CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6 CJCSM 3150.07E
DISTRIBUTION: A, B, C, JEL, S 8 November 2013

JOINT REPORTING STRUCTURE FOR CYBERSPACE OPERATIONS STATUS

References:

a. Joint Publication (JP) 3-12, "Cyberspace Operations," 5 February 2013

b. DoD Directive 5100.1, "Functions of the Department of Defense and Its Major Components," 21 December 2010

c. DoD Manual 8910.01M, June 1998, "Department of Defense Procedures for Management of Information Requirements"

Other Supplemental Resources

1. DoD Directive O-5100.30, "Department of Defense (DoD) Command and Control (C2)," 5 January 2006
2. CJCSM 3150.01 Series, "Joint Reporting Structure General Instructions," 22 March 2013
3. Title 10, United States Code

1. Purpose. This manual identifies requirements to provide the Joint Staff, Combatant Commands, Military Services, and Defense Agencies (CC/S/As) with situational awareness of current operational activities in the cyberspace domain to include cyberspace domain status and health therein, and other emergent cyber-related events that affect the Department of Defense's (DoD) ability to build, defend, and operate in and through cyberspace.

2. Superseded/Cancellation. CJCSM 3150.07D, 30 June 2011, is hereby superseded.

3. Applicability. This manual applies to CC/S/As and the Joint Staff.

4. Policy. The Joint Staff and CC/S/As depend on cyberspace to assimilate information, exercise authority, and direct forces over a large geographical area and under a wide range of conditions. The Cyberspace Operations Daily Report (CODR) provides operational impact summary information on theater and

global cyberspace events that have an impact on major users' service requirements. The CODR is published on the United States Cyber Command (USCYBERCOM) portal at the SECRET level. See Enclosure A for general guidance on CODR submission.

5. Procedures. See Enclosure A.

6. Summary of Changes. This manual presents terminology, best practices, and changes updated during the last year. All changes are in accordance with information approved in reference a.

7. Releasability. This manual is approved for public release; distribution is unlimited. DoD Components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this manual through the Internet from the Chairman Joint Chiefs of Staff Directives Home Page--http://www.dtic.mil/cjcs_directives. Joint Staff activities may also access or obtain copies of this manual from the SIPRNET Directives Electronic Library.

8. Effective Date. This manual is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

Dave Goldfein

DAVID L. GOLDFEIN, Lt Gen, USAF
Director, Joint Staff

Enclosures:

A – Cyberspace Operations Daily Report (CODR)
GL – Glossary

DISTRIBUTION

Distribution A, B, C, and JEL plus the following:

	Copies
DoD Office of the Chief Information Officer	1
Commander, U.S. Cyber Command (USCYBERCOM)	2
U.S. Forces Japan	2
U.S. Forces Korea	2

(INTENTIONALLY BLANK)

ENCLOSURE A

CYBERSPACE OPERATIONS DAILY REPORT (CODR)

1. Purpose. Provide the Joint Staff, CC/S/As with situational awareness of current operational activities, the status and health of the DoD information Network (DoDIN), and other emergent cyberspace-related events that affect the DoD's ability to build, defend, and operate in and through cyberspace.

2. Posted By. USCYBERCOM Joint Operations Center (JOC) will develop and maintain a dynamically updated posting of the CODR to the USCYBERCOM SIPRNET portal page, located on the USCYBERCOM Dashboard at:
https://www.cybercom.smil.mil/dashboard/default.aspx.
A CODR tab under the Daily Briefs and Report section will be created. The CODR can also be found at
http://intelshare.intelink.sgov.gov/sites/uscybercom/joc/pages/CODR.aspx.

3. When Posted. The CODR is dynamically updated on the CYBERCOM portal, and will contain activity noted in the preceding 24-hour period. During exercises, crises, or war, reports will be posted as directed by the Joint Staff. Time sensitive material such as a Commander's Critical Information Requirement (CCIR) updates should be posted as soon as possible to increase situational awareness throughout the force.

4. Submission

a. Classification. The CODR will be classified according to content. The CODR should be written at SECRET level to enable maximum distribution. The CODR will be written for release to allies and coalition partners when possible and each item within the CODR will be properly marked with the correct classification caveat in accordance with reference b. Developing the report in this manner will allow CC/S/As to develop similar products for dissemination to coalition partners and allies. In instances that content needs to be classified at a higher level, a TOP SECRET addendum to the CODR should be produced and hosted on a USCYBERCOM Joint Worldwide Intelligence Communications System (JWICS) site. Instructions on how to access this site should be included in the CODR.

b. Method of Transmission. The report will be hosted on the USCYBERCOM SIPRNET Dashboard/Webpage. If the USCYBERCOM Web server is non-operational, the report will be sent via alternate methods to the Joint Staff National Joint Operations and Intelligence Center, Military Services, Combatant Command (CCMD) Joint Cyber Centers (JCCs) or Theater DoDIN Operations Control Centers, Global DoDIN Operations Control Centers, National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center, DoD Cyber Crime Center (DC3), Department of Homeland Security (DHS)/Department of Justice National Criminal Intelligence Resource Center, DHS National Cyber Security and Communications Integration Center, and other addressees who have identified a requirement for the report.

5. Reports Requirements. Reports required by this manual are exempt from review and approval procedures in accordance with paragraph C4.4. of reference c.

6. Specific Reporting Instructions. The CODR is a narrative report, as defined in paragraph 7 which is posted to the CYBERCOM portal. The CODR is a comprehensive report covering the operational impact of the DoDIN or shared allied networks, systems, and sensor outages; vulnerabilities and alerts; cyberspace-related orders issued by USSTRATCOM and USCYBERCOM, Defensive Cyberspace Operations (DCO) Internal Defense Measures (IDM) and Response Actions (RA), and foreign cyber threat activity derived from intelligence reporting. To ensure standard reporting by CC/S/As, USCYBERCOM will establish reporting requirements for CC/S/As to allow the CODR to serve as the single report format to cover all DoDIN and cyberspace issues. If an event is reported that contains pertinent information imposing serious threat or degradation of cyberspace operations or cyberspace operations supporting other operations, reporting process will follow normal operational report (OPREP) procedures. Additional details and status updates will be provided in the daily CODR.

7. Report Content

a. Part I, Significant Events. This section provides a high-level overview of significant cyberspace events of interest to top-level leadership that have a major impact on theater and global operations (e.g., Vol VI Cyberspace Conferences). This section provides a status of any operationally significant cyberspace events as determined by CC/S/As that relate to vulnerabilities and threats and their operational impact to DoDIN or shared allied networks. Typically, this section will reflect USCYBERCOM CCIRs. Cyberspace threats and vulnerabilities reported may include but are not limited to:

(1) Incident of successful installation or rapidly spreading malware across networks.

(2) Confirmation or suspicion of any Denial of Service or Offensive Cyberspace Operations against the DoDIN impacting operations, mission essential, or mission critical systems.

(3) Confirmation of significant unmitigated vulnerability (e.g., Command Cyber Readiness Inspection (CCRI) finding, zero-day exploit, etc.) that poses a threat to the DoDIN.

(4) Any suspected or confirmed compromise of a classified network compromise or cross-domain violations.

(5) Confirmed root level access on Mission Assurance Category (MAC) I or MAC II systems, Tier I or Tier II Task Critical Asset systems, public key infrastructure (PKI) compromise, and/or Electronic Key Management System or EKMS.

(6) Any incidents that result in a significant data integrity compromise or exfiltration of DoD or shared allied network data.

(7) Any intrusion detection system/intrusion prevention system degradation at the Internet access point (IAP)/enterprise level.

(8) Any successful exploitation involving beaconing, data compromise or exfiltration, as well as any other significant event related to named intrusion sets.

(9) Any new intelligence or information on adversary activities that may lead to a compromise or disruption of the DoDIN or a DoDIN-enabled network service.

(10) Any exploitation involving the use of compromised credentials (i.e., public key infrastructure (PKI)).

b. Part II, Outages. This section provides an accounting of any unscheduled outages that significantly degrade the CC/S/A's capability to perform a mission or provide a service. These outages include, but are not limited to:

(1) Any outage of a C4 capability with operational impact or significant operational degradation as determined by CC/S/A.

(2) Any network outage lasting longer than 4 hours that isolates a fixed or expeditionary base, camp, post, station, or CCMD headquarters, including but not limited to:

(a) Data Networks (e.g., NIPRNET, SIPRNET, JWICS, Coalition).

(b) Voice Networks (e.g., DSN, DRSN, VOSIP, SVOIP, VOIP).

(c) SATCOM (e.g., Commercial Satellite, MILSAT, MCSAT).

(d) Video Networks (e.g., UAV, GBS).

(3) CC/S/As or DoD-level loss of service or application with an enterprise or regional effect lasting greater than 4 hours, including but not limited to:

(a) Any Top-10 Defense Information System Agency (DISA) Defense Enterprise Computing Center-hosted application as determined by DISA Computing Services Directorate.

(b) Any Top-10 Service Portal (e.g., Army Knowledge Online or AKO, Defense Knowledge Online (DKO), etc.) mission application.

(c) Any IAP boundary protection or enterprise sensor outage.

c. Part III, Authorized Service Interruptions (ASIs). This section provides a list of all scheduled ASIs for the next 7 days that could significantly degrade the DoD's capability to perform a mission or provide a mission essential service.

d. Part IV, Information Control (INFOCON) Level. This section provides the current global INFOCON level and the status of any CC/S/A operating at a higher INFOCON level than the global level.

e. Part V, Orders. This section provides a list of appropriate orders OPORDs, FRAGOs, PLANORDs, and WARNORDs released in the last 7 days or expected to be released within the next 96 hours.

f. Part VI, Command Cyber Readiness Inspections (CCRIs). This section provides a list of all CCRIs scheduled to begin within the next 14 days and the results of all CCRIs completed within the past 7 days.

g. Part VII, Vulnerability Alerts and Messages. This section provides an overview of USCYBERCOM-released messages and alerts that address large-scale vulnerabilities including:

(1) A summary of threat and operational impacts addressed in any Priority Level I DoDIN Operations Task Message (DOTM).

(2) Any released Information Assurance Vulnerability Alerts (IAVAs) and Information Assurance Vulnerability Bulletins (IAVBs) that present technical or operational challenges and result in a CC/S/As submitting a plan of action and milestones with an anticipated delay of greater than 90 days for achieving compliance.

(3) Any released Information Assurance Vulnerability Alert (IAVA) or Information Assurance Vulnerability Bulletin (IAVB) that addresses serious security findings that continued operation of the NIPRNET/SIPRNET would pose a significant risk to ongoing operations and missions supported by the DoDIN.

h. Part VIII, Named Intrusion Intelligence. This section will provide significant intelligence updates that have occurred in the past week on any of the Named Intrusion Sets determined by the Threat Mitigation Framework process and identified on the "Dynamic Network Defense Operations (DNDO) Priorities List" Page located at: http://www.intelink.sgov.gov/wiki/USCYBERCOM_DNDO_Priorities_List.

8. Sample Report. See Appendix A to this Enclosure.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE A

CONTENT FOR CYBERSPACE OPERATIONS DAILY REPORT (CODR)

I. Significant Events (Paragraph 7.a. refers)

II. Outages (Paragraph 7.b. refers)

a. Description, Location, and Cause of Outage

b. Date and Time of Outage

c. Operational Impact of Outage

d. Fix Action or Next Actions

III. Authorized Service Interruptions (ASIs) (Paragraph 7.c. refers)

a. Description and Location of ASI

b. Date and time of ASI

c. Operational Impact of ASI

IV. INFOCON Level (Paragraph 7.d. refers)

a. Global INFOCON level

b. CC/S/A INFOCON level if different than Global level

V. USCYBERCOM Orders (Paragraph 7.e. refers)

a. Product Released

b. Title of USCYBERCOM Order

c. Date of Release or Expected Date of Release

VI. Command Cyber Readiness Inspections (CCRIs) (Paragraph 7.f. refers)

a. Organization and Location of CCRI

b. Dates of CCRI

c. Results of CCRI if Applicable

VII. Vulnerability Alerts and Messages (Paragraph 7.g. refers)

a. Product Released

b. Title of IAVA/IAVB/DOTM

c. Date released

d. Date of required compliance (if applicable)

e. STIG Finding Severity Level (if applicable)

VIII. Named Intrusion Intelligence (Paragraph 7.h. refers)

a. Named Intrusion

b. One to two sentence historical background on Intrusion/Operation

c. Current Intel Update

d. Operational Impact of new Intel

GLOSSARY

AKO	Army Knowledge Online
ASI	authorized service interruption
C4	command, control, communications, and computers
CCIR	Commander's Critical Information Requirement
CCRI	Command Cyber Readiness Inspection
CCMD	Combatant Command
CC/S/A	Combatant Commands/Services/Defense Agencies
CJCS	Chairman Joint Chief of Staff
CODR	Cyberspace Operations Daily Report
CSS	Central Security Service
DC3	DoD Cyber Crime Center
DCO-IDM	Defensive Cyberspace Operations-Internal Defense Measures
DCO-RA	Defensive Cyberspace Operations-Response Actions
DTM	DoDIN Ops Task Message
DHS	Department of Homeland Security
DISA	Defense Information System Agency
DKO	Defense Knowledge Online
DNDO	Dynamic Network Defense Operations
DoD	Department of DefenseDoDIN Department of Defense
Information NetworksDOTM	DoDIN Operations Task Message
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
EKMS	Electronic Key Management System
FRAGO	Fragmentary Order
GBS	Global Broadcast Service
IAP	Internet access point
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
INFOCON	Information Control
JCC	Joint Cyber Center
JOC	Joint Operations Center
JWICS	Joint Worldwide Intelligence Communications System
MAC	Mission Assurance Category
MCSAT	Multichannel Satellite
MILSAT	Military Satellite

NIPRNET	Non-classified Internet Protocol Router Network
NSA	National Security Agency
OPORD	operations order
OPREP	Operational Report
PKI	public key infrastructure
PLANORD	planning order
SATCOM	Satellite Communications
SIPRNET	Secret Internet Protocol Router Network
STE	Secure telephone equipment
STIG	Security Technical Implementation Guide
SVOIP	Secure Voice over Internet Protocol
UAV	Unmanned Aerial Vehicles
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
VOIP	Voice over Internet Protocol
VOSIP	Voice over Secure Internet Protocol
WARNORD	warning order