1. Maintain current lists of POCs at US-CERT, Mission Owners, and relevant
1294 MCNDs/BCNDs:
- 1295 a) Cyber event and incident response reporting (see Figure 1 – DoD Cloud CND C2 Model),
1296 including: guidance/orders and reporting
- 1297 b) CND coordination (see Figure 2 - DoD Cloud CND C3 Data Sharing), including: SARs
1298 distribution and CND data sharing
- 1299 c) Distribution lists for: SARs, POA&Ms, external assessments (plans, reports, findings), VS
1300 schedules, and outage notices
- 1301 G-2.B.2. Maintain CSP POC list; with every POC change, distribute changes to POC list to
1302 JFHQ-DoDIN, DoDIN CND, relevant BCNDs, relevant MCNDs, and relevant Mission Owners
- 1303 G-2.B.3. Provide DIB ID number to MCND
- 1304 G-2.C. Shall Meet Continuous Monitoring and Incident Reporting Requirements
- 1305 G-2.C.1. If the CSO is authorized through FedRAMP, the CSP shall report for Continuous
1306 Monitoring and Incident Reporting via FedRAMP protocols to US-CERT and/or FedRAMP
1307 PMO and to the mission owner as articulated in the SLA. In addition, the SLA may contain
1308 reporting requirements specific to each Mission Owner.
- 1309 G-2.C.2. If the CSO is authorized through a DoD Agency AO (such as FedRAMP+), the CSP
1310 shall report for Continuous Monitoring and Incident Reporting via the terms of the DoD
1311 Authority to Operate (ATO) and Mission Owner SLAs.
- 1312 **G-3. CSP Cyber Incident and Event Procedures**
- 1313 G-3.A. Initial Cloud Activity Assessment
- 1314 G-3.A.1. If initiated via incoming notification from another entity (e.g. BCND, MCND, US-
1315 CERT, etc.) or via internal sensing and analysis, the CSP investigates for scope of impact to DoD
1316 and/or CSO.
- 1317 G-3.A.2. Communicate findings to the impacted Mission Owner(s) in addition to other required
1318 reporting channels (e.g. US-CERT for FedRAMP-authorized CSOs).
- 1319 G-3.A.3. Report updated SARs to Mission Owners.
- 1320 G-3.B. Response to Unauthorized Access / Intrusion
- 1321 G-3.B.1. CSP notifies all potentially impacted Mission Owners, who in turn notify their MCNDs
1322 to initiate a Mission impact assessment.
- 1323 G-3.B.2. If incident or event occurred on a FedRAMP-authorized CSO, CSP reports incident or
1324 event to US-CERT.
- 1325 G-3.B.3. CSP periodically reports remediation progress to potentially impacted Mission Owners
1326 until closure.

- 1327 G-3.C. Response to Unsuccessful Activity Attempt
- 1328 G-3.C.1. If the event is identified by the CSP, the CSP develops a SAR and distributes it to the
- 1329 impacted Mission Owners.
- 1330 G-3.D. Response to DoS
- 1331 G-3.D.1. Execute CSP Initial Cloud Activity Assessment, Section G-3.A.
- 1332 G-3.E. Response to Non-Compliance Activity
- 1333 G-3.E.1. Execute CSP Initial Cloud Activity Assessment, Section G-3.A.
- 1334 G-3.F. Response to Reconnaissance
- 1335 G-3.F.1. If the event is identified by the CSP, the CSP develops a SAR and distributes it to the
- 1336 impacted Mission Owners.
- 1337 G-3.G. Response to Malicious Logic
- 1338 G-3.G.1. Execute CSP Initial Cloud Activity Assessment, Section G-3.A.
- 1339 G-3.H. Response to Explained Anomaly
- 1340 G-3.H.1. Execute Initial Cloud Activity Assessment, Section G-3.A.
- 1341 G-3.H.2. If possible, implement process or tool update to reduce occurrence of Explained
- 1342 Anomaly.
- 1343 G-3.I. Response to Spillage/Unauthorized Disclosure
- 1344 G-3.I.1. Execute CSP Initial Cloud Activity Assessment, Section G-3.A.
- 1345 G-3.I.2. Support Mission Owner and MCND investigation into spillage/unauthorized disclosure.
- 1346 G-3.I.3. Support Mission Owner and MCND in remediation effort. As directed by Mission
- 1347 Owner, execute CSP data spill/unauthorized disclosure cleanup method as defined in CSO PA
- 1348 Assessment.
- 1349 G-3.J. Performing VS
- 1350 G-3.J.1. CSP performs VS within the CSO authorization boundary.
- 1351 G-3.J.2. CSP creates POA&M.
- 1352 G-3.J.3. CSP reports results to FedRAMP PMO.
- 1353 G-3.K. Performing Annual External Assessments
- 1354 G-3.K.1. If the CSP provides some of the controls to the Mission Owner via the SLA, then:

- 1355 a) CSP receives notice from the Mission Owner of an Annual External Assessment plan.
1356 b) CSP coordinates resources to support Annual External Assessment (e.g., Pen Test, Red
1357 Team, etc.).
1358 c) CSP delivers data packages to Mission Owner to complete its role in the Annual External
1359 Assessment.

1360 G-3.L. Performing CM/Patching

1361 Patching is a required, routine activity. CSPs and Mission Owners can incorporate into SLA that
1362 Mission Owners will utilize FedRAMP reports to satisfy CSP reporting responsibilities to the Mission
1363 Owner.

1364 G-3.L.1. CSP receives a patch for systems/apps of the CSO.

1365 G-3.L.2. CSP follows reporting responsibilities to FedRAMP, US-CERT, Mission Owner.

1366 G-3.L.3. CSP follows defined patch process. If outage is required, CSP would follow Section G-
1367 3.MG-3.N, Performing Planned Outage procedures.

1368 G-3.L.4. CSP reports restoration of service and success of patch deployment to Mission Owner,
1369 FedRAMP PMO, US-CERT.

1370 G-3.M. Performing Planned Outage

1371 G-3.M.1. If the Planned Outage is initiated by CSP

1372 a) CSP plans outage.

1373 b) CSP notifies Mission Owners.

1374 c) If CSO operates under FedRAMP authorization, CSP notifies US-CERT and FedRAMP
1375 PMO.

1376 d) At conclusion of Planned Outage, CSP notifies Mission Owners of restoration of service.

1377 G-3.M.2. If the Planned Outage is initiated by DoD, the CSP will be notified of planned outage
1378 by Mission Owners.

1379 G-3.N. Response to Unplanned Outage

1380 G-3.N.1. CSP notifies Mission Owners.

1381 G-3.N.2. If CSO operates under FedRAMP authorization, CSP notifies US-CERT and FedRAMP
1382 PMO.

1383 G-3.N.3. At conclusion of Unplanned Outage, CSP notifies Mission Owners of restoration of
1384 service.

1385 G-3.O. Performing Disaster Recovery

1386 G-3.O.1. Assist Mission Owner upon request in executing disaster recovery procedures to restore
1387 Cloud-hosted functionality.

1388 G-3.P. Response to Training and Exercises

1389 The following procedure pertains to cyber incidents detected by the CSP that are determined to be
1390 associated to a training or exercise event.

1391 G-3.P.1. Execute CSP Initial Cloud Activity Assessment, Section G-3.A.

DRAFT

1392
 1393
 1394

1395 **ANNEX H: CLOUD CND COMMUNICATIONS MATRIX**

1396 The below table represents the means of communications available to be used by CND Organization to
 1397 report or share data regarding CDN incidents and events.

1398 **Table 2 - Cloud CND Communications Matrix**

Means of Communications	milCloud	CSP (CSO On-Prem)	CSP (CSO Off-Prem)	Mission Owner	MCND	BCND	DoDIN CND	JFHQ-DODIN	US-CERT
CSP (milCloud)									
JIMS					X				
Classified Comms (e.g. SIPRNet, STE, etc.)				X	X				
Unclassified Comms (e.g. NIPRNet, Phone, etc.)				X	X				
CSP (CSO On-Prem)									
US-CERT Incident Response System									X
DIBNet				X	X				X
Unclassified Comms (e.g. Internet, Phone, etc.)				X	X				X
CSP (CSO Off-Prem)									
US-CERT Incident Response System									X
DIBNet				X	X	X			X
Unclassified Comms (e.g. Internet, Phone, etc.)				X	X	X			X
Mission Owner									
DIBNet		X	X						
Classified Comms (e.g. SIPRNet, STE, etc.)	X				X				
Unclassified Comms (e.g. NIPRNet, Phone, etc.)	X	X	X		X				

UNCLASSIFIED

Means of Communications	milCloud	CSP (CSO On-Prem)	CSP (CSO Off-Prem)	Mission Owner	MCND	BCND	DoDIN CND	JFHQ-DODIN	US-CERT
MCND									
JIMS					X	X	X	X	
DIBNet		X	X						
Classified Comms (e.g. SIPRNet, STE, etc.)	X			X	X	X	X	X	
Unclassified Comms (e.g. NIPRNet, Phone, etc.)	X	X	X	X	X	X	X	X	
BCND									
JIMS					X	X	X	X	
DIBNet			X						
Classified Comms (e.g. SIPRNet, STE, etc.)					X	X	X	X	
Unclassified Comms (e.g. NIPRNet, Phone, etc.)			X		X	X	X	X	
DoDIN CND									
US-CERT Incident Response System									X
JIMS					X	X		X	
JWICS						X		X	X
Classified Comms (e.g. SIPRNet, STE, etc.)					X	X		X	
Unclassified Comms (e.g. NIPRNet, Phone, etc.)					X	X		X	X
JFHQ-DODIN									
US-CERT Incident Response System									X
JIMS					X	X	X		
JWICS							X		X
Classified Comms (e.g. SIPRNet, STE, etc.)					X	X	X		
Unclassified Comms (e.g. NIPRNet, Phone, etc.)					X	X	X		X

Means of Communications	milCloud	CSP (CSO On-Prem)	CSP (CSO Off-Prem)	Mission Owner	MCND	BCND	DoDIN CND	JFHQ-DODIN	US-CERT
US-CERT									
US-CERT Incident Response System	X	X	X				X	X	
Classified Comms (e.g. JWICS, SIPRNet, STE, etc.)							X	X	
DIBNet		X	X						
Unclassified Comms (e.g. Internet, Phone, etc.)	X	X	X				X	X	

1399

DRAFT

UNCLASSIFIED

1400 RME, DEFENSE INFORMATION SYSTEMS AGENCY
1401 CHAMBERSBURG, PENNSYLVANIA 17201
1402 21 Sep 2015

1403 **ANNEX I: REFERENCES**

- 1404 (a) Joint Chiefs of Staff. (2012, July). Chairman of the Joint Chiefs of Staff Manual (CJCSM)
1405 6510.01B: Cyber Incident Handling Program.
1406 http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf
- 1407 (b) DoD O-8530.1-M CNDSP C&A Process Manual.
- 1408 (c) DoDI 8530.1 Evaluator Scoring Metrics.
- 1409 (d) Defense Information Systems Agency (DISA). (2015, February). DoD Cloud Computing SRG.
1410 http://iase.disa.mil/cloud_security/cloudsrg/Pages/home.aspx
- 1411 (e) DISA. (2014, June). DISA's Strategy for Defensive Cyber Operations.
- 1412 (f) DISN Connection Process Guide (CPG) Home Page. [http://www.disa.mil/Services/Network-](http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide)
1413 [Services/Enterprise-Connections/Connection-Process-Guide](http://www.disa.mil/Services/Enterprise-Connections/Connection-Process-Guide)
- 1414 (g) FedRAMP Home Page. <http://cloud.cio.gov/fedramp>
- 1415 (h) United States Code, Title 44.
- 1416 (i) National Institute of Standards and Technology. (2011, September). NIST SP800-145: The NIST
1417 Definition of Cloud Computing. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- 1418 (j) US-CERT Federal Incident Reporting Guidelines. [https://www.us-cert.gov/government-](https://www.us-cert.gov/government-users/reporting-requirements#tax)
1419 [users/reporting-requirements#tax](https://www.us-cert.gov/government-users/reporting-requirements#tax)<https://www.us-cert.gov/government-users/reporting-requirements#tax>
- 1420 (k) DISA. (2015, June). Cloud Access Point (CAP) Security Functional Requirements Document
1421 (FRD).
- 1422 (l) Joint Chiefs of Staff. (2011, February). CJCSM 6510.01F: Information Assurance (IA) and
1423 Support to Computer Network Defense (CND).
1424 http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
- 1425 (m) US-CERT. (2014, October). US-CERT Federal Incident Notification Guidelines. [https://www.us-](https://www.us-cert.gov/incident-notification-guidelines)
1426 [cert.gov/incident-notification-guidelines](https://www.us-cert.gov/incident-notification-guidelines)
- 1427 (n) DoD CIO. (2013, August). DoDI 8320.02: Sharing Data, Information, and Information
1428 Technology (IT) Services in the Department of Defense.
1429 www.dtic.mil/whs/directives/corres/pdf/832002p.pdf

UNCLASSIFIED

UNCLASSIFIED

- 1430 (o) DoD CIO. (2015, August). DoDI 8320.07: Implementing the Sharing of Data, Information, and
1431 Information Technology (IT) Services in the Department of Defense.
1432 www.dtic.mil/whs/directives/corres/pdf/832007p.pdf
- 1433 (p) DoD. (2012, February). DoDM 5200.01 Vol 3: DoD Information Security Program: Protection of
1434 Classified Information. http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf

DRAFT

UNCLASSIFIED

1435
1436
1437

1438 **ANNEX J: ABBREVIATIONS AND ACRONYMS**

- 1439 ACAS Assured Compliance Assessment Solution
- 1440 APT Advanced Persistent Threat
- 1441 AS&W Attack Sensing & Warning
- 1442 ATO Authority to Operate
- 1443 AV Anti-Virus
- 1444 BCAP Boundary Cloud Access Point
- 1445 BCND Boundary Computer Network Defense
- 1446 C2 Command and Control
- 1447 C3 Command, Control, and Communications
- 1448 CAP Cloud Access Point
- 1449 CCB Configuration Control Broad
- 1450 CC/S/A/FA Combatant Command/Service/Agency/Field Activity
- 1451 CI Counterintelligence
- 1452 CJCSM Chairman of the Joint Chiefs of Staff Manual
- 1453 CM Configuration Management
- 1454 CMRS Continuous Monitoring and Risk Scoring
- 1455 CND Computer Network Defense
- 1456 CNDSP Computer Network Defense Service Provider
- 1457 CPT Cyber Protection Team
- 1458 CSO Cloud Service Offering
- 1459 CSP Cloud Service Provider
- 1460 CTO Cyber Task Order

UNCLASSIFIED

1461	DIBNet	Defense Industrial Base Network
1462	DISA	Defense Information Systems Agency
1463	DISN	Defense Information Systems Network
1464	DoD	Department of Defense
1465	DoDI	Department of Defense Instruction
1466	DoS	Denial of Service
1467	DoDIN	Department of Defense Information Network
1468	DoDIN CND	Department of Defense Information Network Computer Network Defense
1469	DoDM	Department of Defense Manual
1470	FedRAMP	Federal Risk and Authorization Management Program
1471	HBSS	Host Based Security System
1472	I&W	Indications & Warnings
1473	IaaS	Infrastructure as a Service
1474	IAP	Internet Access Point
1475	ICAP	Internal Cloud Access Point
1476	JAB	Joint Authorization Board
1477	JCC	Joint Cyber Center
1478	JFHQ-DoDIN	Joint Force Headquarters DoD Information Network
1479	JIE	Joint Information Environment
1480	JIMS	Joint Incident Management System
1481	LE	Law Enforcement
1482	MCND	Mission Computer Network Defense
1483	NIST	National Institute of Standards and Technology
1484	NTOC	National Security Agency/Central Security Service Threat Operations Center
1485	PaaS	Platform as a Service
1486	PA	Provisional Authorization

UNCLASSIFIED

UNCLASSIFIED

1487	POA&M	Plan of Action and Milestones
1488	POND	Period of Non-Disruption
1489	RME	Risk Management Executive
1490	RTO	Recovery Time Objective
1491	SaaS	Software as a Service
1492	SA	Situational Awareness
1493	SAR	Situational Awareness Report
1494	SIEM	Security Information and Event Management
1495	SLA	Service Level Agreement
1496	SRG	Security Requirements Guide
1497	SQL	Structured Query Language
1498	TIPR	Threat Intelligence Product Report
1499	US-CERT	United States Computer Emergency Readiness Team
1500	VPN	Virtual Private Network
1501	VS	Vulnerability Scan
1502	XCA	Cross-Cloud Analysis
1503	XSS	Cross-Site Scripting

RME, DEFENSE INFORMATION SYSTEMS AGENCY
CHAMBERSBURG, PENNSYLVANIA 17201
21 Sep 2015

1504
1505
1506

1507 **ANNEX K: CLOUD CND DEFINITIONS**

1508 **Boundary Cloud Access Point (BCAP):** DISN perimeter gateway that provides a barrier of protection
1509 between the DISN and the CSO.

1510 **Boundary Computer Network Defense (BCND):** The CNDSP for a BCAP; the BCAP aligns to a
1511 BCND. The BCND defends the DISN at the BCAP.

1512 **Blue Team:** As defined in CNSSI-4009, *“A group of individuals that conduct operational network
1513 vulnerability evaluations and provide mitigation techniques to customers who have a need for an
1514 independent technical review of their network security posture. The Blue Team identifies security threats
1515 and risks in the operating environment, and in cooperation with the customer, analyzes the network
1516 environment and its current state of security readiness. Based on the Blue Team findings and expertise,
1517 they provide recommendations that integrate into an overall community security solution to increase the
1518 customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a
1519 Red Team employment to ensure that the customer's networks are as secure as possible before having the
1520 Red Team test the systems.”*

1521 **Classified Information:** As defined in CNSSI-4009, *“Information that has been determined pursuant to
1522 Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure
1523 and is marked to indicate its classified status when in documentary form.”*

1524 **Cloud Service Provider (CSP):** Commercial vendor or Federal organization offering or providing cloud
1525 services (Includes DoD CSPs); the provider of CSOs.

1526 **Community Cloud:** A multi-tenant cloud in which services are provided for the exclusive use of the
1527 DoD and Federal Government organizations. Resources providing the cloud services must be dedicated to
1528 Federal Government use and require physical separation from non-DoD/non-Federal customers.

1529 **Computer Network Defense (CND):** As defined in CNSSI-4009, *“Actions taken to defend against
1530 unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as
1531 trend and pattern analysis), and response and restoration activities.”*

1532 **Computer Network Defense Service Provider (CNDSP):** Provides CND services and C2 direction
1533 addressing the protection of the network, detection of threats, and response to incidents; certified in
1534 accordance with DoDI 8530.2: Support to Computer Network Defense.

1535 **Configuration Control Board (CCB):** As defined in CNSSI-4009, *“A group of qualified people with
1536 responsibility for the process of regulating and approving changes to hardware, firmware, software, and
1537 documentation throughout the development and operational lifecycle of an information system.”*

UNCLASSIFIED

1538 **Continuous Monitoring:** As defined in CNSSI-4009, *“The process implemented to maintain a current*
1539 *security status for one or more information systems or for the entire suite of information systems on which*
1540 *the operational mission of the enterprise depends. The process includes: 1) The development of a strategy*
1541 *to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the*
1542 *effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or*
1543 *changes that affect IA risks, and 4) Publishing the current security status to enable information sharing*
1544 *decisions involving the enterprise.”*

1545 **Countermeasure:** As defined in CNSSI-4009, *“Actions, devices, procedures, or techniques that meet or*
1546 *oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing*
1547 *the harm it can cause, or by discovering and reporting it so that corrective action can be taken.”*

1548 **Cyber Incident:** As defined in CNSSI-4009, *“Actions taken through the use of computer networks that*
1549 *result in an actual or potentially adverse effect on an information system and/or the information residing*
1550 *therein. See incident.”*

1551 **Denial of Service (DoS):** As defined in CNSSI-4009, *“The prevention of authorized access to resources*
1552 *or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours,*
1553 *depending upon the service provided.)”*

1554 **Defense Information Systems Network (DISN):** As defined in JP 1-02, *“The integrated network,*
1555 *centrally managed and configured by the Defense Information Systems Agency to provide dedicated*
1556 *point-topoint, switched voice and data, imagery, and video teleconferencing services for all*
1557 *Department of Defense activities. Also called DISN. (JP 6-0)”*

1558 **DoD Information Network (DoDIN):** As defined in JP 1-02, *“The set of information capabilities, and*
1559 *associated processes for collecting, processing, storing, disseminating, and managing*
1560 *information on-demand to warfighters, policy makers, and support personnel, whether*
1561 *interconnected or stand-alone, including owned and leased communications and*
1562 *computing systems and services, software (including applications), data, security services,*
1563 *other associated services, and national security systems. Also called DODIN. (JP 6-0)”*

1564 **Event:** As defined in CNSSI-4009, *“Any observable occurrence in a system and/or network. Events*
1565 *sometimes provide indication that an incident is occurring.”*

1566 **Gateway:** As defined in CNSSI-4009, *“Interface providing compatibility between networks by*
1567 *converting transmission speeds, protocols, codes, or security measures.”*

1568 **Incident:** An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or
1569 availability of an information system; or the information the system processes, stores, or transmits; or that
1570 constitutes a violation or imminent threat of violation of security policies, security procedures, or
1571 acceptable use policies.

1572 **Infrastructure as a Service (IaaS):** As defined in NIST SP 800-145, *“The capability provided to the*
1573 *consumer is to provision processing, storage, networks, and other fundamental computing resources*
1574 *where the consumer is able to deploy and run arbitrary software, which can include operating systems*
1575 *and applications. The consumer does not manage or control the underlying cloud infrastructure but has*

UNCLASSIFIED

1576 *control over operating systems, storage, and deployed applications; and possibly limited control of select*
1577 *networking components (e.g., host firewalls).”*

1578 **Joint Authorization Board (JAB):** The primary governance and decision-making body for the
1579 FedRAMP program.

1580 **Malware:** From Evaluator Scoring Metrics, *“Malware refers to a program that is covertly inserted into*
1581 *another program with the intent to destroy data, run destructive or intrusive programs, or otherwise*
1582 *compromise the confidentiality, integrity, and/or availability of the victim’s data, application, or*
1583 *information system. Malware is the most common external threat to most hosts, causing widespread*
1584 *damage and disruption and necessitating extensive recovery efforts within most organizations.”*

1585 **Mission Computer Network Defense (MCND):** The CNDSP for a Mission Owner; the Mission Owner
1586 aligns to an MCND. The MCND defends the Mission Owner’s resources (e.g. virtual systems,
1587 applications, data, etc.) hosted on CSOs.

1588 **Mission Owner:** A DoD Cloud Consumer. As defined in NIST SP 500-292, *“A cloud consumer*
1589 *represents a person or organization that maintains a business relationship with, and uses the service from*
1590 *a cloud provider.”* Acquires cloud services from the CSP; owner of the Cloud-hosted M

1591 **Penetration Testing:** As defined in CNSSI-4009, *“A test methodology in which assessors, typically*
1592 *working under specific constraints, attempt to circumvent or defeat the security features of an information*
1593 *system.”*

1594 **Platform as a Service (PaaS):** As defined in NIST SP 800-145, *“The capability provided to the*
1595 *consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created*
1596 *using programming languages, libraries, services, and tools supported by the provider. The consumer*
1597 *does not manage or control the underlying cloud infrastructure including network, servers, operating*
1598 *systems, or storage, but has control over the deployed applications and possibly configuration settings for*
1599 *the application-hosting environment.”*

1600 **Private Cloud:** Cloud in which services are provided for the exclusive use of the DoD; supporting
1601 multiple DoD tenants or DoD sponsored tenants in the same cloud. The DoD maintains ultimate authority
1602 over the usage of the cloud services, and any non-DoD use of services must be authorized and sponsored
1603 through the DoD. Resources providing the cloud services must be dedicated to DoD use and have
1604 physical separation from resources not dedicated to DoD use.

1605 **Red Team:** As defined in CNSSI-4009, *“A group of people authorized and organized to emulate a*
1606 *potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red*
1607 *Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of*
1608 *successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an*
1609 *operational environment.”*

1610 **Scanning:** As defined in CNSSI-4009, *“Sending packets or requests to another system to gain*
1611 *information to be used in a subsequent attack.”*

1612 **Secure State:** As defined in CNSSI-4009, *“Condition in which no subject can access any object in an*
1613 *unauthorized manner.”*

1614 **Software as a Service (SaaS):** As defined in NIST SP 800-145, *“The capability provided to the*
1615 *consumer is to use the provider’s applications running on a cloud infrastructure. The applications are*
1616 *accessible from various client devices through either a thin client interface, such as a web browser (e.g.,*
1617 *web-based email), or a program interface. The consumer does not manage or control the underlying*
1618 *cloud infrastructure including network, servers, operating systems, storage, or even individual*
1619 *application capabilities, with the possible exception of limited user-specific application configuration*
1620 *settings.”*

1621 **Spillage or Data Spill:** an unauthorized transfer of classified information or Controlled Unclassified
1622 Information to an information system that is not accredited for the applicable security level of the data or
1623 information.

1624 **Threat:** As defined in CNSSI-4009, *“Any circumstance or event with the potential to adversely impact*
1625 *organizational operations (including mission, functions, image, or reputation), organizational assets,*
1626 *individuals, other organizations, or the Nation through an information system via unauthorized access,*
1627 *destruction, disclosure, modification of information, and/or denial of service.”*

1628 **Virtual Private Network (VPN):** As defined in CNSSI-4009, *“Protected information system link*
1629 *utilizing tunneling, security controls (see Information Assurance), and endpoint address translation*
1630 *giving the impression of a dedicated line.”*

1631 **Vulnerability:** As defined in CNSSI-4009, *“Weakness in an information system, system security*
1632 *procedures, internal controls, or implementation that could be exploited by a threat source.”*

1633 **Vulnerability Assessment:** As defined in CNSSI-4009, *“Systematic examination of an information*
1634 *system or product to determine the adequacy of security measures, identify security deficiencies, provide*
1635 *data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of*
1636 *such measures after implementation.”*