

UNCLASSIFIED

**CJCSI 3151.02A
21 June 2023**

**COMMON OPERATIONAL
PICTURE STAFF ASSISTANCE
VISIT PROGRAM**



**JOINT STAFF
WASHINGTON, D.C. 20318**

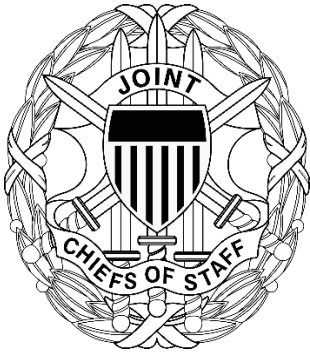
UNCLASSIFIED

UNCLASSIFIED

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3

DISTRIBUTION: A, B, C, S

CJCSI 3151.02A

21 June 2023

COMMON OPERATIONAL PICTURE STAFF ASSISTANCE VISIT PROGRAM

References:

See Enclosure B.

1. Purpose. This instruction establishes policy and procedures for conducting common operational picture (COP) staff assistance visits (SAVs).
2. Superseded/Cancellation. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3151.02, "Common Operational Picture/Shared Situational Awareness Command Assistance Visit Program," 17 June 2016 is hereby superseded.
3. Applicability. This instruction applies to the Services, Joint Staff, Combatant Commands (CCMDs), Defense Information Systems Agency (DISA), and those activities and agencies (hereinafter referred to as Components) reporting to the CJCS.
4. Policy
 - a. The CJCS conducts COP SAVs in fulfillment of the responsibility prescribed in reference j to advise the Secretary of Defense (SecDef) on development of joint command, control, communications, and cyber capabilities, including integration and interoperability of such capabilities, through requirements, integrated architectures, data standards, and assessments.
 - b. Responsibilities are prescribed in reference k to define the scope and document National Military Command System (NMCS) operations, its required components and procedures, and designated primary command-capable supporting elements, and develop policies, procedures, and standards and regularly exercise plans for using NMCS resources to support unified command and endure compliance through annual command and staff assessment visits.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

c. The CJCS delegates authority to conduct COP SAVs and otherwise to discharge the responsibilities in this directive to the Joint Staff Deputy Director for Nuclear and Homeland Defense Operations (DDNHDO), J-36.

d. The Joint Staff uses COP SAVs to assess the ability of critical sites in the Global COP (GCOP) architecture to meet the reporting requirements in reference a and operating policy in reference b, and make recommendations for improvements to their operations in support of GCOP development.

e. The Department of Defense's (DoD's) effort to advance command and control (C2) capabilities for the future is through the Joint All-Domain Command and Control (JADC2) initiative. Along with current systems of record, use of emerging and future JADC2 capabilities that become operationally employed for global C2 situational awareness will be assessed against the reporting requirements of reference a. The assessment criteria in this instruction will be adapted to include JADC2 capabilities as appropriate.

f. All designated COP critical sites are eligible for the COP SAV Program. Critical sites are those sites outlined in reference b and validated by the Joint Staff J-36 that provide information, data feeds, or other services critical to global C2 operations in support of the NMCS. Critical sites typically include:

- (1) National Military Command Center (NMCC).
- (2) Alternate NMCC (Site R).
- (3) Mission Management Center.
- (4) CCMD headquarters (HQs).
- (5) Service Component and Functional Component HQs of CCMD HQs.
- (6) Sub-unified Joint Commands, standing Joint Task Force HQs, and Joint Special Operations Task Force HQs.
- (7) Other special interest critical sites validated by the Joint Staff J-36.

Note: The active list of designated critical sites is maintained and updated annually by Joint Staff J-36 and is available upon request. Further information regarding critical sites can be found in reference b.

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

g. Critical sites receive COP SAVs to help them establish, maintain, and improve the skills, procedures, and material capabilities necessary to meet their C2 reporting responsibilities specified in references a and b.

h. COP SAVs are conducted at CCMDs, the NMCC, and Site R at least once every two years, or when the DDNHDO determines that such a visit is warranted. These sites may request an out-of-cycle SAV. All other critical sites (or their higher HQ) may request a COP SAV.

5. Definitions. See Glossary.

6. Responsibilities. As outlined in Enclosures A and B, and the following:

a. Component Heads (Critical Sites). To be effective, COP SAVs require active participation and support by Component staff from the Directorate for Intelligence, J-2; Directorate for Operations, J-3 (component lead); and Directorate for Command, Control, Communications, and Computers/Cyber, J-6, with augmentation from other directorates such as the Directorate for Manpower and Personnel, J-1 and Directorate for Joint Force Development, J-7, when necessary.

(1) Provide assistance as required to plan and execute COP SAVs.

(2) Submit requests for out-of-cycle COP SAVs to the DDNHDO in accordance with (IAW) Enclosure A.

(3) Fund visits that are not sponsored by the Joint Staff; e.g., out-of-cycle COP SAV.

b. DDNHDO

(1) Ensure the NMCC, alternate NMCC, and CCMD HQs each receive a COP SAV at least every two years.

(2) Exercise decision authority regarding out-of-cycle and other critical site COP SAV requests.

(3) Publish a schedule each year for the next year's visits.

(4) Designate an O-6/GS-15 to serve as Team Chief for each visit.

UNCLASSIFIED

CJCSI 3151.02A

21 June 2023

c. Chief, National and Nuclear Command, Control, and Communications Division, J-36

(1) Determine who serves as Team Chief for COP SAVs, unless directed otherwise by the DDNHDO.

(2) Provide day-to-day oversight of the COP SAV program.

d. Chief, Global Command and Control Operations Branch, J-36. Serve as the Joint Staff office of primary responsibility (OPR) for this directive.

7. Summary of Changes

a. Includes new requirements for Common Intelligence Picture (CIP) reporting and highlights the importance of the intelligence component of the COP.

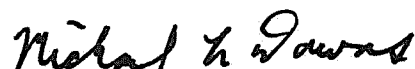
b. Adds off-year COP self-assessments and reporting requirements for CCMDs/NMCC.

c. Explains procedures to request out-of-cycle or critical site requested COP SAVs.

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Internet Protocol Router Network (NIPRNET). 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 web site.

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

For the Chairman of the Joint Chiefs of Staff:



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

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

Enclosures

A – Common Operational Picture Staff Assistance Visit

B – References

GL – Glossary

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

DISTRIBUTION

Distribution A, B, C plus the following:

Under Secretary of Defense for Acquisition and Sustainment
Under Secretary of Defense for Intelligence and Security
Department of Defense Chief Information Officer
President, National Defense University

OPR for the subject directive has chosen electronic distribution to the above organizations via e-mail. The Joint Staff Information Management Division has responsibility for publishing the subject directive to the SIPRNET and NIPRNET Joint Electronic Library web sites.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

TABLE OF CONTENTS

ENCLOSURE A – COMMON OPERATIONAL PICTURE	
STAFF ASSISTANCE VISIT	A-1
General	A-1
SAV Procedures	A-1
SAV Conduct	A-2
SAV Responsibilities	A-4
SAV Assessment Areas	A-6
Appendix A – SAV AREAS OF ASSESSMENT	A-A-1
Appendix B – POST-SAV FOLLOW UP AND SELF-ASSESSMENTS	A-B-1
ENCLOSURE B – REFERENCES	B-1
GLOSSARY OF ACRONYMS AND ABBREVIATIONS	GL-1

LIST OF TABLES

1. Track Latency Guidelines	A-A-D-1
2. URN Assignment Blocks	A-A-F-2
3. UID Table Example	A-A-F-3

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ENCLOSURE A

COMMON OPERATIONAL PICTURE STAFF ASSISTANCE VISIT

1. General. Assessment areas will follow the general outline below but can be tailored to a particular command based on mission or specific needs.

2. SAV Procedures

a. COP SAVs will be conducted at each CCMD and the NMCC primary and alternate sites/Joint Staff Support Center (JSSC) as described below. COP SAVs at all other critical sites will be conducted as necessary¹ or when requested by the critical site command or higher HQ.

b. The Joint Staff will assess each CCMD and the NMCC/JSSC once every two years. CCMDs, Component commands, and NMCC/JSSC may request an out-of-cycle SAV. Command requested or follow-up² SAVs will be coordinated on a case-by-case basis. To facilitate planning, the Joint Staff J-36 will publish a SAV master schedule for the upcoming year at the annual COP Working Group (WG) meeting.

c. The year following each Joint Staff-led SAV, CCMDs and NMCC/JSSC will conduct a self-assessment of their ability to execute the reporting requirements established in reference a. The self-assessment schedule will be included in the annual SAV master schedule. CCMDs and NMCC/JSSC will provide a summary of the assessment results to the DDNHDO, Joint Staff J-36 IAW the guidance at Appendix B.

d. To the extent feasible, Joint Staff will conduct command requested SAVs at Component commands and other critical sites in conjunction with a Joint Staff-sponsored CCMD SAV whenever geographic proximity permits. Other visits will be coordinated and scheduled directly with the requesting command and/or higher HQ—these visits may require command sponsorship and funded travel.

e. SAVs offer outside expertise to deliver focused assistance and training to address specific operational and technical issues. In addition, SAV teams will assist the staff's training division and conduct a review of all training plans, records, and local training directives.

¹ When a situation arises that has adverse effects on the comprehensiveness, timeliness, or accuracy of the GCOP or other similar factors that warrant Joint Staff review.

² A follow-up SAV could result from an incomplete assessment, or the identification of issues that require further evaluation or assistance from the SAV team.

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

f. SAV objectives and team composition will be tailored to meet the specific mission of the organization being visited; e.g., functional versus geographic CCMDs, air component versus maritime component commands. SAV team's normal core membership will consist of personnel who are subject-matter experts (SMEs) in COP and CIP from Joint Staff J-36, J-28 Battlespace Awareness, J-6 Deputy Director for Cyber and Command, Control, Communications, and Computers Integration, and DISA Global Command & Control System-Joint (GCCS-J) Program Management Office. The team chief duties will be executed by the senior Joint Staff J-36 member of the team as described in paragraph 4. SAV teams may be augmented by SMEs from the Joint Staff J-7 Joint Interoperability and Data Link Training Center (JID-TC), the JSSC, other Joint Staff J-6 offices, U.S. Strategic Command's GCOP management team, and others as appropriate.

g. SAVs will normally last 2–3 working days; however, multiple SAVs may be combined for efficiency (e.g., U.S. European Command and U.S. Africa Command may be conducted during the same visit, covering 4–5 days). To minimize staff scheduling disruptions, every effort will be made to minimize the time that personnel are detailed to a SAV team.

h. Prior to departure, the SAV team will conduct a formal outbrief to the command's identified leader. The DDNHDO will sign-out the final report sent to the command outlining the SAV team's observations and recommendations provided within 45 days following SAV completion.

i. Follow-up SAVs may be conducted as noted in the report or upon CCMD request.

3. SAV Conduct

a. Sixty days prior to the SAV, the Joint Staff J-36 will send a memo to the CCMD Chief of Staff regarding the SAV. The memo will include the purpose of the SAV and identify the SAV team chief and the SAV coordinator.

b. Thirty days prior to the SAV, the SAV coordinator will send an updated/tailored Area of Assessment Questionnaire to the CCMD.

c. The general COP SAV assessment areas discussed below in paragraph 5, SAV Assessment Areas, are to be used by CCMDs to guide SAV preparations.

d. In-Brief. The SAV team chief will provide an in-brief to members of the command prior to commencement of the SAV. The in-brief is open to COP/CIP stakeholders at any level; however, at a minimum, O-6/GS-15 representatives

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

from the J-2/J-3/J-6 are strongly encouraged to attend. The in-brief will cover the minimum following items:

(1) Introduction of the SAV team and the CCMD staff sections that will be visited. SAV team will consist of Joint Staff J-36 personnel, and other representatives as appropriate depending on the focus of the assessment. SMEs from other commands may also be on the team.

(2) The purpose of the COP SAV and its evolution over time.

(3) A review and finalization of CCMD sections to be visited, the SAV agenda, timeline, and any changes to the criteria or special requirements of the CCMD.

e. Review of Assessment Areas. Following the in-brief, members of the SAV team will engage with counterparts from the CCMD to review the Assessment Area Questionnaire and discuss other relevant issues and trends. In addition to completing the questionnaire, the SAV team (on a not-to-interfere basis) will tour Ops/Intel watch floor(s) to observe daily operations of the Watch Teams. It is highly beneficial for the SAV team to see a CCMD's operations and intelligence briefing and view any unique capability demonstrations, exercises, or C2-related tactics, techniques, and procedures (TTPs) in action.

f. Out-Brief. The out-brief to the command will provide a summation of the assessment, focus areas, specific findings and recommendations, and any areas of concern. Out-brief is open to anyone interested. O-6/GS-15 representatives from the J-2/J-3/J-6 should attend. General officer/flag officer/Senior Executive Service participation in the out-brief is encouraged. In addition, the SAV team will:

(1) Provide timetable for publication of final SAV after-action report (AAR), to include applicable references, recommendations, and timetable for command response, if applicable.

(2) Include a consolidated listing of action items, best practices, and lessons learned.

(3) Provide follow-up discussions with individual directorates (e.g., J-2/J-3/J-6) upon request.

(4) If desired, the team chief will conclude the visit with an executive summary brief for the commander or their designated representative after all assessment areas have been out-briefed.

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

4. SAV Responsibilities

a. Joint Staff

(1) Chief, Global Command and Control Operations Branch, J-36

(a) Recommends Joint Staff-sponsored SAVs to address significant changes or shortfalls in COP management, capabilities, policy, or procedures, or any issue that adversely affects the GCOP. The Joint Staff will conduct and sponsor SAVs to each CCMD on a biennial basis or when circumstances require a different frequency.

(b) The Joint Staff J-36 will maintain records from each SAV, as well as a consolidated listing of action items, best practices, and lessons learned.

(2) SAV Team Chief

(a) Typically, the Chief, Global Command and Control Operations Branch (GC2 OPS), J-36 or their designated representative (may be a SME from a supporting directorate or agency).

(b) Represents the Joint Staff to the Combatant Commander (CCDR).

(c) Presents the in-brief and out-brief to the command.

(d) Has overall responsibility for the SAV team and conduct of the SAV.

(e) Ensures all SAV objectives are addressed prior to the completion of the visit.

(3) SAV Coordinator

(a) Designated by the Chief, GC2 OPS, J-36 and serves as the Joint Staff point of contact for all SAVs.

(b) Coordinates and advertises available SAV dates for upcoming fiscal year.

(c) Coordinates with the command and develops an agenda to include a comprehensive list of SAV objectives that are aligned with reference a

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

and the command's mission, and that address specific issues or areas of concern identified by the command. Based on the compiled objectives, recommends team composition to the team chief.

(d) Finalizes SAV objectives in coordination with other team members and develops tasks and discussion items to meet SAV objectives. Disseminates final SAV objectives and tasks to the team and the visited command or organization.

(e) Requests and coordinates SAV team augmentation with SMEs in specific areas needed to support unique SAV objectives. Cost for augmentee participation will be the responsibility of the augmenters' parent organization. If funding for augmentee participation is not available, the requested organization should immediately notify the SAV Coordinator so other arrangements can be made.

(f) Conducts SAV team coordination meetings, as required, with members to review SAV objectives, tasks to be completed, SAV agenda, and trip arrangements. If the SAV team is augmented from other than the Joint Staff, this coordination may be via phone or e-mail until personnel are assembled at the SAV site.

b. Combatant Commands, Component Commands, and other Critical Sites

(1) Contact Chief, Global C2, J-36 at 703-693-9679, DSN 223, for information on how to request an out-of-cycle SAV.

(2) In the request, identify areas to focus the SAV's limited time to assist the commander to achieve meaningful and timely improvements.

(3) Submit all requests for SAV support through the command's J-3 staff sections to Joint Staff J-3 to ensure proper coordination of SAV requirements, to include travel, facilities, resources, and local arrangements to support SAV team members.

(4) For non-Joint Staff-sponsored SAVs (command-initiated), provide travel funding and accounting information to the SAV coordinator not later than (NLT) 45 days prior to the first day of travel.

(5) CCMD participation in SAVs at their Components and other critical sites significantly improves overall SAV outcomes and C2 operations in and between the CCMD and their Components/critical sites. While real-world operational needs may supersede SAV support, if requested by the Joint Staff,

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

CCMDs should make all attempts to provide personnel to attend and actively participate in SAVs at their Components and other critical sites.

c. SAV Team Personnel

(1) This section applies to SAV team personnel identified in paragraph 2.f.

(2) Travel to SAV site and conduct assistance visit activities, to include, but not limited to:

(a) Conduct a review of the command's initial, recurring, and supplemental COP policies and procedures, including a review of the command's adherence to COP requirements IAW references a-i and Enclosure A.

(b) Provide comments to requesting command personnel as required during the SAV.

(c) Prepare input for the SAV out-brief and support preparation for the AAR IAW instructions provided by the team chief.

5. SAV Assessment Areas

a. Manning and Training

(1) Manning to support CCDR's COP (Top COP) and GCOP missions 24/7.

(2) Joint Data Network Operations (JDNO)/Joint Interface Control Officer (JICO) functions.

(3) System administration.

(4) CIP development and maintenance.

(5) Security.

(6) Position Descriptions (PDs)/Statements of Work (SOWs).

(7) Formal Training/Command Specific Training.

(8) Continuity of Operations (COOP).

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

- (9) Surge Operations.
- b. Baseline COP Reporting
 - (1) Baseline COP information.
 - (2) Baseline COP development.
- c. CIP Management and Reporting/Intelligence Support to C2
 - (1) General Intelligence Support to C2 (ISC2) Support.
 - (2) ISC2 Architecture.
 - (3) Geospatial Intelligence.
 - (4) Additional Information.
- d. CCMD Data Management
 - (1) Time value (latency).
 - (2) Data sources.
 - (3) Time delay.
 - (4) Track management.
- e. CCMD COP Operational Architecture and Data Exchange Formats
 - (1) Operational availability.
 - (2) Communications.
 - (3) Data exchange and receipt formats.
 - (4) Daily operations.
 - (5) COOP.
 - (6) Air Tasking Order/Airspace Control Order (ATO/ACO) use.

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

f. CCMD Unit Reference Number and Unique Identifier Management. The team will assess command Unit Reference Numbers (URNs) and Unique Identifiers (UIDs) registration.

g. Security. The team will review adherence to security responsibilities as outlined in references b and c.

h. Requirements Management. The team will review command C2 requirements.

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

APPENDIX A TO ENCLOSURE A

SAV ASSESSMENT QUESTIONNAIRE

1. Purpose

a. Enclosure A provides additional details relating to the individual assessment areas for a SAV. It provides references and questions for each of the COP SAV assessment areas outlined in Enclosure A. It will be used as a guide by participating commands and SAV team members. The intent is to provide an updated/tailored questionnaire to the command 30 days prior to the assessment date of its SAV.

b. Following the SAV, the SAV team will write an AAR signed-out by the Joint Staff Deputy Director for Nuclear and Homeland Defense Operations, J-36 and provided to the command's Chief of Staff, J-2, J-3, and J-6. Copies will be provided to CCMD personnel who participated in the SAV. The report will include SAV findings and assigned action items, applicable references, recommendations, and a timetable for OPR (command, Joint Staff, DISA, etc.) command response, if applicable.

(1) Commands control further dissemination of their SAV reports. Command preference will be discussed and collected at the conclusion of the SAV out-brief. Commands are strongly encouraged to allow sharing via the Joint Staff J-36.

(2) The greatest value of the COP SAV Program is the accumulation of a body of knowledge based on C2 best practices and lessons learned across the Joint Force. Broadly sharing that knowledge throughout the C2 community of stakeholders is highly important to universally improving the COP.

2. Areas of Assessment. The outline of assessment areas below will be used as a guide to organize time and topics during the assessment. This listing will be tailored for each command according to mission areas, organizational structure, and command-specific requirements. These areas may be expanded, combined, or modified according to command requirements. The Joint Staff J-36 will coordinate with each command prior to the SAV to tailor their checklist. Assessment areas will include the Top COP, GCOP mission, and ISC2.

3. SAV Assessment Questionnaire. General COP/CIP information:

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

- (1) What software version of GCCS-J is the command using for operations?
- (2) If not on the latest version, what are your plans/schedule to update?
 - (a) Is equipment purchased/ordered?
 - (b) Will you conduct dual operations prior to cutover—if so, for how long?
- (3) What additional tools/capabilities does the command use to maintain situational awareness? Whether tools/capabilities are identified as part of the DoD JADC2 effort?
- (4) Does the command participate in the COP/CIP/C2 forums, such as the COP Capability Sub-WG, COP WG, Joint All Domain Situational Awareness-Operational Planning Team, and ISC2 WG?

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX A TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – A: MANNING AND TRAINING

1. Commanders must ensure they have highly trained and proficient track managers, network administrators, system administrators, and operators to build a complete and accurate COP and CIP. To support CCMD manning requirements, the Services must facilitate individual training necessary to support COP and CIP functions within the joint community.

2. Assessment of Manning and Training. CCMD J-1, J-2, J-3, and J-6 representatives will be included as appropriate.

a. Assessment topics will include manning for development and management of the Top COP, GCOP mission, JDNO, JICO, System Administration, CIP, and Security.

b. PDs/SOWs, formal training, command specific training, and capacity to support COOP and surge operations will also be reviewed.

c. Applicable references from Enclosure B may apply. The team will also address any other manning issues that impact the CCMD's ability to support 24/7 COP operations or concerns/issues that the command has.

3. Manning

a. Do the command's manning documents reflect billets for the JDNO, JICO, Joint Intelligence Center Watch Officer, Joint Interface Control Cell Manning Officers (Officer and Enlisted), COP operators/managers, system administrators, CIP managers, and Deployable Joint Command and Control personnel as appropriate?

b. If not, does the command (or one of its components) have an individual assigned to handle these duties on their behalf (specify how—e.g., additional duty, contract personnel, etc.)?

c. Is the command's current manning adequate to support all aspects of 24/7 COP operations during steady state?

d. What is the command's capacity to support COOP?

e. What is the command's capacity to support surge operations?

Annex A
Appendix A
Enclosure A

A-A-A-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

4. PD/SOW Review

a. In addition to tracking training, does the command have published PDs for COP and CIP personnel (i.e., PDs for COP operators, track managers/ database managers, and system administrators)?

b. Have PDs/SOWs been shared to the GCOP portal to assist other organizations in developing similar documents?

5. Formal Training. Have the command personnel supporting COP and CIP operations attended/completed requisite formal training from Joint Deployment Training Center (JDTC), Air Education & Training Command (AETC), or JID-TC? Formal training includes:

a. COP basic and advanced operator courses (JDTC).

b. Integrated Imagery and Intelligence (I3) Operator Course (JDTC).

c. Joint Interface Control Officer Course (JID-TC).

d. System Administration Courses (AETC).

e. Joint Data Network Staff Course (JID-TC).

6. Command-Specific Training. Does the command have an established training program to support command-specific COP and CIP operations?

a. What does training entail? (on-the-job training program, standard operating procedures (SOPs), TTPs, etc.).

b. Does training cover all positions? (SA/DBs, COP Operators/Managers, JICO, JDNO, CIP).

c. Does training address previously mentioned topics such as data sources, message formats, communications channels, time latency of data, manual vs automated inputs, track management procedures, security issues etc.?

d. Does the command identify skill sets and track trained/qualified personnel to include experience levels, and any special training/qualifications?

Annex A
Appendix A
Enclosure A

A-A-A-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

7. Continuity of Operations and Surge Operations. Does the command have adequate personnel identified and trained to support:

(a) COOP?

(b) Surge operations for exercises/real world operations?

8. Other Command Concerns/Issues. Does the command have any additional input?

Annex A
Appendix A
Enclosure A

A-A-A-3

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

A-A-A-4

UNCLASSIFIED

Annex A
Appendix A
Enclosure A

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX B TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – B: BASELINE COP REPORTING

1. IAW reference a, commanders establish COP reporting requirements and ensure that those reporting requirements are satisfied through COP procedures, training, and policy as specified in the Operation Task (OPTASK) COP and other local guidance. Baseline COP information may include current position and associated movement data for hostile, neutral, and friendly forces. Interagency, coalition partners, and forces of interest within a CDR's AOR will also be included.

2. Baseline COP Information

- a. Has the command established baseline COP reporting requirements?
- b. How has the command established guidance for maintaining the baseline COP? (view manuals, SOPs, memorandums of agreement (MOAs), etc.)
- c. Does the command's baseline COP information cover all domains?
- d. Does the command's baseline COP information include items such as positions and associated movement data for hostile, neutral, and friendly, including interagency and forces of interest; overlays; and command designated amplifying information such as in an ATO?
- e. Does the command's baseline COP include adequate intelligence products/information to support operations?
- f. How frequently is the information updated?

3. Baseline COP Development

a. Are written instructions provided (SOPs, Concepts of Operations, OPTASK COP, etc.) that outline policy and procedures to be followed for passing COP data? CDRs have the responsibility to direct procedures for components and deployed forces within their respective AORs to maintain an accurate theater COP.

(1) Do Services and Components provide curated COP information to the command that satisfy reporting requirements? If not, what steps have been taken to rectify?

Annex B
Appendix A
Enclosure A

A-A-B-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(2) Do Service-unique functions that enhance the COP follow the migration path for GCCS-J, meeting the appropriate level of common operating environment compliance?

b. Does the command have current Data Owners Guidance?

c. Are functions that support reporting to the COP joint and universal in application?

d. In addition to Service and Component information, how are other organizations and agencies (e.g., National Maritime Intelligence Center, local entities) contributing to the command's COP? Are any MOAs or memorandums of understanding in place to support their submissions?

e. Does the command effectively manage their Top COP to ensure the information they are passing to the GCOP is accurate, timely, and complete?

f. Are there any additional issues/concerns from the command?

g. Are there any notable best practices?

Annex B
Appendix A
Enclosure A

A-A-B-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX C TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – C: CIP MANAGEMENT AND REPORTING/ INTELLIGENCE SUPPORT TO C2

1. Military commanders need an integrated intelligence and operational picture across all domains (air, land, maritime, space, and cyberspace) that combines intelligence information from a CIP with operational information on U.S., allied, and coalition forces (the COP). An integrated COP/CIP will facilitate understanding the operational environment and contribute to the commander's decision-making process by providing reasoned insight into future conditions or situations. The integrated picture should leverage shared information from all security domains (Unclassified to Top Secret) to the maximum extent appropriate.

2. The J-2 SAV team representative will meet with command ISC2 stakeholders from the J-2, J-3, and J-6 staffs to discuss the following issues.

3. General ISC2 Support

a. What are the command's ISC2 policies, processes, procedures (e.g., OPTASK COP, OPTASK CIP, Theater CIP TASKORD)?

b. Has the command established baseline CIP reporting requirements for the HQ and subordinates (e.g., Components, Joint Task Forces (JTFs))?

(1) Are the Components in compliance?

(2) If not, why?

c. Does the command have the necessary infrastructure, subject matter expertise, and resources to develop integrated COP/CIP management procedures in order to coordinate across the HQ and subordinate staffs?

d. Does the command J-3 coordinate with the J-2 for integration of intelligence products/analysis into the COP?

e. Has the command established a data management plan with implemented business process management to enable efficient and timely updates to the COP/CIP to include geospatial and non-geospatial data?

f. Are there challenges in resolving correlation or data conflicts?

Annex C
Appendix A
Enclosure A

A-A-C-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

- g. Are there system or architecture issues hindering red track management?
- h. Does the command develop and maintain a relevant, timely red force picture? If not, why?
- i. What are the command's internal processes/workflow for storage and access of data (non-track data) with geospatial and non-geospatial information?
- j. Do Services and Components face any challenges in properly populating the CIP? If so, what specifically is preventing compliance?
- k. What gaps do the command and its components perceive in their ability to provide an integrated COP/CIP and how is it addressing those gaps?
- l. What are the command's ISC2 challenges in providing operational intelligence products via the COP/CIP?
- m. What gaps does the command perceive in its ability to provide target intelligence support to C2, what are the origins of these gaps, and how is it addressing those gaps?

4. ISC2 Architecture

a. As defined in references a and l, "The common intelligence picture is a single identical display of relevant, instructive, and contextual intelligence information regarding adversary and neutral force disposition, intentions, and supporting infrastructures, derived from all sources at any level of classification, shared by more than one command, that facilitates collaborative planning and assists all echelons to achieve situational awareness and decision advantage."

b. As noted in reference a, "Close linkage between relevant hostile and neutral tracks and the Modernized Integrated Database are critical to maintaining the relevance of the theater and global CIP."

(1) Is the Modernized Integrated Database/Machine-Assisted Analysis Rapid-Repository System (MIDB/MARS) order of battle and general military intelligence readily available via the COP/CIP?

(2) With respect to maintaining the relevance of the COP/CIP, what is the command's process for ensuring synchronization between MIDB/MARS

Annex C
Appendix A
Enclosure A

A-A-C-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

and hostile and neutral track data derived from tactical sensors or manual input?

c. What is the command's process for accessing component input for the CIP; e.g., how do the command Joint Intelligence Operations Centers (JIOCs) receive input from subordinate components and/or JTFs? Are Service Distributed Common Ground System (DCGS) nodes able to generate CIP tracks and forward them to the JIOC for consolidation?

d. Regarding imagery products that are available for display via the COP/CIP:

(1) What are the command's sources of imagery for the COP/CIP (e.g., tactical, national, full motion video, electro optical/infrared)?

(2) How is the imagery placed into the COP/CIP?

e. What GCCS-I3 capabilities are most useful to the command, and why?

f. What GCCS-I3 capabilities are least useful and/or not used, and why?

g. What other tools are being used for CIP visualization and why?

h. Regarding Common Data Framework-based federated content, discovery and retrieval/enterprise federation search:

(1) Do the command's analysts/users utilize DCGS Integrated Backbone-based federated search and discovery to support day-to-day analytical operations?

(a) If so, to what extent?

(b) If not, how do analysts/users access the mission data needed to perform analytical operations?

(2) By which means do analysts/users provide feedback on the operational effectiveness and improvements to federated information sharing, process, and capabilities across the command's enterprise?

5. Geospatial Intelligence

Annex C
Appendix A
Enclosure A

A-A-C-3

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

- a. What is the access and storage of geospatial intelligence (GEOINT) /imagery support for targeting, routine intelligence products, national production; and exercises (i.e., iStore or other)?
- b. What is the command's internal process/workflow process for storage and access of GEOINT/imagery products?
- c. Does the command have a requirement for GEOINT data retention (e.g., how long, how often)?
- d. Are there any existing GEOINT latency issues with access to imagery products?
- e. Are analysts utilizing any additional GEOINT storage such as local storage, shared folders, and/or desktop?
- f. Does the command have a requirement for historical data storage, historical data query, and data deletion?
- g. Does the command have any COOP requirements with respect to GEOINT/imagery capability?

6. Additional Information

- a. Are there areas where the Joint Staff can provide SME support/ assistance and or advocate for policy or material improvements that support the command's or component's ISC2 mission?
- b. To support future SAVs, are there additional areas of interest/need or SAV assessment methodologies that can be aligned with the command's specific mission and objectives?
- c. Active participation by Commands, Services, and Agencies in the ISC2 WG (IAW reference e) is critical to the DoD's ability to deliver ISC2 capabilities needed to meet warfighter requirements.
 - (1) Are there areas of concern that could be addressed by the ISC2 WG on behalf of the command?
 - (2) Are there initiatives that the ISC2 WG could conduct that would increase the command's level of participation in the WG and or the overall value of participation to the command?

Annex C
Appendix A
Enclosure A

A-A-C-4

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

d. Relevant to ISC2, are there any additional comments or areas of concern that the command would like to bring to the Joint Staff's attention?

e. The command is asked to provide advance copies of ISC2-relevant policy/SOP documentation to the Joint Staff J-28 SAV representative. The command is also asked to make knowledgeable staff members available who can speak to the topics noted above during the assistance visit. Written responses to the questions above are requested and highly encouraged. This will ensure the SAV team captures the command's processes, procedures, capabilities, strengths, needs, and concerns.

Annex C
Appendix A
Enclosure A

A-A-C-5

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

A-A-C-6

UNCLASSIFIED

Annex C
Appendix A
Enclosure A

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX D TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – D: COMBATANT COMMAND DATA MANAGEMENT

1. Information to build situational awareness is time sensitive. Real-time, near-real-time, and non-real-time information serves to provide the commander a sense of the environment in which he is operating. Delays due to data processing, slow communications networks, or any other transport delays can further degrade the value of information. It is imperative that data managers understand the time value of data displayed, take action to ensure timeliness of track and other required information, and comply with reporting criteria contained in the Global and Top COP and CIP guidance.

2. Time Value (Latency)

a. Do the command track managers and operators understand the time value of data being displayed in the COP/CIP and communicate this to commanders? If track latency exceeds time limitations (see Table 1, Track Latency Guidelines, in reference a), the command COP manager should use the guidelines in Table 1 that were derived from reference d as the standard. (NOTE: In all cases, extreme caution must be taken when deleting tracks to ensure relevant information is not lost).

b. If the command does not use Table 1 for track latency, what are they using?

DOMAIN	FRD	AFD	NEU	SUS	HOS	UNK	PND
Surface	15 min	4 hours	6 hours	24 hours	24 hours	6 hours	0
Subsurface	6 hours	6 hours	6 hours	24 hours	24 hours	2 hours	0
Space	24 hours	24 hours	24 hours	24 hours	24 hours	24 hours	0
Conventional	4 hours	4 hours	4 hours	24 hours	24 hours	2 hours	0
Air	3 min	3 min	3 min	3 min	3 min	3 min	0
SOF	4 hours	N/A	N/A	N/A	N/A	N/A	0
TBM (special)	N/A	N/A	N/A	6 hours	6 hours	6 hours	0

FRD: Friend
HOS: Hostile

AFD: Assumed Friend
UNK: Unknown

NEU: Neutral
PND: Pending

SUS: Suspect

Table 1. Track Latency Guidelines

Annex D
Appendix A
Enclosure A

A-A-D-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

3. Data Sources. Which of the following data sources does the command utilize?

- a. Automatic detection by remote, dedicated, or organic surveillance sensors.
- b. Units that automatically report their position or status (e.g., through non-terrestrial Force XXI Battle Command Brigade-and-Below – Blue Force Tracking, or other GPS-based tracking systems).
- c. Data automatically injected from other C2/GCCS-J databases.
- d. What manually entered data does the command rely on (situation reports (SITREPs), readiness systems, or other source reports)?
- e. Data derived from national, theater, and tactical collection, and reported via intelligence broadcast (e.g., Integrated Broadcast System (IBS), Link 16).
- f. Other—please specify.
- g. Are there other data sources that GCCS-J does not currently support that the command could benefit from?

4. Time Delay

- a. What does the command do to minimize operational impacts of time delays due to processed data? (Note: Processed data has high operational value, but good judgement with regards to the time value and close coordination between operational and intelligence personnel is an important planning factor.)
- b. What does the command do to maximize automatic inputs and minimize manual input of data to update COP displays?
- c. How does the command further define manual reporting relevant for the type and scope of operations in their AOR?

5. Track Management

- a. Does the command resolve data conflicts through the correlation process and have they developed procedures to resolve track attribute conflicts?

Annex D
Appendix A
Enclosure A

A-A-D-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

b. Does the command exercise effective track management discipline via delete tracks or merge tracks when sufficient information proves that erroneous tracks exist?

c. Does the command perform track correlation and fusion of data processes in order to match contact reports to visually displayed tracks?

Annex D
Appendix A
Enclosure A

A-A-D-3

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

Annex D
Appendix A
Enclosure A

A-A-D-4

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX E TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – E: COMBATANT COMMAND COP OPERATIONAL ARCHITECTURE AND DATA EXCHANGE FORMATS

1. The COP is a tool for sharing critical standing and situation-dependent information across CCMDs, and enhances the flow of situational awareness information to the SecDef and the Joint Staff. The COP both supplements and amplifies theater commanders' SITREPs, operational reports, and other reports outlined in reference a.

2. Operational Availability (IAW reference b)

a. Does the command's operational architecture meet the established requirements for critical sites in order to maintain operational availability?

b. What is the site's GCCS-J operational availability?

c. Has the command appointed a GCCS-J Site Coordinator and provided contact information to the JSSC and the GCOP Manager?

d. Are processes in place to provide outage and monthly reporting to the JSSC and the GCOP Manager?

3. Communications

a. What GCCS-J communication interfaces does the command COP employ (Note: CCMDs must ensure the communication interfaces chosen do not adversely affect other COP participants)?

b. Are communication interfaces identified in the OPTASK COP, OPTASK request/reply message?

c. Does the command's COP architecture overly burden communication assets required for mission accomplishment?

d. Is the time standard for GCCS-J COP universal time coordinated with an automatic conversion capability with local time?

e. Is the command's architecture diagram up to date and on the GCOP portal <<https://intelshare.intelink.sgov.gov/sites/globalcop/SitePages/Home.aspx>>?

Annex E
Appendix A
Enclosure A

A-A-E-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

f. Are plans in place for the command to maintain operations while in a susceptible state (i.e., in a denied-disconnected, intermittent, limited environment)?

g. Do the command COP Managers monitor the GCOP Chat Room <<https://chatsurfer.proj.nro.smil.mil/#/>>?

h. Are there any additional issues or concerns?

4. Data Exchange and Receipt Formats. Which of the following data exchange and receipt formats does the command use?

a. COP Synchronization Tool.

b. Message Data Transmission.

c. Over-the-Horizon Gold, IBS, Common Interactive Broadcast, Tactical Data Link (TDL) injects.

d. Keyhole Markup Language/ Keyhole Markup Language (Zipped).

e. Moving Target Indicator.

f. United States Message Text Format.

g. Multi-TDL Capability.

h. Joint Range Extension Application Protocol-C.

i. E-mail.

j. Beacon Track.

k. Others.

5. Daily Operations

a. How does the command use the COP to conduct daily operations (briefings, daily ops updates, command center continuous view, etc.)?

Annex E
Appendix A
Enclosure A

A-A-E-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

b. Where does the command specify data priorities such as air, space, ground, maritime, special interest tracks, as well as intelligence, environmental, and chemical, biological, radiological, and nuclear data?

c. Are there any ongoing issues that we should be aware of (problem reports, requirements, policy)?

d. Are there any best business practices the command is using that may be beneficial to other commands?

6. Air Tasking Order/Airspace Control Order

a. Is the COP displaying the ATO and ACO correctly?

b. Does the CCMD use GCCS-J to distribute the ATO to facilitate information flow and coordination (Note: The ATO can be posted or e-mailed as necessary)?

c. Does the CCDR make ATOs/ACOs available to the GCOP Management Center (GCMC) and the NMCC for all operations and circumstances?

d. During crisis monitoring, does the CCDR ensure the designated air component commander provides the ATO/ACO via the GCMC to the supporting CCDRs using GCCS-J?

e. Is there policy in place to assure the ATO/ACO will be provided as soon as published or updated as required?

f. During JTF Operations, is CCMD policy in place to ensure that the designated Joint Force Air Component Commander provides the ATO/ACO via the GCMC to the supporting CCDRs daily?

g. Are there any other ATO/ACO-related issues not previously captured above?

Annex E
Appendix A
Enclosure A

A-A-E-3

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

A-A-E-4

UNCLASSIFIED

Annex E
Appendix A
Enclosure A

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX F TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – F: COMBATANT COMMAND UNIT REFERENCE NUMBER AND UNIQUE IDENTIFIER MANAGEMENT DATABASES

1. URNs are associated with the Variable Message Format. Through the employment of URNs, blue force situational awareness is enhanced. These unique numbers facilitate tactical and operational battlespace situational understanding, provide blue force position location information, and friendly force status to reduce fratricide risk while increasing warfighting capability.
2. UIDs are used to uniquely identify each individual GCCS-J server. Each track contains attributes which include the UID of the GCCS-J server from which it originated. This identification is required to preserve accountability of track pedigree and is critical to maintain COP accuracy and authoritativeness through merging, fusing, and curating track data, to include reconciliation of duplicate and false tracks.
3. Does the command have a URN and UID manager assigned/designated?
4. Is there a command SOP or command policy that describes URN/UID management?
5. When was the SOP or policy last updated?
6. Are there any best business practices the command is using that could be passed on to other commands?
7. Are there any other URN or UID issues (e.g., cannot get an account for the database)?
8. Are the registered URNs/UIDs up to date and are UIDs correctly registered? (Note: A listing of registered UIDs will be reviewed as part of the SAV.)

Annex F
Appendix A
Enclosure A

A-A-F-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ORGANIZATION	URN ASSIGNMENT BLOCKS
U.S. ARMY	0 THROUGH 1999999
U.S. MARINE CORPS	2000000 THROUGH 2999999
U.S. AIR FORCE	3000000 THROUGH 3999999
U.S. NAVY	4000000 THROUGH 4999999
U.S. CENTRAL COMMAND	5000000 THROUGH 5349999
U.S. EUROPEAN COMMAND	5350000 THROUGH 5699999
U.S. NORTHERN COMMAND	5700000 THROUGH 5799999
U.S. INDO-PACIFIC COMMAND	5800000 THROUGH 6149999
U.S. SOUTHERN COMMAND	6150000 THROUGH 6349999
U.S. STRATEGIC COMMAND	6350000 THROUGH 6359999 6400000 THROUGH 6499999
JOINT STAFF	6360000 THROUGH 6369999
JOINT PERSONNEL RECOVERY AGENCY	6500000 THROUGH 6599999
U.S. SPECIAL OPERATIONS COMMAND	6380000 THROUGH 6389999
U.S. AFRICA COMMAND	6390000 THROUGH 6399999
U.S. SPACE FORCE, U.S. SPACE COMMAND, U.S. CYBER COMMAND	*TBD
COMBATANT COMMAND RESERVED	6600000 THROUGH 7999999
NETWORK ENABLED WEAPONS	8000000 THROUGH 8032767

Table 2. URN Assignment Blocks

*URN Blocks will be updated IAW reference i.

Annex F
Appendix A
Enclosure A

A-A-F-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

XYZCOM UIDs

[illegible]

Table 3. UID Table Example

Annex F
Appendix A
Enclosure A

A-A-F-3

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

A-A-F-4

UNCLASSIFIED

Annex F
Appendix A
Enclosure A

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX G TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – G: SECURITY

1. Each site must implement security for DoD information technology (IT) systems IAW reference c. Additionally, each GCCS-J site is responsible for ensuring meeting installation and configuration requirements, to include site-specific security controls and for appointing GCCS-J security positions as referenced below in writing.
2. Is the command in compliance with GCCS-J site security responsibilities as outlined in reference c?
3. Site GCCS-J Authorizing Official. Has the command appointed an authorizing official (AO) in writing to ensure instantiation of GCCS-J complies with assigned security requirements and controls, and that all site-inherited controls are implemented and maintained?
4. Site GCCS-J Program Manager/Systems Manager. Has the command appointed a program manager/systems manager (PM/SM) in writing to ensure implementation of the Risk Management Framework for all GCCS-J systems? The PM/SM is also responsible for applying approved system updates to GCCS-J software, and for ensuring that Plans of Action & Milestones are developed, tracked, and resolved.
5. Site GCCS-J Information System Security Manager. Has the command appointed an information system security manager (ISSM) in writing to ensure that security policies and security oversight of single or multiple sites are maintained? The ISSM also coordinates GCCS-J security measures, including analysis, testing, evaluations, verification, authorization, and review of GCCS-J installation at the appropriate classification level within the sites network structure.
6. Site GCCS-J Information System Security Officer. Has the command appointed an information system security officer (ISSO) in writing to develop, implement, and manage the GCCS-J site security program, to include security education, training, and awareness? The ISSO is also responsible for collecting and reviewing selected remote facility records, documenting any reported problems and corrective actions, and forwarding them to the site AO.

Annex G
Appendix A
Enclosure A

A-A-G-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

7. GCCS-J System Maintenance. Is the command up to date on patching? Is the command completing required weekly security scans?

Annex G
Appendix A
Enclosure A

A-A-G-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ANNEX H TO APPENDIX A TO ENCLOSURE A

ASSESSMENT AREA – H: REQUIREMENTS MANAGEMENT

1. The Net-Enabled Requirements Identification Database (NRID) is the repository and primary mechanism used by Joint Staff and CCMDs, Services, and Agencies for Capability Needs (CN) generation and management. The NRID and the Decision Support Toolkit serve as Joint C2 requirements collection and analysis tools.³
2. The NRID process flows from CN generation to solution development and warfighter capability delivery. CN refinement and decomposition is critical to ensuring the capability requirements manager and the materiel developer both have the necessary details to meet the warfighter's expectations. The Integrated Priority List (IPL) is the CCCR's opportunity to identify those capability gaps that introduce a level of risk to their ability to execute the operational, contingency, and campaign plans that support our National Military Strategy.
3. Does the command have an NRID/IPL manager or POC?
4. Does the command track submitted NRIDs/IPLs? If so, when was the last update?
5. Does the command currently need to submit an NRID/IPL for missing capability needs?
6. Does the command participate in requirements forums (e.g., COP Capability Sub-WG, COP WG, Council of Colonels, Executive Steering Committee, CNWG, Joint All Domain Situational Awareness Operational Planning Team, GCCS-J Deployment Hotwash, GCCS-J Bi-Monthly Community Meeting)?
7. Does the command have concerns about capability gaps with the GCCS-J or other C2 capabilities?

³ The NRID and Decision Support Toolkit are located on SIPRNET at <<https://intelshare.intelink.sgov.gov/sites/nrid>> for classified inputs and on NIPRNET at <<https://intelshare.intelink.sgov.gov/sites/ccd/ds/NRID-U>>.

Annex H
Appendix A
Enclosure A

A-A-H-1

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

Annex H
Appendix A
Enclosure A

A-A-H-2

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

APPENDIX B TO ENCLOSURE A

POST SAV FOLLOW UP AND SELF-ASSESSMENTS

1. General

a. Six-months after each Joint Staff-led SAV, the Joint Staff J-36 will initiate a Task Management Tool tasker at the O-6/GS-15 level requesting status on action items that were assigned to the CCMD from the SAV.

b. The year following each Joint Staff-led SAV, CCMDs will conduct a biennial self-assessment of their ability to execute the reporting requirements established in reference a. Once the command has completed their self-assessment, the Joint Staff J-36 will host a video teleconference with the command to discuss:

- (1) Any remaining open action items.
- (2) Obstacles/roadblocks encountered during the self-assessment.
- (3) New developments/changes/updates since the Joint Staff-led SAV.

c. Depending on a CCMD's level of need for subject matter expertise and assistance, they may request a CCMD-sponsored/-funded, in-person follow-up SAV in lieu of the six-month post-SAV activity or the biennial self-assessment and report. See formal requests for out-of-cycle SAVs in paragraph 6.b.

2. Self-Assessment Reports

a. CCMDs will use Appendix A to Enclosure A and the AAR from their previous SAV as a guide to conduct their self-assessment. The command should focus on changes since their previous SAV and progress on command-assigned action items.

b. The command will develop a summary that identifies self-assessment findings, progress made on previous action items, obstacles or roadblocks encountered and any changes to manning, training, procedures, etc., since the previous SAV. The summary should be included as part of a written memorandum signed by the command Director of Operations to the Joint Staff J-36 via e-mail NLT 45 days following the completion of the self-assessment.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

A-B-2

UNCLASSIFIED

Appendix B
Enclosure A

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

ENCLOSURE B

REFERENCES

- a. CJCSI 3151.01 Series, “Reporting Requirements for Global Command and Control: Common Operational Picture, Common Tactical Picture, and Common Intelligence Picture”
- b. CJCSI 3155.01 Series, “Global Command and Control System-Joint (GCCS-J) Operational Framework Policy”
- c. DoDI 8510.01 Series, “Risk Management Framework for DOD Information Technology”
- d. CJCSM 3115.01 Series, “Joint Data Network (JDN) Operations: Volume I”
- e. CJCSI 3265.01 Series, “Command and Control Governance and Management
- f. Updated Policy for Standardized Unique Identifiers (UID) in the Global Command and Control System, message, 131956Z March 2018
- g. CJCSI 3265.02 Series, “Joint Command and Control Systems Training Management”
- h. CJCSM 3265.01 Series, “Joint Command and Control (C2) Requirements Management Process and Procedures”
- i. CJCSI 3910 Series, “Friendly Force Tracking (FFT) Operations”
- j. Title 10, U.S. Code, section 153
- k. DoDD S-3710.01, “National Leadership Command Capability,”
- l. JP 2-0, 26 May 2022, “Joint Intelligence”

UNCLASSIFIED

CJCSI 3151.02A
21 June 2023

(INTENTIONALLY BLANK)

UNCLASSIFIED

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ACO	Airspace Control Order
AETC	Air Education & Training Command
AO	authorizing official
AOR	area of responsibility
ATO	Air Tasking Order
C2	command and control
CCDR	Combatant Commander
CCMD	Combatant Command
CIP	Common Intelligence Picture
CJCS	Chairman of the Joint Chiefs of Staff
COP	common operational picture
COOP	continuity of operations
GCCS-J	Global Command & Control System–Joint
GCOP	Global Common Operational Picture
GCMC	Global COP Management Center
GEOINT	geospatial intelligence
GPS	Global Positioning System
I3	Integrated, Imagery & Intelligence
IPL	Integrated Priority List
ISC2	Intelligence Support to Command & Control
ISSM	information system security manager
ISSO	information system security officer
JDNO	Joint Data Network Operations
JDTC	Joint Deployment Training Center
JICO	joint interface control officer
JID-TC	Joint Interoperability and Data Link-Training Center
JIOC	Joint Intelligence Operations Center
JSSC	Joint Staff Support Center
JTF	Joint Task Force
MIDB/MARS	Modernized Integrated Database/Machine Assisted Analysis Rapid-Repository System
MOA	memorandum of agreement
NRID	Net-Enabled Requirements Identification Database
NMCC	National Military Command Center

OPTASK	operation task
PD	position description
PM	program manager
SAV	staff assistance visit
SITREP	situational report
SM	system manager
SOP	standard operating procedures
SOW	statement of work
TASKORD	tasking order
TTP	tactics, techniques, and procedures
UID	Unique Identifier
URN	Unit Reference Number
WG	working group

UNCLASSIFIED

(INTENTIONALLY BLANK)
Inner Back Cover

UNCLASSIFIED

UNCLASSIFIED

INTENTIONALLY BLANK
(BACK COVER)

UNCLASSIFIED