

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3
DISTRIBUTION: A, B, C

CJCSI 3155.01B
8 January 2016

GLOBAL COMMAND AND CONTROL SYSTEM-JOINT (GCCS-J) OPERATIONAL FRAMEWORK POLICY

References: See Enclosure C.

1. Purpose. This instruction provides the framework necessary to ensure the Global Command and Control System-Joint (GCCS-J) meets operational requirements in support of the National Military Command System (NMCS).
2. Canceled/Superseded. Chairman of the Joint Chiefs of Staff (CJCSI) 3155.01A, 15 August 2013, "Global Command and Control System-Joint (GCCS-J) Operational Framework Policy," is hereby superseded.
3. Applicability. This instruction applies to the Combatant Commands, Services, Defense Agencies, Joint Staff, and all GCCS-J users.
4. Policy
 - a. GCCS-J is the Department of Defense (DoD) system of record for situation awareness supporting command and control (C2) for joint operations. It enables and facilitates the military decision-making process (references a, b, and c). The information that GCCS-J provides should be accurate, relevant, essential, timely, and available.
 - b. The GCCS-J operational environment includes automatic data processing hardware and software, communications hardware and software, applicable portions of the Defense Information Systems Network, and support activities at various sites. These GCCS-J sites shall adhere to GCCS-J operational requirements for system availability (Enclosure A) and GCCS-J management functions (Enclosure B) to provide the required operational readiness.

5. Definitions

a. GCCS-J. A worldwide system that provides the Department of Defense, Joint Staff, Combatant Commands, Services, Defense Agencies, Joint Task Forces and their Service Components, and others with information processing and dissemination capabilities necessary to support global/joint C2.

b. Critical Site. A GCCS-J site that provides information, data feeds, or other services critical to global/joint C2 operations in support of the NMCS and validated by Joint Staff J-33. Critical sites must maintain an operational availability of greater than or equal to 99.8 percent with a mean time between failures of 1,000 hours. These sites must also provide continuity of operations (COOP) capability. Critical sites require 24/7 monitoring. In the event of an unscheduled outage, critical sites must follow specific reporting instructions and reestablish operational availability within 2 hours of discovery of the outage.

c. Operational Availability. Operational availability is the ability of a site to perform mission-essential GCCS-J tasks or functions.


6. Responsibilities. Local commanders of GCCS-J sites are responsible for management and operation of the GCCS-J at their respective sites. Furthermore, in accordance with Reference e (Enclosure C of this instruction), Combatant Command Support Agents are responsible for any resource requirements to maintain critical site status, including the purchase of associated hardware.

7. Summary of Changes. This document replaces CJCSI 3155.01A, 15 August 2013, and includes changes reflecting administrative updates, additions, and corrections for clarity.

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET. DoD Components (including the Combatant Commands), other Federal Agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at: <http://www.dtic.mil/cjcs_directives/>. Joint Staff activities may also obtain access via the SIPRNET Directives Electronic Library Web sites.

9. Effective Date. This INSTRUCTION is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:


WILLIAM C. MAYVILLE, JR.
LTG, USA
Director, Joint Staff

Enclosures:

- A—GCCS-J Operational Requirements for System Availability
- B—GCCS-J Operational Management Functions
- C—References
- GL—Glossary

(INTENTIONALLY BLANK)

ENCLOSURE A

GCCS-J OPERATIONAL REQUIREMENTS FOR SYSTEM AVAILABILITY

1. Critical Sites

a. Within GCCS-J, certain information resources at key sites are defined as critical to global/joint C2 operations. These sites must maintain an operational availability of 99.8 percent or better with a mean time between failures of 1,000 hours and must provide COOP capability. Operational availability is a system's ability to perform mission-essential functions during operational use. It is measured as uptime/(uptime + unscheduled outages), with a failure defined as an unscheduled outage. Furthermore, in the event of an unscheduled outage, critical sites must follow reporting instructions outlined in Enclosure B and reestablish operational availability within 2 hours of discovery. As a MAC I system, GCCS-J sites require 24/7 monitoring and other resiliency requirements as discussed in references c and f. If a critical site is unable to provide this level of support, it must consent to 24/7 monitoring by the Joint Operations Support Center (JOSC). Current critical sites are identified below:

- (1) National Military Command Center (NMCC).
- (2) Alternate NMCC (Site R).
- (3) Mission Management Center (MMC).
- (4) Combatant Command headquarters (HQ).
- (5) Service Component and Functional Component HQ of Combatant Commands.
- (6) Service HQ.
- (7) Sub-unified Joint Commands, standing Joint Task Force HQ, and Joint Special Operations Task Force HQ.
- (8) Other special interest critical sites validated by the Joint Staff J-33, Nuclear and National Command, Control, and Communications (N2C3) Division.

b. To meet the operational availability requirement, critical sites will endeavor to achieve:

- (1) Fully redundant critical circuits.

(2) Uninterrupted power supply for all critical components comprising an end-to-end system.

(3) Global status monitoring on site identified critical infrastructure components.

(4) Elimination of single points of failure.

(5) Adequate staffing, training, and maintenance support.

c. Scheduled outages shall be conducted in accordance with the procedures specified in Enclosure B.

d. The GCCS-J Program Management Office (PMO) will be available to provide installation assistance to critical sites. The U.S. Marine Corps GCCS-J delta training program will provide functional training for new capabilities and version updates, as required and validated by the Global Command and Control Training Working Group. The GCCS-J PMO will provide critical sites with technical training assistance in conjunction with initial fielding.

e. The GCCS-J PMO will maintain a list of the minimum applications and their versions that critical sites require for full functionality within GCCS-J (e.g., browsers and versions, Java and versions, Microsoft Office Suite and version). Changes will be identified in sufficient time for critical sites to be updated prior to deployment of a new capability.

f. Failure to comply with guidance in this instruction will result in a loss of critical site status and associated support, as will any site that declines critical site status. Once downgraded, a site will be required to establish a service-level agreement with the Defense Information Systems Agency (DISA) for future support.

g. Joint Staff J-33 will provide a list of critical sites to DISA annually and provide interim updates as required.

2. Noncritical Sites. All other sites have an operational availability requirement of the same level or better than SIPRNET availability established by their site. To ensure operational availability, sites must provide adequate engineering, staffing, training, and maintenance support. Backup power must be available for extended primary power outages.

3. Joint Staff Support Center (JSSC). JSSC is responsible for disseminating additional time-sensitive operational guidance on behalf of Joint Staff J-33 to GCCS-J sites. Sites should follow this guidance to maintain operational availability.

ENCLOSURE B

GCCS-J OPERATIONAL MANAGEMENT FUNCTIONS

1. General Reporting Procedures. This section defines the GCCS-J critical sites' recurring requirements for providing reports to the Joint Staff. The Joint Operations Support Center (JOSC) is responsible for receiving, compiling, and forwarding the reports to designated Joint Staff elements. Contact JOSC using one of the following methods:

- Telephone: 703-695-0671 (DSN: 225-0671).
- SIPRNET e-mail: disa.pentagon.JSSC.mbx.josc@mail.smil.mil.
- SIPRNET Web site: <http://www.gmc.nmcc.smil.mil/hd/index.html>.

The format and information required for each report are described below.

a. Scheduled Outages

(1) Critical sites shall notify the JOSC (Pentagon) of all scheduled outages at least 48 hours in advance. Outages under 6 hours can be approved by JOSC personnel. Outages in excess of 6 hours require approval by the Joint Staff J-33 N2C3 Division (operational agent for GCCS-J) and notification of the Chief, Combat Capability Development Division, within the Joint Staff J-6 Deputy Directorate for Command and Control, Communications, Computers, and Cyber (DDC5I). Once an outage has been approved, the JOSC will enter the data into the trouble ticketing system as a planned outage, where it can be tracked in the database. Planned outages scheduled less than 48 hours in advance will be reported to the JOSC help desk by telephone, newsgroup, or e-mail. For statistical purposes, these short-notice outages may be considered unscheduled outages. The GCCS-J Site Coordinator (GSC) shall provide the following information when requesting an outage:

- (a) GCCS-J site name.
- (b) Start date and time of the outage in Zulu time.
- (c) Stop date and time of the outage in Zulu time (or best estimate).
- (d) Brief explanation of the outage.
- (e) Point of contact (name and telephone number).

(2) Regularly scheduled outages such as backups, training, and preventive maintenance can be sent on a monthly basis, but no more than 30 days in advance. Specific dates, times, and explanations must be provided for each event.

b. Unscheduled Outages. GCCS-J critical sites shall report all GCCS-J outages and problems to the JOSC. GCCS-J outages are considered the loss of hardware, software, or connectivity capabilities that degrade, impair, or sever a site's ability to perform its C2 mission. The sites will attempt to notify the JOSC of all unscheduled outages within 10 minutes of the problem occurring. If the site was not manned at the initial time of outage occurrence, the JOSC will be immediately notified on discovery of an outage. In many cases, the system and network management tools will alert the JOSC of major problems through the smart agents. These problems will be captured by software that is fed from the smart agents. If the JOSC has not received communication from the site when a major problem occurs, it will start calling the site after 10 minutes. For that reason, each critical site must provide the JOSC with up-to-date 24-hour contact information including the telephone number, e-mail address, and whether contact(s) are on-site or on call. Status information must be reported to the JOSC at least hourly and as significant changes in status occur until the problem is resolved. The GSC should provide the following information via secure e-mail, newsgroup, or secure telephone equipment when reporting an outage:

- (1) Reason for Outage. Explanation of the problem.
- (2) Status of Actions. Explanation of actions being taken to resolve the problem.
- (3) Estimated Time for Repair. Best estimate of how long it will take to fix the problem.
- (4) Corrective Action. Final closeout status report with corrective actions and restoral time.

c. Software Cutover Report. This report will be used by the GCCS-J critical sites to report the installation of software releases or segment upgrades to the JOSC. The JOSC will notify the GSC(s) when updated versions of software are available for the GCCS-J suite of software. The JOSC will give instructions for downloading, installation, and verification testing of the new software. A timetable will be given specifying when all actions should be completed. This cutover report will provide the necessary feedback to the JOSC to ensure sites have complied with the instruction. The following information will be provided via telephone or e-mail to the JOSC when reporting an update to a site's software configuration:

(1) Software Installed. Software release version.

(2) Time Installed. Date and Zulu time the software was installed in the operational system.

(3) Problems With Installation. Any problems encountered with installing the change.

d. Attainment of Priority Mode Operations. Priority mode represents a higher state of readiness and is used to provide maximum support to the operational mission. The JOSC will ensure that all GCCS-J sites are notified and proper system and network procedures are implemented when the GCCS-J is placed in priority mode. This report will be used by the GCCS-J sites to notify the JOSC that their facility has attained the specified priority. The JOSC will be notified via telephone or e-mail for this report. If the notification is via telephone, the site's GSC must follow up with an e-mail within 24 hours. If communications are down, the JOSC will be notified within 4 hours of the time e-mail connectivity is restored. Provide the following information to the JOSC when reporting compliance with priority mode operations:

(1) Date and Zulu Time of Attainment. Provide the date and Zulu time that the GCCS-J site attained the proper mode in accordance with this document.

(2) Degraded Operations. List any site GCCS-J system or network problems that exist at the time of the attainment. Degraded conditions must be reported to the JOSC in this subparagraph.

(3) Telephone Numbers. Provide special telephone numbers for the GSC if the site requests the JOSC to call a special number instead of the telephone number normally used at the site.

e. Classification of Reporting Data. Classify outage and performance data for GCCS-J in accordance with the GCCS-J security policy (reference c).

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

- a. DoD Directive (DoDD) 3700.01, 22 October 2014, “Department of Defense (DoD) Command and Control (C2)”
- b. CJCSI 3265.01 series, “Command and Control Governance and Management”
- c. CJCSI 6731.01 series, “Global Command and Control System Security Policy”
- d. CJCSI 3151.01 series, “Global Command and Control System Common Operational Picture Reporting Requirements”
- e. DoDD 5100.03, 9 February 2011, “Support of the Headquarters of Combatant and Subordinate Unified Commands”
- f. DoD Instruction 8500.01, 14 March 2014, “Cybersecurity”

(INTENTIONALLY BLANK)

GLOSSARY

ABBREVIATIONS AND ACRONYMS

CCMD	Combatant Command
DDC5I	Deputy Directorate for Command and Control, Communications, Computers, and Cyber
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense directive
C2	command and control
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
COOP	continuity of operations
GCCS-J	Global Command and Control System-Joint
GSC	GCCS-J Site Coordinator
HQ	headquarters
JOSC	Joint Operations Support Center
JSSC	Joint Staff Support Center
MMC	Mission Management Center
N2C3 Division	Nuclear and National Command, Control, and Communications Division
NMCC	National Military Command Center
PMO	Program Management Office

(INTENTIONALLY BLANK)