CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3
DISTRIBUTION: A, B, C,

CJCSI 3155.01C
24 January 2024

OPERATING POLICY: GLOBAL COMMAND AND CONTROL SYSTEM-JOINT

References:
See Enclosure C.

1. Purpose. This instruction establishes policy and assigns responsibilities for operating and managing the Department of Defense (DoD) system of record for situational awareness (SA), Global Command and Control (C2) System-Joint (GCCS-J). It ensures GCCS-J, along with its global architecture, supporting technologies, and skilled workforce, provides a relevant, comprehensive, timely, and accurate global common operational picture (COP) to meet operational requirements supporting the National Military Command System (NMCS).

2. Superseded/Cancellation. Chairman of the Joint Chiefs of Staff (CJCS) Instruction (CJCSI) 3155.01B, 8 January 2016, "Global Command and Control System-Joint (GCCS-J) Operational Framework Policy" is hereby superseded.

3. Applicability. This instruction applies to the Joint Staff, Services, Combatant Commands (CCMDs), Defense Agencies, and all DoD Components that employ GCCS-J.

4. Policy

a. This instruction fulfills the below CJCS responsibilities established in references (a) through (d).

(1) Establishes operational requirements for C2 capabilities, systems, services, and solution suitability to meet operational expectations.

(2) Defines DoD C2-enabling capabilities required to support the full range of military operations, and integrates these capabilities, data strategies and standards, architectures, operational concepts, and mission partner operations.

(3) Ensures NMCS elements meet Presidential and Secretary of Defense requirements, including uninterrupted processing, display, and exchange of operational information (to include SA and operational, intelligence, and planning information) throughout the spectrum of conflict.

b. Global C2 architecture is a DoD C2-enabling capability as defined in reference (a) and is the NMCS element that encompasses the doctrine, policies, procedures, technologies (e.g., GCCS-J), and personnel (to include the National Command Authority, Joint Force Commanders, and warfighters) that enable and execute missions within the C2 joint functional area (reference (e)).

(1) GCCS-J, with its globally integrated C2 architecture, is the primary C2-enabling technology that provides a relevant, comprehensive, timely, and accurate global COP. It is supported by auxiliary systems such as GCCS-Integrated Imagery and Intelligence or other common intelligence picture tools to generate the most accurate rendering of the operating environment. GCCS-J also incorporates emerging technologies such as SA Service-Enhanced, also known as Ground to Air SA.

(2) The integrity and consistency of COP data throughout the operational environment is essential for effective C2. Thus, consumption of GCCS-J COP data by external systems requires coordination and discipline. It is critical that external systems and applications that consume COP data from GCCS-J coordinate development of new interfaces, such as bi-directional data flow, with the Joint Staff Deputy Directorate for Nuclear and Homeland Defense Operations (J-36) and the Defense Information Systems Agency (DISA) GCCS-J Program Management Office (PMO).

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Summary of Changes. This revision incorporates security policy and assigns security responsibilities for GCCS-J and its strategic server enclaves.

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Integrated Protocol Router Network. DoD Components (including the CCMDs), other Federal Agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at: <https://www.jcs.mil/library/>. Joint Staff activities may also obtain access via the Secret Internet Protocol Router Network (SIPRNET) Directives Electronic Library website.

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

For the Chairman of the Joint Chiefs of Staff:

Michael L Downs

MICHAEL L. DOWNS, Maj Gen, USAF
Vice Director, Joint Staff

Enclosures:
A – Global Command and Control System-Joint System Operations
B – Responsibilities
C – References

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE A

GLOBAL COMMAND AND CONTROL SYSTEM-JOINT SYSTEM OPERATIONS

1. Purpose. GCCS-J is the DoD system of record for joint C2 and is a worldwide system that provides the Joint Staff, CCMDs, Services, Defense Agencies, Joint Task Forces and their Service Components, and other DoD Components with information processing and dissemination capabilities necessary to execute operations. GCCS-J is the authoritative data source for numerous fielded capabilities and emerging technologies. Its proper operation, management, and security is essential to C2 at all echelons and across the competition continuum.

2. Operations

a. Global Command and Control System-Joint Critical Sites. Critical sites are those that provide information, data feeds, or other services critical to C2 operations in support of the NMCS and are so designated by the Joint Staff J-36/National and Nuclear C2 and Communications (N2C3) Division. Critical sites must meet requirements for operational availability (A_O), continuity of operations (COOP), and outage restoration as established in Appendix A to Enclosure A. Critical sites include:

(1) National Military Command Center (NMCC)

(2) Alternate NMCC (Site R)

(3) U.S. Strategic Command (USSTRATCOM) headquarters (HQ)

(4) Mission Management Center

(5) CCMD HQs

(6) Sub-unified Joint Commands, standing Joint Task Force HQ, Joint Special Operations Task Force HQ, and Service and functional Component HQ of CCMDs.

(7) Joint Deployment Training Center

(8) Other special interest sites as designated by the Joint Staff J-36.

b. Management. The Global COP was developed to support global C2 and inform and add value to Commanders and decision makers at all levels by providing common global SA across all domains and shared users. When a critical site's ability to provide data is hampered in any way, the resultant cascading impacts can significantly influence operations at all levels globally. It is imperative to report outages, increased latency, or reduced throughput. GCCS-J operational management functions and guidance are contained in Appendix B to Enclosure A.

c. Security. Cybersecurity across the vast and complex global architecture is critical to our warfighting capability. Security policy and guidance for GCCS-J and its strategic server enclaves are contained in Appendix A to Enclosure B.

APPENDIX A TO ENCLOSURE A

CRITICAL SITE DEPENDABILITY

1. Purpose. Information system dependability includes availability, reliability, redundancy, and security. GCCS-J critical sites must be dependable to meet senior leader and warfighter requirements. This appendix addresses availability, reliability, and redundancy requirements for critical sites. Security responsibilities are addressed in Appendix A to Enclosure B.

2. Continuity of Operations. To meet criteria for critical site designation, global C2 COOP capabilities are required to support the CJCS's mission-essential function responsibilities within the NMCS in accordance with (IAW) reference (c). All GCCS-J critical sites will develop and exercise plans for COOP that include, but are not limited to, measures that sustain operations during a loss of primary electrical power, connectivity, or cooling; or active shooter emergencies.

3. Availability. Joint Staff-designated GCCS-J critical sites must maintain a rolling annual A_O rate of 99.8 percent.

a. A_O is the fraction of time that GCCS-J is required to be operational during 365 contiguous days (8760 hours/365 days), calculated as:

(1) A_O = operational hours ÷ 8760 hours x 100

(2) operational hours = 8760 hours - outage hours

b. Outages may consist of complete or partial loss of hardware, software, or connectivity; increase in latency; or sensor outages that compromise completion, timeliness, and accuracy of the Global COP. For instance, loss of tracks flowing from the common tactical picture (CTP) at the Joint Task Force level or below to the TOP COP is an outage, while use of an alternate/backup communications path to provide required data is not considered an outage.

c. Unscheduled outages contribute to total outage hours and total outages. Scheduled outages that are requested at least 48 hours in advance do not contribute toward total outage hours/outages. Scheduled outages that are requested less than 48 hours in advance may contribute to the total outage hours/outages at the discretion of the Joint Staff J-36.

4. Mean Time Between Failures. GCCS-J critical sites must maintain a rolling annual mean time between failures (MTBF) rate of at least 1,000 hours. MTBF is the average time between outages, calculated as:

MTBF = operational hours ÷ number of outages.

5. Monitoring. GCCS-J critical sites require 24/7 monitoring and other resiliency and redundancy requirements as defined in paragraph 4. The Joint Staff Support Center (JSSC) Joint Operations Support Center (JOSC) can provide monitoring services to any critical site. Critical sites that do not have adequate on-premises support for 24/7 monitoring must consent to and enable monitoring by the JOSC. Scheduled outages shall be conducted IAW the procedures specified in Appendix B to Enclosure A.

6. Non-Critical Sites. All other GCCS-J sites have an A_O requirement of the same level or better than SIPRNET availability established by their site. To ensure A_O, sites must provide adequate engineering, staffing, training, and maintenance support. Backup power must be available for extended primary power outages. Additionally, all sites must adhere to the security requirements outlined in Appendix C to Enclosure A.

APPENDIX B TO ENCLOSURE A

MANAGEMENT

1. General Reporting Procedures. This section defines GCCS-J recurring critical site requirements for providing reports to the Joint Staff. The JOSC is responsible for receiving, compiling, and forwarding reports to designated Joint Staff elements, the Global COP manager, and other offices as appropriate. GCCS-J critical sites submit reports as directed in paragraphs 2 through 5, IAW reference (f), to the JOSC at:

(1) Unclassified telephone: 703-695-0671 (Defense Switched Network (DSN): 312-225-0671).

(2) Voice Over Secure Internet Protocol telephone: 302-221-0299.

(3) SIPRNET email: <disa.pentagon.JSSC.mbx.josc@mail.smil.mil>.

(4) SIPRNET website: <https://www.gmc.nmcc.smil.mil/hd/index.html>.

2. Scheduled Outages

a. GCCS-J Site Coordinators (GSCs) request outages no more than 30 days in advance and provide:

(1) GCCS-J site name.

(2) Start date and Zulu time.

(3) Estimated stop date and Zulu time.

(4) Reason.

(5) Mitigations, such as COOP plan activation.

(6) Point of contact (POC) name and telephone number.

b. Joint Staff J-36

(1) Exercises approval authority for outages lasting 6 hours or more.

(2) Determines whether approved outages requested less than 48 hours

in advance count toward the total outage days.

c. Joint Operations Support Center

(1) Exercises approval authority for outages lasting less than 6 hours.

(2) Populates approved outages in the trouble ticketing system.

(3) Notifies NMCC and the Global COP Manager and report the outage in the Global COP Chat Room for community awareness: <https://chatsurfer.proj.nro.smil.mil/#/messages/dcs/gccs_global_cop>

3. Unscheduled Outages

a. Global Command and Control System-Joint Site Coordinators

(1) Report unscheduled outages via secure communications **within 10 minutes** of discovery and provide the following:

(a) Cause.

(b) Corrective actions in progress.

(c) Estimated time to restore operations.

(d) Corrective action taken and restoration time.

(2) Provide status updates at least once each hour, and as significant changes occur, until the outage is resolved.

(3) Provide a final report detailing which corrective actions were successful and what time service was restored.

b. In some cases, system and network management tools will alert the JOSC of major problems through smart agents. In this case, if the JOSC has not received communication from the site after 10 minutes, it will start calling the site. Additionally, Global COP Managers identify abnormalities or failures within the system and will contact the site to correct the issue. The JOSC and Global COP managers require up-to-date 24-hour contact information for each critical site (provided in the monthly report as directed in paragraph 5).

c. JOSC reports unresolved unscheduled outages within 2 hours to the NMCC watch floor and Global COP Manager, and posts to the Global COP Chat

Room for community awareness.

4. Global Command and Control System-Joint Software Upgrade/Cutover Report

a. Global Command and Control System-Joint Site Coordinators Report

(1) Estimated completion date for software update/cutover.

(2) Completion of a change, including:

(a) Software release version.

(b) Date and Zulu time of completion.

(c) Problems encountered during installation, if any.

b. GSCs update their site's Unique Identifier (UID) information in the UID registration portal on SIPRNET at: <https://disa.deps.smil.mil/sites/gccs_uid/_layouts/15/start.aspx#/>.

5. Monthly Status Report. 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 onsite or on call. Reports are due to the JOSC by the tenth day of each month. JOSC will maintain the consolidated list and share it with the Global COP manager.

(INTENTIONALLY BLANK)

ENCLOSURE B

RESPONSIBILITIES

1. Joint Staff

a. The Deputy Director, Joint Staff J-36 is delegated authority to discharge CJCS responsibilities relevant to this instruction, and will:

(1) Serve as the GCCS-J Operational Sponsor.

(2) Designate GCCS-J critical sites.

b. The Chief, Joint Staff J-36/N2C3 Division is delegated responsibility for day-to-day oversight and management of the activities in this instruction.

c. The Joint Staff J-36/Global C2 Operations Branch is the Joint Staff office of primary responsibility for this instruction, and will:

(1) Maintain a master list of GCCS-J critical sites, update this list annually or as needed, and provide copy of this list to the DISA GCCS-J PMO, JOSC, and the USSTRATCOM Global COP Manager.

(2) Assess compliance with the guidance in this instruction during COP staff assistance visits (reference (g)).

(3) Receive and process requests for external systems to consume data from GCCS-J.

2. Services

a. In support of CCMD and Service C2 requirements, Services will manage and operate GCCS-J sites IAW this instruction and reference (h).

b. IAW reference (a), provide necessary resources and support for subordinate GCCS-J sites, to include Service Component Commands, Service-resourced Joint Task Force(s), and functional Component Commands to meet the requirements of paragraphs 5 and 6 of this Enclosure and paragraph 3 of Appendix A to Enclosure B.

c. Services will adhere to the GCCS-J software version life cycle guidance issued by DISA, the GCCS-J Operational Sponsor, and the GCCS-J Authorizing Official (AO).

3. Combatant Commands

a. In support of the NMCS, Global COP, and CCMD C2 requirements, CCMDs will manage and operate GCCS-J sites IAW this instruction and reference (h).

b. CCMDs will provide oversight to ensure subordinate GCCS-J sites, i.e., Joint Task Force(s), Service and functional Component Commands meet the requirements of paragraphs 5 and 6 of this Enclosure and paragraph 3 of Appendix A to Enclosure B.

c. CCMDs will adhere to the GCCS-J software version life cycle guidance issued by DISA, the GCCS-J Operational Sponsor, and the GCCS-J AO.

4. U.S. Strategic Command. In addition to the responsibilities in paragraph 3 of this Enclosure, USSTRATCOM will:

a. Serve as the GCCS-J AO as specified in Appendix A to Enclosure B.

b. Serve as the Global COP Manager IAW references (h) and (i).

5. Defense Information Systems Agency

a. Global Command and Control System-Joint Program Management Office

(1) Provide required Joint Staff-designated critical site licenses and support subscriptions for applications in the GCCS-J baseline, to include Red Hat JBoss Enterprise Application Platform, Sybase Database, Oracle Database, ForgeRock OpenAM, and the GV3 Image/Video Viewer. Critical sites are required to provide their own licenses for operating systems (i.e., Red Hat Enterprise Linux, Windows, Windows Server) and hypervisor (i.e., VMware vSphere, Red Hat KVM, etc.).

(2) Maintain a list of the minimum hardware resources and software applications and their versions that critical sites require for full functionality within GCCS-J (e.g., servers/clients, memory, video card, operating systems, browsers, Java, Microsoft Office Suite, etc.). Changes will be identified in sufficient time for critical sites to be updated prior to deployment of new capability.

(3) Notify appropriate stakeholders when updated versions of software and security patches are available.

(4) Provide installation assistance to critical sites, to include instructions for download, installation, and verification tests of new software.

(5) Provide just-in-time training for GCCS-J System Administrators at critical sites ahead of major system releases to assist with installation. Limited on-site support is subject to the available GCCS-J PMO budget. Sites also have the option to provide funding to the GCCS-J PMO for onsite assistance.

(6) Support the Joint Staff J-36 in processing external system requests for interfaces with GCCS-J, and maintain the GCCS-J System Data Exchange Matrix, SV-6, or equivalent artifact which documents all approved and proposed interfaces with systems that consume COP data from GCCS-J.

b. Joint Staff Support Center Joint Operations Support Center

(1) Provides 24/7 GCCS-J technical expertise/helpdesk support to the global C2 system.

(2) Monitors the operating status of sites consistent with agreements with those sites.

(3) Disseminates lists of critical sites and GSCs, and time-sensitive operational guidance, on behalf of the GCCS-J Operational Sponsor.

(4) Receives, compiles, and disseminates reports, as appropriate.

(5) Tracks critical sites' software configuration .

6. All Global Command and Control System-Joint Sites

a. DoD Components that employ GCCS-J will:

(1) Be responsible for the site's management and operation IAW this instruction and reference (h).

(2) Comply with security responsibilities as specified in Appendix A to Enclosure B.

(3) Be responsible for any resource requirements, including the purchase of associated hardware and required software licenses, necessary to operate the current operationally-approved GCCS-J software versions.

(4) Comply with time-sensitive operational guidance from the GCCS-J Operational Sponsor, disseminated by the JOSC, to maintain operational availability.

b. Information sharing (GCCS-J COP data) beyond the GCCS-J Global Architecture is an important element of enhanced SA across the Joint Force. To maintain alignment with the DoD Data Strategy and ensure COP data is usable for operational effect, it is equally important to maintain accurate and up-to-date awareness of the architecture, including all interfaces to external data consumers. Organizations developing and implementing new operational interfaces with GCCS-J nodes under their purview will:

(1) Submit requests to the Joint Staff J-36, and an info copy to DISA GCCS-J PMO, for the establishment of new interfaces with GCCS-J for consumption of COP data.

(2) Requests from non-GCCS-J site organizations shall be made through a sponsoring GCCS-J Site (O-6/GS-15 from the Joint Staff Directorate for Operations (J-3)).

(3) Requests will identify the interfacing system or capability, and describe the purpose of the interface, intended connection points, access controls on the data, any planned data format transformations, and any plans to further disseminate the data. The requests will also describe the planned approach related to timeliness and periodicity of processing and visualizing this COP data, with the objective of being able to characterize any deltas from GCCS-J data or displays that might arise as a result.

7. Global Command and Control System-Joint Critical Sites. In addition to the responsibilities in paragraph 5 of this Enclosure, GCCS-J critical sites will:

a. Comply with dependability and management requirements contained in Appendices A and B to Enclosure A.

b. Designate a GSC in writing and provide contact information to the JSSC JOSC.

c. The GSC will serve as the main POC for all GCCS-J operational matters at the site and is responsible for management functions outlined in Appendix B to Enclosure A.

8. Global Command and Control System-Joint Non-Critical Sites. Non-critical sites are responsible for all software licensing and support subscriptions for applications in the GCCS-J baseline.

9. Joint Deployment Training Center. IAW reference (j), the Joint Deployment Training Center provides formal functional user training for new capabilities and version updates as required and validated by Joint C2 Training and COP working groups (WGs).

10. Air Education and Training Command. IAW reference (j), Air Education and Training Command provides formal technical user training for GCCS-J.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE B

SECURITY RESPONSIBILITIES

1. Global Command and Control System-Joint Authorizing Official

a. The CJCS appointed the Director, Joint Staff Directorate for C3 and Computers/Cyber (DJ-6) as the Principal AO for Warfighting Mission Area information technology (IT) systems.

b. The Principal AO (via DJ-6 memo, "Defense Information Systems Agency Command and Control Portfolio Capabilities Authorizing Official Appointment Letter, 5 October 2017) designated GCCS-J as a Warfighting Mission Area system and appointed USSTRATCOM as the GCCS-J AO.

(1) The AO authorizes Joint C2 systems and service connections to external systems, and ensures GCCS-J sites and users comply with security policies and controls.

(2) The AO provides the type of authorization and authority to operate (ATO) GCCS-J, authorizing GCCS-J sites to deploy and install identical system version releases.

c. The AO will:

(1) Provide continuous visibility to the receiving enclave(s) or site(s) of the system security authorization package through use of or export to the Enterprise Mission Assurance Support System or other automated tools.

(2) Provide status updates of Risk Management Framework activities and resolve any security issues that are raised.

(3) Issue an ATO for the GCCS-J version being deployed.

(4) Lead the C2 Governance and Management-directed Security WG IAW reference (d) to address cybersecurity issues for Joint C2 systems managed by DISA.

2. Information System Owner

a. DISA serves as the Information System Owner/Program Manager (PM). and develops, maintains, and tracks the security plan for GCCS-J.

b. DISA will:

(1) Develop and release security patches in response to information assurance vulnerability alerts and make them available through the Defense Asset Distribution System (DADS) for download and installation by sites.

(2) Ensure security tests and evaluations address any additional receiving Component security controls or requested adjustments to assigned security controls that are identified during Joint Staff/USSTRATCOM level security reviews.

(3) Ensure the system complies with direction under the Information Assurance Vulnerability Management Program and operational orders issued by U.S. Cyber Command.

(4) Provide installation and configuration requirements documentation, including applicable DoD Security Technical Implementation Guides, to receiving site(s) prior to system deployment. Documentation includes installation guides and procedures, cybersecurity implementation guidance, configuration management documents, and applicable DISA Security Technical Implementation Guides.

3. Global Command and Control System-Joint Sites. This section applies to all DoD Components that employ GCCS-J.

a. Each GCCS-J site:

(1) Will implement cybersecurity for DoD IT systems IAW references (f) and (k).

(2) Is responsible for ensuring installation and configuration requirements are met, to include site-specific security controls.

(3) Must maintain compliance with security updates and emerging DoD security requirements, and download and install security patches from DADS. Any deviations from DADS installation and configuration instructions must be reported to USSTRATCOM J-672 and document the deviation IAW reference (f).

(4) Will complete weekly Assured Compliance Assessment Solution scans on GCCS-J servers and all clients IAW reference (l).

(5) Maintains SA of GCCS-J assessment activities via the Enterprise Mission Assurance Support System or other automated tools.

(6) Makes the receiving enclave(s) security authorization package available if requested by USSTRATCOM or DISA.

(7) Determines the security impact of connecting GCCS-J within the receiving enclave(s).

(a) Security controls that are built into the major application will not be retested, as they do not change when the system is deployed.

(b) Inherited controls (i.e., controls that will be implemented by the receiving enclaves) must be validated by the receiving enclave and supporting documentation or artifacts must be developed.

(8) Implements any receiving site augmenting security controls required to support GCCS-J.

(9) In unusual circumstances where operational requirements demand the continued operation of sunset versions of GCCS-J:

(a) With approval of the operational sponsor and the GCCS-J AO, executes a documented agreement with DISA (e.g., memorandum of understanding/agreement, service-level agreement) for the maintenance and monitoring of the system's security posture (e.g., security controls, computer network defense service provider, etc.). The document must specify the duration of the agreement and address topics such as operating constraints, operation environment, monitoring and status reporting requirements, security maintenance, and roles and responsibilities.

(b) All costs associated with extended support are the responsibility of the site(s).

(10) Issues an authorization to connect and operate GCCS-J. This includes a statement by the site AO granting approval for GCCS-J to connect to the enclave. The AO's decision is based on the determination that the risk to the network is acceptable.

(a) Provides a copy of implementing documentation (e.g., "authorization to connect") to USSTRATCOM.

(b) Notifies and provides guidance to subordinate site(s) that GCCS-J is authorized to operate and/or connect only in the authorized configuration.

(11) Updates enclave authorization and/or connection documentation to reflect the incorporation/connection of the GCCS-J application.

(12) Ensures mitigations are maintained IAW the GCCS-J Plan of Action and Milestones.

(13) Appoints in writing the following GCCS-J Security positions, IAW reference (f):

(a) Site Authorizing Official. Mission operations may necessitate deviations from the controls outlined in the Security Technical Implementation Guide. Prior to implementing a site deviation, a site risk assessment must be conducted to determine the potential impacts to the site's security posture. The Site AO:

1. Provides senior-level oversight and accountability at the operational site level.

2. Ensures the required DoD-level security polices, as well as guidance from the GCCS-J AO at USSTRATCOM, are rapidly and effectively implemented.

3. Notifies USSTRATCOM J672 (DSN telephone 703-912-6163 or commercial telephone 402-912-6163) of the rationale and a waiver to configurate when deviations from DADS instructions are necessary

5. May approve such deviations if the risk is considered manageable and must notify the USSTRATCOM AO of the deviation and document the deviation IAW reference (f).

(b) Site Program Manager/Security Manager. The Site PM/Security Manager ensures the site's GCCS-J system is correctly configured and maintained, and applies approved GCCS-J system software updates issued from the GCCS-J PMO.

(c) Site Information System Security Manager. The site Information System Security Manager (ISSM) will:

i. Provide direction to the Information System Security Officer (ISSO) IAW reference (f).

ii. Coordinate with the organization's security manager to ensure issues affecting the organization's overall security are addressed appropriately.

(d) Site Information System Security Officer. The site ISSO will:

i. Develop, implement, and manage the site GCCS-J security policies and procedures to include security education, training, and awareness in support of the ISSM.

ii. Ensure site cybersecurity assessments are completed for GCCS-J.

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. DoDD 3700.01, 22 October 2014, “DoD Command and Control (C2) Enabling Capabilities”

b. DoDD S-3710.01, 27 May 2015 “National Leadership Command Capability (NLCC)”

c. CJCSI 3280.01E, 4 February 2022, “National Military Command System”

d. CJCSI 3265.01A, 29 November 2013, “Command and Control Governance and Management”

e. Joint Publication (JP) 1, Volume 1, 27 August 2023, “Joint Warfighting”

f. DoD Instruction (DoDI) 8510.01, 19 July 2022, “Risk Management Framework for DoD Systems”

g. CJCSI 3151.02A, 21 June 2023, “Common Operational Picture Staff Assistance Visit Program”

h. CJCSI 3151.01D, 28 August 2020, “Reporting Requirements for Global Command and Control: Common Operational Picture, Common Tactical Picture, and Common Intelligence Picture”

i. Global Common Operational Picture (COP) Concept of Operations, 15 July 2009

j. CJCSI 3265.02, 10 October 2014, “Joint Command and Control Systems Training Management”

k. DoDI 8500.01, 14 March 2014, incorporating Change 1, 7 October 2019, “Cybersecurity”

l. Joint Force HQ-DoDIN Task Order 20-0020, 6 May 2020, “Assured Compliance Assessment Solution (ACAS) Operational Guidance”

m. Office of the Chairman of the Joint Chiefs of Staff, “DoD Dictionary of Military and Associated Terms”

(INTENTIONALLY BLANK)

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk (*) *have definitions in PART II*

AO	Authorizing Official
A_O	operational availability
ATO	authority to operate
C2	command and control
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
COOP	continuity of operations
COP	common operational picture
CTP	common tactical picture
DADS	Defense Asset Distribution System
DISA	Defense Information Systems Agency
DJ-6	Director, Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber
DoD	Department of Defense
DSN	Defense Switched Network
GCCS-J	Global Command and Control System-Joint*
GSC	Global Command and Control System-Joint Site Coordinator
HQ	headquarters
IAW	in accordance with
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	information technology
J-3	Joint Staff Directorate for Operations
J-36	Joint Staff Deputy Directorate for Nuclear and Homeland Defense Operations
JOSC	Joint Operations Support Center

JP	Joint Publication
JSSC	Joint Staff Support Center
MTBF	Mean Time Between Failures
N2C3	Joint Staff J-36/National and Nuclear Command, Control, and Communications Division
NMCC	National Military Command Center
NMCS	National Military Command System
PM	Program Manager
PMO	Program Management Office
POC	point of contact
SA	situational awareness
SIPRNET	Secret Internet Protocol Router Network
UID	Unique Identifier
USSTRATCOM	U.S. Strategic Command

PART II – TERMS AND DEFINITIONS

Note: Unless identified as extracted from DoD Dictionary (reference (m)), these definitions are not standardized within the DoD and are applicable only within the context of this instruction.

Common Operational Picture. A single identical display of relevant information shared by more than one Command that facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called COP. (Source: JP 3-0.)

Common Tactical Picture. An accurate and complete display of relevant tactical data that integrates tactical information from the multi-tactical data link network, ground network, intelligence network, and sensor networks. Also called CTP. (Source: JP 3-01.)

Dependability. The measure of an information system's availability, reliability, maintainability, redundancy, and security.

Global Command and Control System-Joint. A deployable system supporting forces for joint and multinational operations across the range of military operations with compatible, interoperable, and integrated communications systems. Also called GCCS-J.

Global Command and Control System-Joint Critical Sites. GCCS-J sites that provide information, data feeds, or other services critical to C2 operations in support of the NMCS and are so designated by the Joint Staff J-36/N2C3 Division.

Global Command and Control System-Joint Site Coordinator. Designated main POC for all GCCS-J operational matters and management functions at a GCCS-J critical site. Also called GSC.

Global Common Operational Picture. The fusion of the CCMDs' TOP COP information to deliver a near-real-time rendering of the worldwide operational environment providing global situational awareness to support C2 of globally integrated operations.

Global Common Operational Picture Architecture. The globally interconnected, end-to-end set of information capabilities required to collect, process, store, disseminate, and manage Global COP information. It is comprised of the personnel, communications and computing systems and services, GCCS-J software (including applications), data, security services, and other associated capabilities necessary to provide C2 information on demand to warfighters, policy makers, and support personnel.

Mean Time Between Failures. The average time between system breakdowns. Also called MTBF.

Operational Availability. The measure of the percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission. Also called A_O.

Tactical Picture. The real-time or near-real-time integrated battle picture derived from sources managed by a component commander of the Joint Task Force that is a subset of the common tactical picture. Also called TP.

TOP Common Operational Picture. Theater-level COP that is consolidated, curated, and managed by CCMDs for a specified AOR.