CJCSM 3265.01A
29 November 2013

JOINT COMMAND AND CONTROL (C2) REQUIREMENTS MANAGEMENT PROCESS AND PROCEDURES

JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6 CJCSM 3265.01A
DISTRIBUTION: A, B, C, S 29 November 2013

JOINT COMMAND AND CONTROL (C2) REQUIREMENTS MANAGEMENT PROCESS AND PROCEDURES

Reference(s): See Enclosure E.

1. Purpose. This manual describes the process for identifying, documenting, validating, prioritizing, managing, and monitoring fulfillment of Joint C2 capability needs (CNs). When approved, these CNs become requirements for future doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P) development, and a means to complement existing joint requirements generation. This manual also defines various stakeholder responsibilities and describes procedures to submit, verify, assess, and prioritize Joint C2 CNs and requirements.

2. Superseded/Cancellation. This manual supersedes CJCSM 3265.01, 30 October 2010, "Joint Command and Control (C2) CNs/Requirements Management Procedures."

3. Applicability. This manual applies to the Joint Staff (JS), Combatant Commands (CCMDs), Services, Agencies (C/S/A), and National Guard Bureau (NGB). The procedures in this manual apply to Joint C2 requirements.

4. Definitions. See Glossary

5. Procedures. Joint C2 requirements management processes are intended to be agile and responsive and must remain so, and will evolve over time to keep pace with warfighter needs, technological improvements, and commercial practices. Therefore, Enclosure B, Joint C2 Requirements Management Process Flow, Enclosure C, Net-Enabled Requirements Identification Database (NRID) Users' Guide, and Enclosure D, Capability Definition Package (CDP)/Capability Package (CP) Template will be "living," updateable documents.

6. Summary of Changes. The entire manual was revised. This manual transfers Office of Primary Responsibility from JS J-3 to JS J-6 as the Joint C2

capability sponsor and requirements lead and focuses on the process for managing Joint C2 requirements.

7. Releasability. This directive is approved for public release; distribution is unlimited. Department of Defense (DOD) components (to include the CCMDs), other Federal agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at: http://www.dtic.mil/cjcs_directives.

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

For the Chairman of the Joint Chiefs of Staff:

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

Enclosures:

A - General Information
B - Joint C2 Requirements Management Process Flow
C - Net-Enabled Requirements Identification Database (NRID) Users' Guide
D - Capability Definition Package (CDP)/Capability Package (CP) Template
E - References
GL - Glossary (Abbreviations and Acronyms, Terms and Definitions)

DISTRIBUTION

Distribution A, B, and C plus the following:

	Copies
Secretary of Defense	2
Commander, U.S. Coast Guard	2
Commander, U.S. Element, NORAD	2
Director, Federal Emergency Management Agency	2
Director, Joint/Coalition Warfighting Center	2
Commanding General, Marine Corps Combat Development Command	2
President, National Defense University	2
President, Joint Forces Staff College	2
Naval Warfare Development Command	2
Chief, National Guard Bureau	2

The Office of Primary Responsibility 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 websites

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

LIST OF FIGURES

(INTENTIONALLY BLANK)

ENCLOSURE A

GENERAL INFORMATION

1. Background. Per reference a, the Director for Command, Control, Communications, Computers, and Cyber (DJ-6) serves as the capability sponsor and JS OPR for C2 requirements and capability development matters. JS J-6 Deputy Director Command and Control Integration (DDC2I), in accordance with (IAW) reference b, is the Joint Requirements Oversight Council (JROC)-delegated requirements lead for Joint C2. References c, d, and e, further support this JROC-delegated authority. JS J-6 DDC2I executes these responsibilities through the Combat Capability Developer (CCD) Division via the process outlined in this manual and supporting JROC memorandums (JROCMs). JS J-6's authority extends to the approval of all non-Key Performance Parameter (KPP) and Key System Attributes (KSA) changes. KPP change requests are submitted through the Command, Control, Communications, and Computers (C4)/Cyber Functional Capabilities Board (FCB) and the Joint Capabilities Board (JCB) to the JROC for approval.

a. Joint C2 capability is the principal C2 framework for execution of Joint C2 and achievement of decision superiority. These capabilities will enable decision superiority by allowing commanders to rapidly adapt to a changing mission environment defining their information needs and drawing on capabilities to effectively C2 forces to accomplish the mission. Joint C2 capabilities support strategic missions through unit-level commanders to include the Office of the Secretary of Defense (OSD), National Military Command System (NMCS), CCMDs, Service headquarters, Components, Joint Staff, DoD agencies, NGB, joint task forces, and mission partners. Joint C2 requirements are addressed through a streamlined and federated approach to enable delivery of Joint C2 capabilities via rapidly executed releases (with a goal of 12 months or less) by leveraging existing and emerging enterprise technologies.

b. Joint C2 requirements management relies on a requirements oversight structure supporting schedule and content determination as well as priorities of capability releases based upon collaboration between users and materiel developers. This approach ensures appropriate flexibility and oversight to plan for and incorporate evolving technology, addresses changing mission priorities during the requirements' lifecycle, allows early operational release of capability, and offers the ability to adapt and accommodate changes driven by field experience. This Information Technology (IT) Box-compliant structure and process is consistent with reference f guidance and codified in the Joint C2 Capability Development Document (CDD). This approach enables agile prioritization and sequencing of capability development on an annual basis by

providing increased warfighter ownership in the capability development process.

2. Requirements Management Process Overview. The Joint C2 requirements management process goal is to provide an effective, agile, streamlined, and responsive means to identify and manage warfighter requirements by expeditiously capturing, processing and documenting them for approval and subsequent action. The Joint C2 requirements management process includes the identification of DOTMLPF-P shortfalls and recommended approaches provided to the appropriate organization(s) for action. The requirements management process includes end-to-end engagement with warfighters/users, materiel developers, and testers throughout the capability lifecycle - concept development through fielding, sustainment, and sun setting of capability. Key requirements management process responsibilities include defining warfighter requirements and working closely with materiel developers and operational users to implement viable, timely and cost-effective solutions. The Joint C2 requirements management process mandates a strong partnership between the CCD Division, the warfighter/user, OSD/JS/C/S/A stakeholders, operational sponsors, and materiel developers. Figure 1 depicts the high-level (OV-1) diagram of the Joint C2 requirements management process.

a. The Joint C2 requirements management process provides traceability, via the Joint C2 CDD, Requirements Prioritization and Sequencing Plan (RPSP), and applicable CDPs and CPs, from identification of a CN to fielding of a capability. The five phases of the requirements management process include: 1) Identify/Submit; 2) Verify/Assess; 3) Score/Prioritize; 4) Sustain and Modernize Planning; and 5) Develop/Field. Enclosure B, Joint C2 Requirement Process Flow, provides a detailed description of each of the five phases. While each process phase is dependent upon the completion of previous steps and associated results, there are circumstances requiring the acceleration of Joint C2 capability development due to urgent warfighting priorities. Therefore, process acceleration is accounted for in the five Joint C2 requirements phases.

b. The Joint C2 requirements management process begins with warfighters communicating their C2 CNs to the CCD via the NRID with C/S/A O-6 level approval/endorsement (see Para 4 a.). C/S/A CNs are considered for the NRID only if they fall within the Joint C2 mission space. The Joint C2 mission space is defined as: the area supporting command capability and C2 activities from the NMCS through the Joint Force Commander (JFC) to their functional and Service component commanders down to unit level commanders, and includes, but is not limited to, situational awareness (SA)/common operational picture, intelligence support to C2, Planning and Execution, Force Employment, cyber C2 and Core Enabling/Cross Functional capabilities. The CCD develops and coordinates requirements priorities and sequencing, mapped to JROC-validated requirements in the CDD and RPSP, representing multi-year requirements priorities and planned capabilities across the Future Years Defense Program

(FYDP) and beyond. Near-term (within one year) details are more specific while out-years are less specific. The RPSP includes associated CDD and NRID/Forge.mil requirements, user stories and use cases. CCD maintains and updates the RPSP through the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)), and DoD Chief Information Officer (CIO)-led evolving Joint C2 Sustainment and Modernization Planning Process (SMPP) in order to sequence and coordinate the development and fielding of Joint C2 capabilities.

c. The CCD also develops and coordinates a set of fiscal year (FY) operational priorities using RPSP near-term requirements and planned capabilities, resulting in the warfighter's demand signal. These operational priorities, mapped to JROC-validated Joint C2 needs, provide the agility and flexibility to influence or adjust the sequence of delivery based upon warfighter prioritization, consistent with a capability-need based approach. The initial ranking of operational priorities is "bottom-up warfighter-driven" and determined based on the ability of individual planned capabilities to address prioritized capability gaps. These prioritized gaps are updated annually leveraging various "top down" sources, including Capability Gap Assessments (CGA), Integrated Priority Lists (IPL), reference g, reference h, and the Joint C2 CDD. The CCD also conducts an annual capability analysis and operational risk assessment (ORA) to identify and describe operational risks associated with Joint C2 capabilities. ORA results are considered during development and coordination of annual operational priorities and the Sustainment and Modernization Plan (SMP). The accumulation of all of these bottom-up and top-down inputs feeds a pair-wise comparison (each operational priority is matched head-to-head with each of the other operational priorities and scored for priority) methodology resulting in an annual ranking of warfighter operational priorities. Additionally, CCD engages the operational community via the appropriate reference a forums (C2 Working Groups (WG), C2 Council of Colonels (CoC), C2 Executive Steering Council (ESC)) and Joint Staff Action Processing (JSAP) coordination to validate the annual products associated with the operational priorities as to reinforce the warfighters' demand signal to the annual SMP. This process results in an annual JCB-approved list of operational priorities, codified in JROCMs. The resulting JROCM empowers the CCD and the Services to develop CDPs and CPs, as necessary, based on the JCB-approved operational priorities, to provide the most current, detailed/decomposed warfighter requirements. This approach enables warfighters to dynamically define/refine their CNs to enable timely submission of the most current requirements to materiel developers/ providers for acquisition planning in support of agile development.

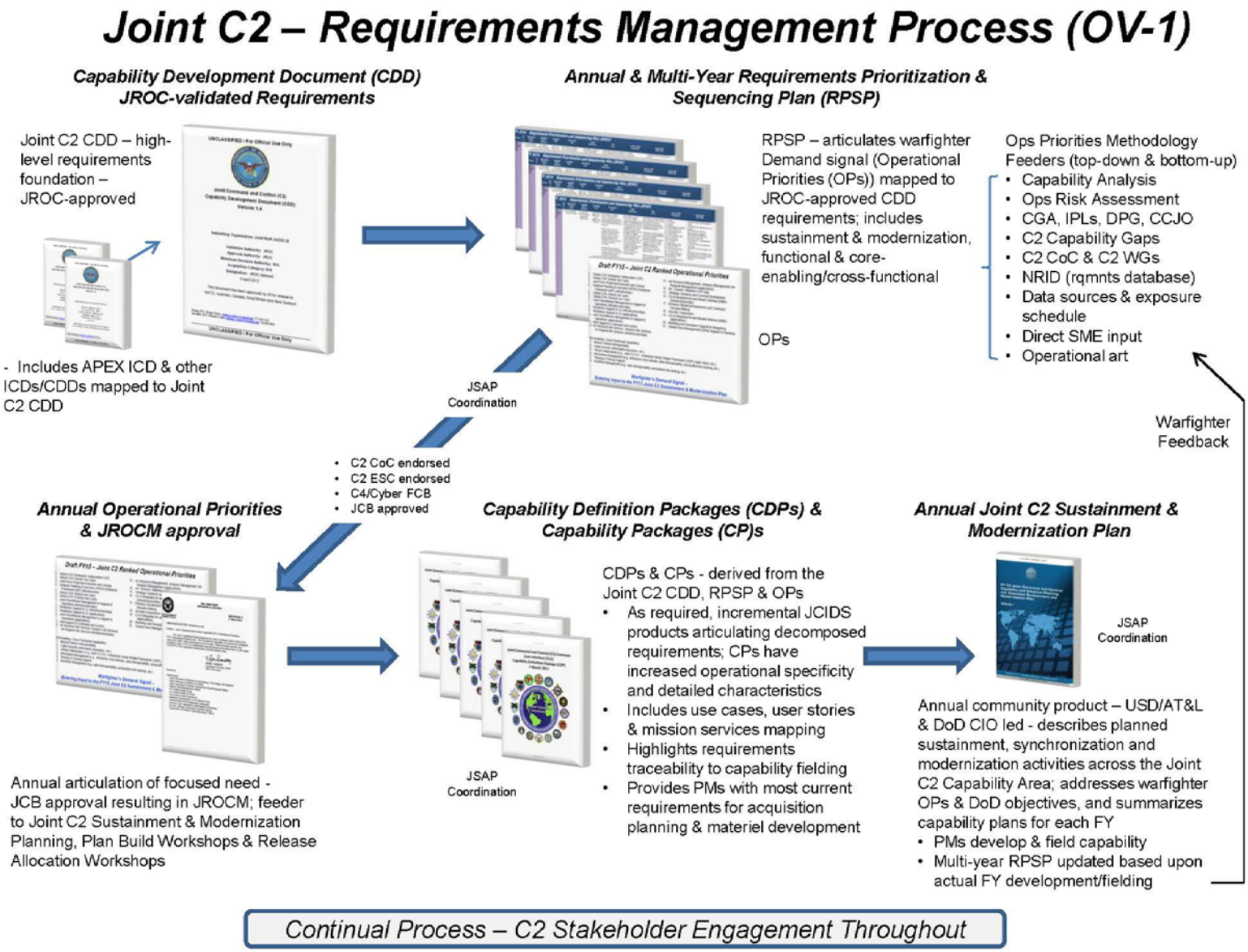

Figure 1. Joint C2 - Requirements Management Process (OV-1)

3. Requirements Management Process Components. The Joint C2 requirements management structure provides annual JCB-approved Joint C2 operational priorities vetted via JSAP staffing, endorsed by the C2 CoC, C2 ESC, and the C4/Cyber FCB. Joint C2 requirements oversight applies to requirements enumerated in the Joint C2 CDD and other Joint Capabilities Integration and Development System (JCIDS)-approved requirements mapped to the Joint C2 CDD, e.g., reference c. The organizational bodies comprising the Joint C2 requirements management structure fulfill the requirement for oversight, direction, and approval of Joint C2 requirements directed by reference b and supporting references c, d, and e. They also ensure Joint C2 CDD requirements management aligns to the IT Box-compliant framework. This IT Box-compliant requirements management structure pushes approval authority down to the lowest possible level to facilitate rapid, timely decision making and streamline the process to deliver CNs to materiel developers.

a. Joint Requirements Oversight Council (JROC). The JROC is the process owner for the JCIDS process. The JROC validates and prioritizes joint military requirements and advises the Secretary of Defense on the extent CCMD, Service and other DoD component program recommendations and budget proposals conform to strategic plans and CCMD priorities. The JROC retains the authority to approve/modify Joint C2 KPPs.

b. Joint Capabilities Board (JCB). The JCB is the second level of requirements oversight. Specifically, the JCB:

(1) Reviews and approves annual Joint C2 operational priorities and C2 authoritative data sources (ADS) data exposure schedules.

(2) Ensures CNs are consistent with C/S/A priorities.

(3) Informs the JROC of capabilities requiring KPP adjustment.

(4) Provides guidance and direction to the C4/Cyber FCB and other subordinate C2 bodies, as appropriate.

c. C4/Cyber Functional Capabilities Board (FCB). The C4/Cyber FCB reviews and assesses Joint C2 requirement documents and, as required, adjudicates lower-level issues prior to review by the JCB. The FCB also reviews prioritizations recommended by the C4/Cyber FCB WG and performs other activities as directed by the JROC or JCB. The C4/Cyber FCB makes recommendations to the JCB on approval or changes to the annual Joint C2 operational priorities and data exposure schedules of supporting C2 ADSs, and recommends to the JCB any adjustments to KPPs.

d. C4/Cyber FCB Working Group (WG). The C4/Cyber FCB WG is the lowest level organizational structure of the JROC. C4/Cyber FCB WG provides initial review/assessment of Joint C2 requirements documents and issues prior to review by the FCB, including the annual operational priorities, and performs other activities at the direction of the FCB Chair.

e. C2 Council of Colonels (CoC). The C2 CoC is a JS/C/S/A O-6-level forum, codified in reference a, integral to the requirements management process. The C2 CoC endorses Joint C2 requirements and operational priorities, including data exposure schedule of supporting ADSs, to the JCB via the C4/Cyber FCB. The C2 CoC reviews and addresses C2 capability issues (e.g., interoperability, integration, implementation, synchronization, fielding) and directs the C2 WGs to research requirements issues and provide recommendations, as needed.

f. JS J-6 Combat Capability Developer (CCD). CCD Division executes Joint C2 requirements lead responsibilities by providing oversight, direction, and approval of Joint C2 requirements at the direction of JS J-6 DDC2I. CCD conducts Joint C2 requirements management oversight supporting schedule and content determination and prioritization of capability releases based upon collaboration with users and materiel capability developers. Specifically, CCD:

(1) Provides direct coupling of warfighter C2 requirements to program managers (PMs) via continuous end-to-end warfighter engagement.

(2) Maximizes user visibility and involvement throughout the Joint C2 requirements management process from CN input through capability development and delivery.

(3) Maintains the NRID and Decision Support Toolkit (DST) as Joint C2 CNs collection and analysis tools.

(4) Tracks status of all Joint C2 requirements from submission through fielding and provides C2 WGs a quarterly update of this status. Requirements traceability is facilitated through recurring interaction with materiel developers.

(5) Continually reviews prioritized requirements, to ensure pending items are not overcome by technology or mission changes. Previous approved priorities are the starting point for developing a consolidated prioritized requirements list.

(6) Facilitates, via the C2 CoC and C2 WGs, the prioritization of C2 requirements.

(7) Per JROC delegation (reference e), executes Joint C2 non-KPP/non-KSA requirements approval authority.

(8) Coordinates with multi-national and mission partners to identify common C2 requirements and priorities, and identifies ongoing and planned partner materiel and non-materiel development efforts, to address common needs.

(9) Coordinates with OUSD(AT&L), and DoD CIO as the Principal Staff Assistant (PSA) for C2, in the development, documentation and promulgation of information exchange requirements (IERs) and standards for migration of Joint C2 functionalities to an agile C2 environment

(10) Promotes and facilitates the synchronization of C2 capability fielding timelines to ensure cross-Service integration.

g. JS J-6 Data and Services Division (DSD)

(1) Conducts CDP and CP reviews for compliance with evolving data and services standards IAW references f and i.

(2) Coordinates with OUSD(AT&L) and DoD CIO for standards-based IER development, verification, and validation in Joint C2 programs and capabilities.

(3) Serves as C2 ADS manager, coordinating C/S/A input and updates of information needs and ADS in the Data Services Environment.

h. Joint Staff J-6 Architecture and Integration Division

(1) Conducts CDP and CP reviews for compliance with JCIDS and Net-Ready-KPP in accordance with references j and k.

(2) Coordinates with OUSD (AT&L) and DoD CIO for architecture development, verification, and validation in Joint C2 programs and capabilities.

(3) Provides integrated Joint C2 architecture products and data enabling federation and/or reuse; provides accessible, visible, understandable, and reusable authoritative architecture data through the Warfighting Mission Area Architecture Portal.

i. Capability Needs Working Group (CNWG). As outlined in reference a, the CNWG is a C2 WG in the cross-functional focus area. The CCD-led CNWG facilitated the identification, validation, and prioritization of functional and cross-functional joint C2 requirements, working in close coordination with the C2 CoC and C2 WGs. The CNWG facilitates requirements interface across all C2 WGs to ensure synchronization and identification of potential duplicative requirements and gaps. The CNWG also addresses any KPP change requests

through the appropriate JCIDS forums. The CNWG engages appropriate OSD/JS/C/S/A stakeholders and operational users to validate and define cross-functional requirements and ensure cross-functional requirement priorities and define cross-functional requirements and ensure cross-functional requirement priorities are included in the RPSP. CNWG membership includes representatives from J-6 DDC2I and other JS directorates, along with OSD/C/S/A and mission partner representatives to other C2 WGs. The CNWG battle rhythm is conducted through monthly virtual engagements and more frequently as required. The CNWG also interfaces with C4/Cyberspace-related forums, e.g., NMCS governance structure NMCS Senior Steering Group (SSG) and NMCS Issues Working Group, Joint Fires Support Executive Steering Committee, Combat Identification - Friendly Force Tracking Executive Steering Committee, Multi-National Information Sharing/Mission Partner Environment (MPE)/ Unclassified Information Sharing and security cooperation requirements management processes, etc., and supporting structures, such as data, services, and architecture forums, to address requirements, interface dependencies, and capability development alignment and synchronization.

j. C2 Working Groups (WG). C2 WGs, as outlined in reference a, are led by an O-6/GS-15 civilian equivalent representative and include JS/C/S/A and multinational and mission partner representatives (generally in grade of O-5/GS-14 or below). The C2 WGs are aligned to the following focus areas: SA, planning and execution (including force employment), and cross-functional capabilities. For Joint C2 requirements, the C2 WGs:

(1) Support C2 requirements prioritization/sequencing and schedule content/allocation. This includes reviewing and endorsing data exposure schedules of supporting C2 ADSs.

(2) Support CCD in managing the identification, aggregation, prioritization, development, integration, and maintenance of C2 requirements/CNs as required throughout the C2 capability development and evaluation processes.

4. Requirements Mechanisms and Sources. While the Joint C2 CDD is the foundational source for the validation of Joint C2 requirements, JS J-6 CCD relies on other mechanisms and sources to identify, submit and process requirements. Joint C2 requirements mechanisms and sources are described below.

a. Net-Enabled Requirements Identification Database (NRID). The NRID is the primary mechanism used by JS and C/S/As to submit CNs. Inputs to the NRID require O-6 level approval/endorsement before they can be submitted. The NRID is located on the Secure Internet Protocol Router Network (SIPRNET) at https://intelshare.intelink.sgov.gov/sites/nrid for classified inputs; Unclassified NRID inputs are located on the Non-Classified Internet Protocol

Router Network (NIPRNET) at
https://intelshare.intelink.gov/sites/ccd/ds/NRID-U.

b. Forge.mil. The Forge.mil community consists of project/PMs, software developers, testers, warfighters, and other stakeholders responsible for the acquisition of IT. Forge.mil provides capabilities where community members can collaborate on open source and DoD community source software. Forge.mil is located at http://www.forge.mil

c. Capability Gap Assessment (CGA). The CGA process examines CCMD identified capability requirements and associated capability gaps, along with other issues and perspectives from the Services and other DOD Components, groups similar gaps, assesses ongoing efforts to close or mitigate capability gaps, and recommends programmatic and/or non-programmatic solutions to close or mitigate capability gaps. The result of the CGA is a list of capability gaps and recommended solutions for mitigation, presented for JROC approval.

d. Integrated Priority Lists (IPL). The IPL is a list of CCMDs' highest priority capability gaps and operational requirements. IPLs cross Service and functional lines, defining shortfalls in key capabilities, in the judgment of the CCMD, adversely affecting the ability of forces to accomplish their mission. IPLs provide recommendations for changes in existing requirements to: accelerate capabilities under development, change policies hindering mission execution, and/or program funds in the planning, programming, budgeting, and execution process.

e. Operational Risk Assessment (ORA). The annual Joint C2 ORA identifies and describes operational risk associated with Joint C2 capabilities and informs the determination of operational priorities in the RPSP. The ORA focuses on risks associated with the degradation of existing Joint C2 capabilities and delays for planned C2 modernization. The ORA begins with a review of previous ORA results. The CCD-led ORA team prepares a set of potential risk events binned into capability areas (CAs) and lists risk events in a web-based survey distributed to JS/C/S/A subject matter experts (SME). The SMEs rate the severity of the operational consequences of each risk event and may suggest additional risk events. The ORA team collects and analyzes the survey data and develops a risk profile for each risk. This includes assigning an estimated likelihood of occurrence and response strategies for each risk. The scoring results rank risks based on a combination of likelihood and consequence.

f. Additional Sources. Additional requirements sources include JROC-validated operational gaps, joint mission threads (JMTs), data sources and data exposure schedules in the Data and Services Environment (DSE), C2 WGs and senior leadership direction, with due consideration of CCMD and Service realities. Joint C2 requirements obtained through these sources are also

informed by operational experience and judgment, considering when, where and for what purpose forces will deploy and employ over time and how they will be employed to attain strategic goals.

5. Requirements Products. The Joint C2 requirements management process is dependent on several products to ensure delivery of timely solutions to the warfighter. First and foremost is the requirement itself. A requirement must clearly explain the gap it is addressing and contain sufficient detail so it is actionable and can be placed on a viable (timely, relevant, cost effective) solution path. The user should articulate who needs the capability along with the operational context and conditions associated with the need. The level of detail a user provides should leave no doubt what is expected from the developer in terms of speed, capacity, performance metrics, etc. A description of the key Joint C2 requirements products follows. Figure 2. depicts the key requirements documents to include iterative development of CDPs and CPs.

a. Requirements Prioritization and Sequencing Plan (RPSP). The RPSP depicts a multi-year view of Joint C2 requirements grouped into operational priorities by CAs. It is a sequence-based living document/database. The RPSP articulates requirements across the FYDP and beyond in general terms, while facilitating maximum agility by focusing on more specific requirements to be addressed in the next 1-18 months via CDPs and CPs. Near-term years are more specific, while out-years are less specific. Near-term requirement details reflect the starting point for content to be included in future CDPs and more detailed CPs. Specifically, the RPSP contains mapping to the Joint C2 CDD, associated gaps, use cases, user stories, mission services, and associated NRID CNs. The RPSP, along with the corresponding operational priorities, reflects direct engagement with the warfighter and serves as the demand signal to the SMPP.

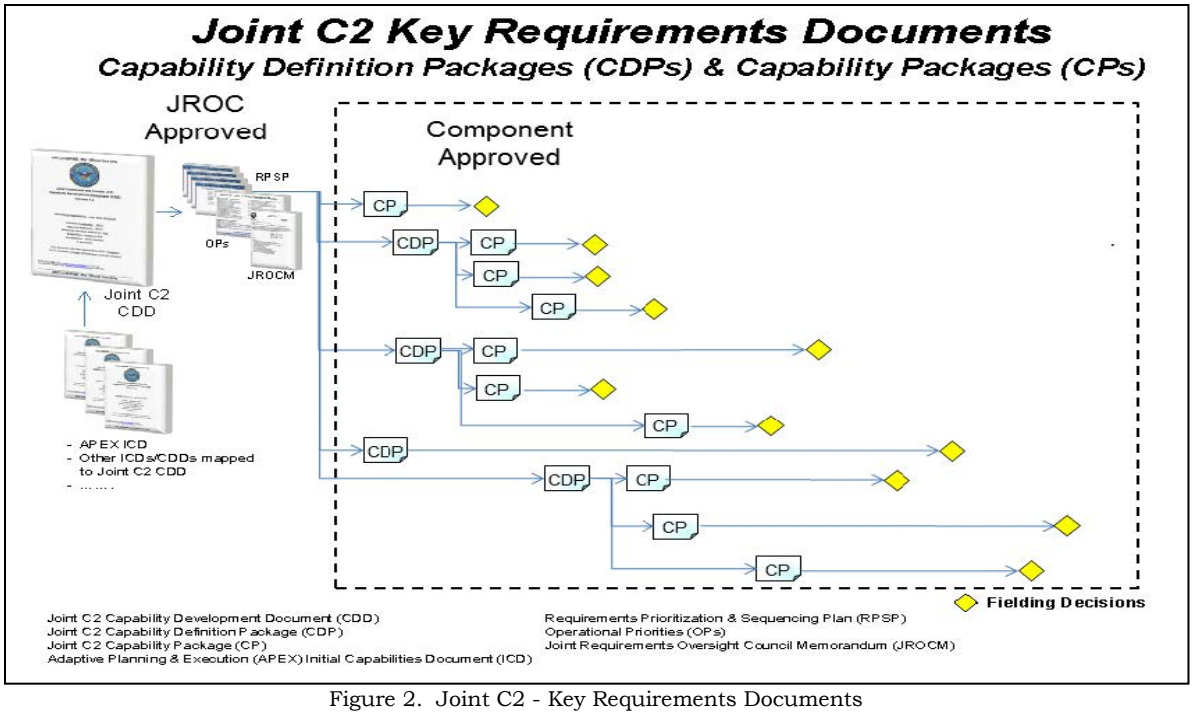

Figure 2. Joint C2 - Key Requirements Documents

b. Capability Definition Packages (CDP). The CDP is Joint C2's instantiation of the Requirements Definition Package (RDP) outlined in reference k. Use of the term "CDP" vice "RDP" was approved by the JROC and is consistent with reference k direction stating, "…Actual names, content and approval process are to be determined by the delegated validation authority." Joint C2 CDPs and CPs were a precursor to, and leveraged in, the development of reference k Information System RDP and Capability Drop (CD) documents. The CDP is a first-level decomposition of one or more requirements contained in or mapped to the Joint C2 CDD. CDPs may include, as required, development of Key Systems Attributes as well as measure of performance (MOP), measure of effectiveness (MOE), and measure of suitability (MOS). CDPs are developed by either the CCD or a C/S/A or operational sponsor in collaboration with the CCD, in conjunction with the operational user and the program office(s). CDPs developed by the CCD, a CCMD, Agency or operational sponsor are coordinated through the JSAP process. Service-developed CDPs are staffed through Service-specific channels (Air Force Requirements Oversight Council (AFROC), Marine Requirements Oversight Council (MROC), Army Requirements Oversight Council (AROC), Navy Requirements Oversight Council (NROC), etc.) and, via CCD, using the JSAP process. CDPs are approved by the Service component while CCD-developed CDPs are approved by JS J-6 DDC2I. CCMD, Agency, or operational sponsor-developed CDPs are also approved by JS J-6 DDC2I. CDPs align with one or more of the CAs defined in the Joint C2 CDD: SA, planning and execution, force employment, or core enabling/cross-functional. This approach gives the materiel developer a detailed description of CNs binned according to specific operational functions and provides the developer the operational context needed to accelerate

development and delivery of precise and timely solutions. CDPs present requirements with the detail necessary to identify the dependencies and core capabilities providing operational effectiveness below the level of those expressed in the Joint C2 CDD. This helps ensure the capability under development is compatible, integrated, and interoperable with other capabilities operating as shared services in the evolving Joint Information Environment and MPE. The CDP may be used to define requirements for a complete capability or establish the parameters for further decomposition into multiple CPs representing smaller discrete but related planned capabilities comprising something more complete and potentially complex. The result is incremental development and delivery of Joint C2 capabilities without the need for lengthy software development cycles. A guide for writing CDPs and CPs is located on the CCD Intelink website – https://intelshare.intelink.gov/sites/ccd/default.aspx. Enclosure D contains a CDP/CP template.

c. Capability Packages (CP). The CP is Joint C2's instantiation of the CD outlined in reference k. Use of the term "CP" vice "CD," also approved by the JROC, is consistent with reference k direction stating, "…names, content and approval process are to be determined by the delegated validation authority." CPs further decompose one or more requirements articulated in the parent document (CDD or CDP, as appropriate) to provide the materiel developer with greater operational specificity and detailed characteristics of the required capability. CPs may include, as required, development of MOP, MOE, and MOS. Like CDPs, CPs are either developed by the CCD or a C/S/A or operational sponsor in collaboration with the CCD, in conjunction with the user community and materiel developer to ensure they meet the operational need and are traceable to the requirements in the Joint C2 CDD and parent CDP. Typically, multiple CPs are required to express all of the detailed capabilities defined in the CDP. In some cases, a CP can be developed directly from CDD requirements if the capability required by the warfighter is sufficiently articulated in the CDD. CPs developed by the CCD are coordinated through the JSAP process. Service-developed CPs will be staffed through Service-specific channels (AFROC, MROC, AROC, NROC, etc.) and, via CCD, using the JSAP process. CCMD, Agency, and operational sponsor-developed CPs are coordinated through the JSAP process and approved by JS J-6 CCD. Service-developed CPs are approved by the Service component while CCD-developed CPs are approved by JS J-6 CCD. The CP should include a detailed performance and technical description of the operational capabilities a solution must provide to be acceptable to the warfighter, including specific performance parameters, to be developed, fielded, and tested within a single release of capability (notionally less than 12 months). The CP should also include dependencies affecting compatibility, integration, synchronization, and interoperability with other systems. Detailed CP requirements enable the rapid delivery of usable capability while affording the ability to refine/adapt

requirements and accommodate changes driven by field experience or operational need.

(INTENTIONALLY BLANK)

ENCLOSURE B

JOINT C2 REQUIREMENTS MANAGEMENT PROCESS FLOW

1. Purpose. Providing timely, detailed, well-understood, and actionable requirements to the material development community is critical to putting the right capability into the hands of warfighters at the right time (when needed). This section outlines the processes for identifying, capturing, processing, and prioritizing Joint C2 requirements and providing them to the materiel development community in a timely manner. A description of each of the five phases of the process follows.

2. Identify/Submit. The Identify/Submit phase, as depicted in Figure 3, is the process on-ramp for CNs. When users identify new CNs, they will obtain O-6 level endorsement from their organization prior to submission of the CN into the NRID. CCMD users need to ensure their NRID submissions reflect the C2 CNs identified by their command's annual IPL submission. If a user identifies a problem with an existing system, he/she should submit a problem report (PR) to the existing system's Help Desk rather than submitting an NRID input. CCD in coordination with the Program Office and operational sponsor, will review, validate, and prioritize PRs and change requests (CRs) within the scope of the program. If the Help Desk determines the input is not a PR but a CR for an existing system, the Help Desk will contact the submitter to recommend the CN be entered into the NRID.

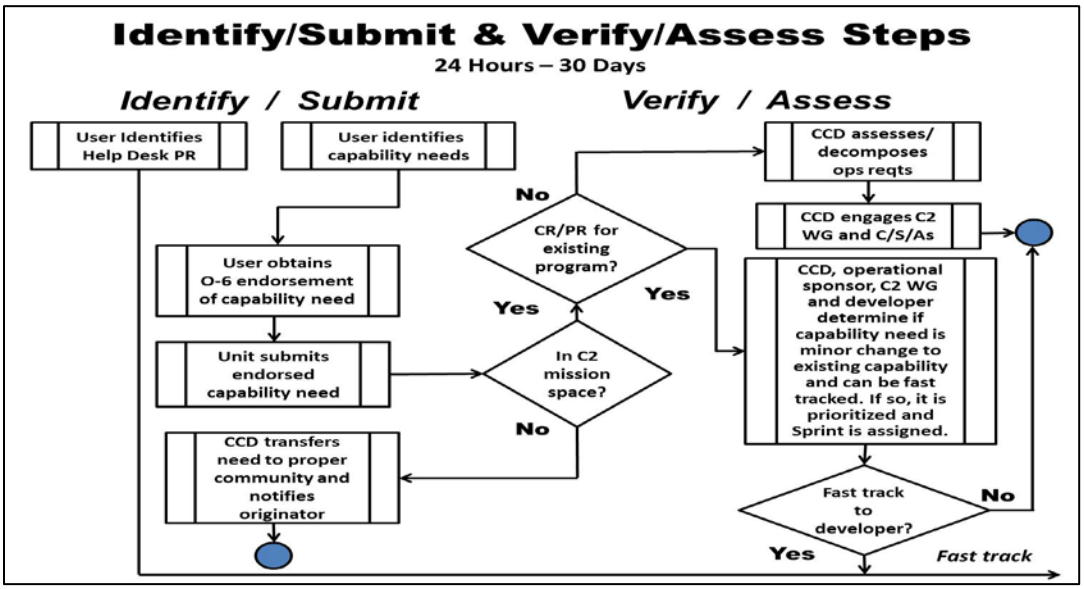

Figure 3. Identify/Submit and Verify/Assess Process Flow Breakout

3. Verify/Assess. During the verification portion of the Verify/Assess phase, CCD conducts a quick look analysis to ensure the CN is clearly articulated, understood, and fits within the Joint C2 mission space. Once the CN is determined to fit within the Joint C2 mission space and is clearly understood, the CN moves to the assessment portion of the Verify/Assess phase. During the assessment step, CCD, in coordination with operational sponsors, C2 WGs and users, decomposes the CN into actionable requirements with sufficient detail to inform scoring/prioritization decisions.

a. If CCD considers the NRID submission to be a PR, CCD and the operational sponsor discuss with the respective Help Desk to determine if the need can be treated as a PR. If the Help Desk agrees the input should be a PR, CCD transfers it to the respective Help desk to run through the program's PR process.

b. If the CN is determined to be a CR, the JS J-6 CCD, the appropriate operational sponsor, C2 WG and the developer review the CR, in close coordination with the submitters. The respective PM provides cost/schedule/performance implications to determine whether the CR can be fast-tracked.

c. The decision to fast track a CR is made jointly by the CCD, appropriate operational sponsor, C2 WG and the developer. CRs generated in the PMO are also discussed with CCD and operational sponsors to align efforts enabling various programs to modernize in the same direction toward enterprise solutions/services.

4. Score/Prioritize

a. CNs become validated requirements upon completing the Verify/Assess phase and being reviewed by the C2 WGs in the Score/Prioritize phase, (see Figure 4). The WG validates the requirement by determining the capability is needed and does not currently exist. WG members score the requirement on a 1-5 scale based on mission impact, with "1" the highest priority and "5" the lowest (scoring criteria is defined below).

(1) Mission Critical ("1") – prevents accomplishment of a mission critical capability with direct impact on mission failure, and /or readiness; no work-around or alternative solutions exist

(2) Mission Essential ("2") – adversely affects the accomplishment of, or degrades, a mission essential capability and no acceptable work-around or alternative solutions exist; requirement is needed to maintain sufficient military capability

(3) Major Mission Improvement ("3") – adversely affects accomplishment of, or degrades, mission essential capability and work-around / alternative solution is known; improvement will provide significant increase in mission capability or C2

(4) Minor Mission Improvement ("4") – results in user/operator inconvenience or annoyance, does not affect mission essential capability or prevent accomplishment of mission responsibilities; improvement will provide a moderate increase in mission capability or C2; addresses minor workaround(s)

(5) Mission Enhancement ("5") – addresses enhancements not critical or essential for mission accomplishment; increases efficiency; nice to have

b. Each C2 WG forum provides the resultant list of content and mission impact scoring to inform content development of planned capabilities prioritized for the Plan Build process. CCD categorizes and groups planned capabilities into Capability Modernization, Infrastructure Modernization, System Integration, or Data Integration. Based upon these groupings, requirements are broken into functionality requirements and technical/infrastructure requirements. Annually, the CCD updates capability gaps and gap priorities from a review of CGAs, IPLs, and Defense Planning Guidance, and coordinates these gaps and gap priorities with C/S/A stakeholders via the CNWG and presents to the C2 CoC for approval. CCD reviews the warfighter CNs, decomposed into requirements with mission impact scores and, in collaboration with C2 WGs, groups them into related planned capabilities intended to be addressed at the CP level. CCD maps the planned capabilities to the C2 CoC-approved prioritized capability gaps, resulting in an annual draft list of prioritized requirements (operational priorities) reflected in the RPSP. CCD and the JS J-6 DSD map all planned capabilities to the associated C2 data needs ensuring ADS requirements associated with those planned capabilities are identified and linked. The RPSP draft operational priorities are coordinated, via JSAP, with the C/S/As and forwarded to the C2 CoC, C2 ESC, C4/Cyber FCB, and to the JCB for approval. The coordinated and approved annual operational priorities are the warfighters' input (demand signal) to the annual SMP process. In parallel, CCD initiates/ coordinates CP development related to the respective operational priorities. As IERs are identified within the planned capabilities, JS J-6 DSD will review those requirements for standards-based applicability and conformance IAW references f and i.

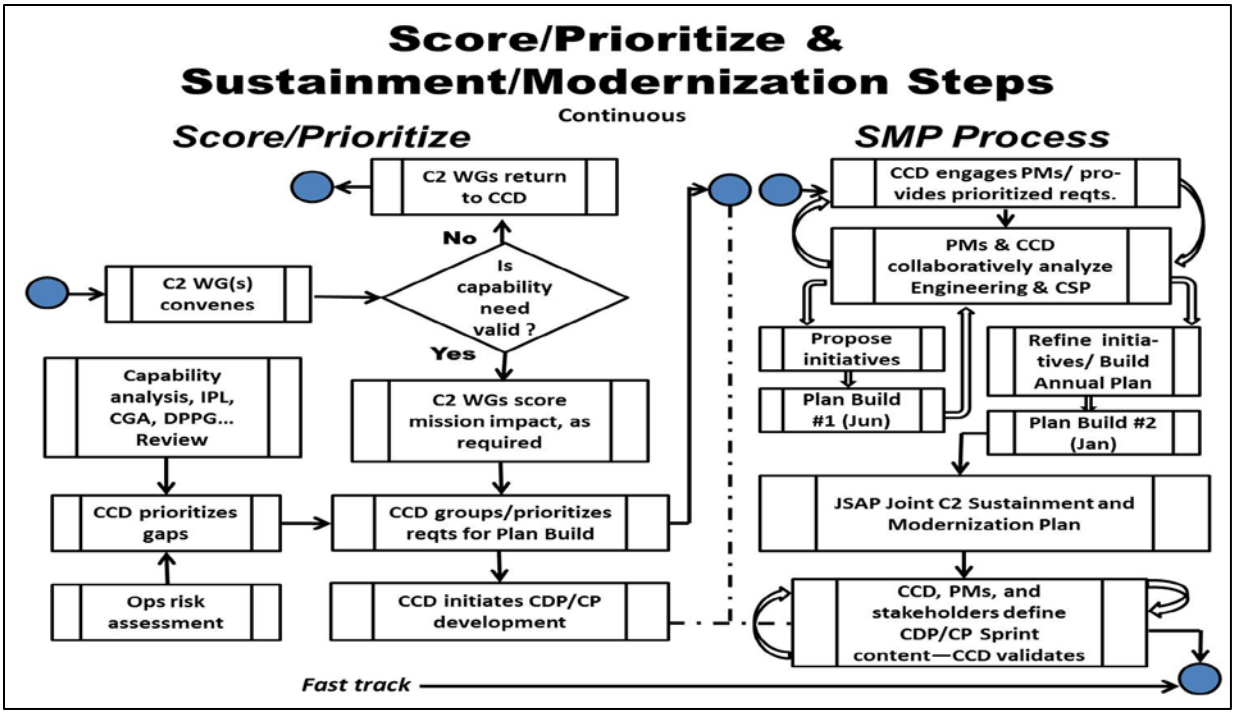

Figure 4. Score/Prioritize and Sustainment & Modernization Planning Process Flow Breakout

5. Sustainment and Modernization Planning Process (SMPP). Annual SMPP begins when CCD presents the JROC-approved operational priorities to the semi-annual Plan Build workshop. CCD engages the DoD CIO C2 PSA staff, OUSD (AT&L), and PMs to align capability development initiatives to approved operational priorities. Plan Build workshops provide an opportunity to collaboratively plan capability development and determine fielding schedule; cost and technical feasibility; cross capability dependencies and synchronization; and ADS accessibility and visibility for tradespace negotiation. The goal is an optimally integrated mix of capabilities based on prioritized modernization needs for the next planned release IAW approved operational priorities, deemed executable within programmed resources, with due consideration given to sustainment/ synchronization efforts. Plan Build workshops use approved operational priorities to project capability releases for the next FY, initial capabilities for the following FY and general details for additional FYs to facilitate Services' and Agencies' ability to make informed decisions. Typically, CCD, PMs, OSD and C2 stakeholders review Sprint content, where sprint is defined as a specific version of software to be released, as it is aligned to CPs, for capability development and fielding. Additionally, Plan Build workshop activities and SMPs are informed by recurring C2 Program Manager-Chief Engineer Steering Group (PM-CESG) and Joint C2 Senior Steering Group for Acquisition (SSG-A) meetings. The PM-CESG provides engineering oversight enabling the functional allocation, interoperability, synchronization, and performance associated with integration and implementation of Joint C2 capabilities and data/technology standards by and across the Joint C2 family of programs (FoP). The Joint C2 SSG-A

coordinates Program Executive Office-level direction to their programs and resolves issues raised by the O6-level Joint C2 PM-CESG to ensure synchronization of all Joint C2 FoP development and implementation activities and related Service/Agency C2 programs.

6. Develop/Field. During the Develop/Field phase, (see Figure 5), materiel developers use the approved annual operational priorities, SMP and CDP/CP requirements documents to develop C2 capability. Utilizing CDPs, CPs, and fast tracked CRs, the CCD, PMs and materiel developers coordinate capability sprints. In the case where the more granular documents (CDPs/CPs) have not been produced, the user stories from each operational priority provide the starting point for defining capability development plans and sprints. The capability sponsor and requirements lead, along with the operational sponsor, and warfighters/users, as required, remain engaged with the materiel developer throughout the development and fielding of capability as depicted in Figure 6. This engagement includes active participation in development of supporting acquisition documentation to further decompose the requirements in, for example, Technical Requirements Documents, System Requirements Documents, System/Software Requirements Specifications, and follow-on Information Support Plans. Capability sponsor and requirements lead engagement also includes active participation in Preliminary Design Reviews and Critical Design Reviews. This collaborative design engagement provides opportunity to not only ensure requirements traceability, but to effect desired operational performance for the user communities being ultimately served by this development activity. The materiel developer provides periodic updates on the status of required capabilities in development and seeks C2 CoC endorsement and CCD approval on non-KPP tradeoff decisions affecting these required capabilities. These required capabilities are delivered to the warfighter once selected materiel solutions have been formally tested and evaluated to ensure operational effectiveness and suitability. The operational sponsor and JS J-6 CCD as capability sponsor, with user inputs received during testing, provide fielding recommendations to materiel developers regarding capability performance satisfaction in meeting warfighter expectations and act as an advocate to ensure the warfighter receives operationally functional, interoperable, and supportable capabilities within the concept of fielding and deployment.

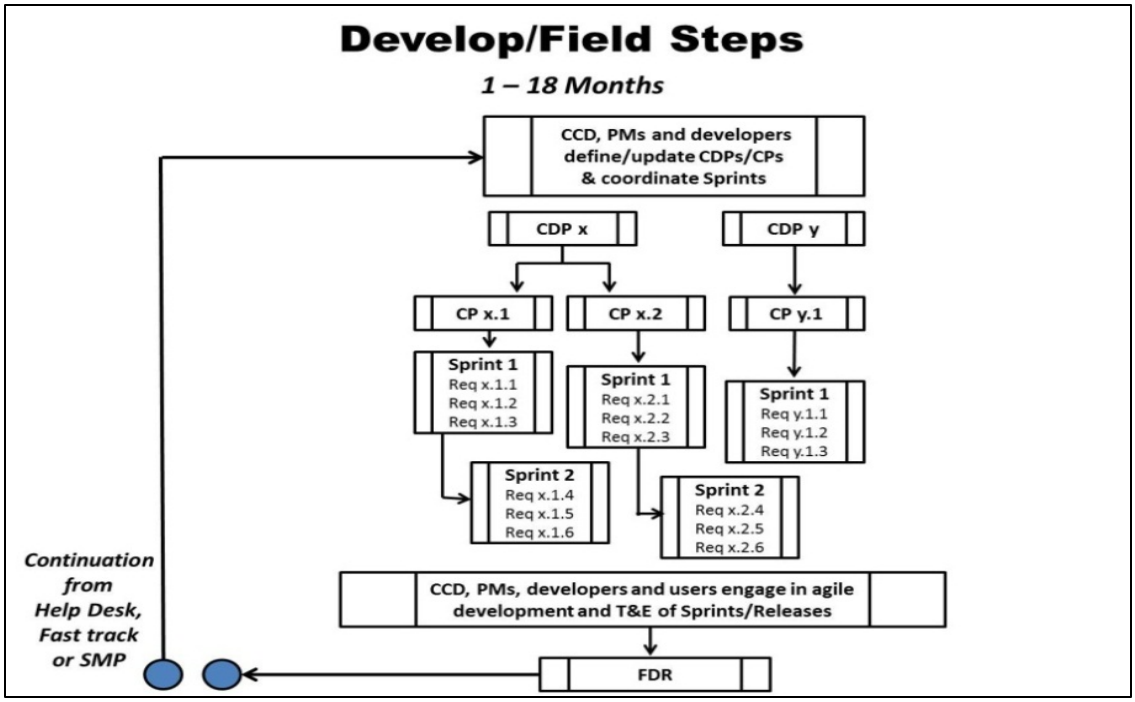

Figure 5. Develop/Field Process Flow Breakout

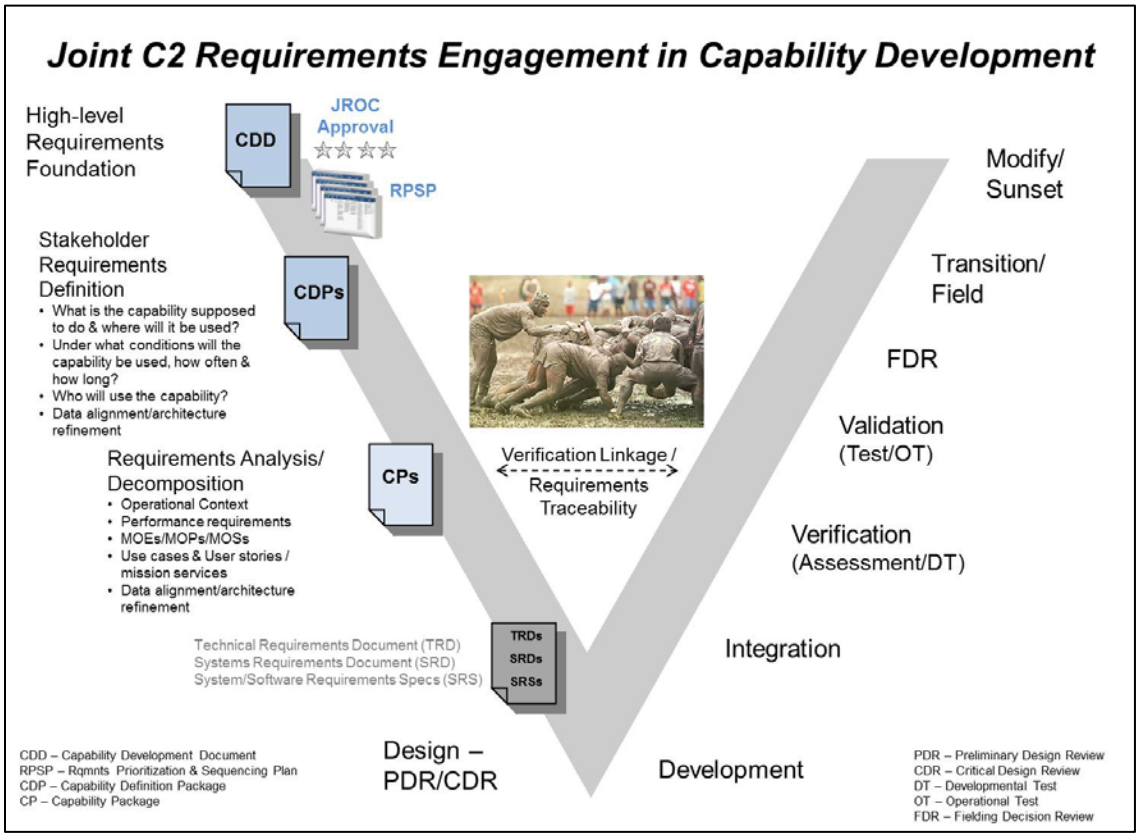

Figure 6. Joint C2 Requirements Engagement in Capability Development

7. Operational Assessment. Annually, immediately following the publication of the Deputy Secretary of Defense's Resource Management Directives (RMD) (or equivalent documents), the CCD will assess all of the prior year's reference a Joint C2 requirements-related products to determine how well its development activities support RMD direction.

(INTENTIONALLY BLANK)

ENCLOSURE C

NET-ENABLED REQUIREMENTS IDENTIFICATION DATABASE (NRID) USER'S GUIDE

1. Purpose. The NRID Users' Guide provides an overview of the NRID process from CN generation to solution development and warfighter capability delivery. Its focus however is on CN submission, the beginning of the NRID process. In addition to providing step-by-step instructions on how to submit a CN, this Users' Guide offers tips on writing an actionable requirement (e.g., a concise well-understood CN giving developers a detailed perspective on what is required). It is important to keep in mind the NRID submission is only a starting point. Dialogue between the submitter and the CCD SME responsible for processing the CN is an ongoing process as more detail on the CN is gathered. This 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.

2. NRID Evolution. Since the NRID's inception in October 2007, the process has continued to evolve in order to improve ease of use and the integration of such features as automatically generated emails triggered by a CN submission and SharePoint Alerts based on CN updates. Since 2010, unclassified NRID CNs have migrated to the NIPRNET DST, where they are analyzed, managed and tracked by CCD as part of its Joint C2 requirements management process. Additionally, the NRID has migrated from a purely SIPRNET tool, known as NRID-S, to NIPRNET, known as NRID-U, specifically accepting, processing and tracking unclassified inputs. Migrating unclassified CNs to NRID-U benefits operational users by providing an unclassified site for submitting CNs enabling use in conjunction with the C2 WG, the C2 CoC, and during collaboration between C2 capability developers. Recent NRID improvements include:

a. Opening up access so creation of a CN no longer requires membership in an "NRID Manager's Group." Now, a CN can be submitted by a user after gaining C/S/A O-6 level approval/endorsement.

b. NRID CN input fields have been updated to reflect continuing improvements to the Joint C2 requirements management process.

c. New fields have been added based upon collaboration with J-6 partners who manage reference l requirements.

d. NRID submissions are followed up with an email to the submitter including a link back to the submitted CN for bookmarking by the submitter.

NRID CN status changes are sent to the submitter via email with SharePoint Alerts.

3. NRID Process. The overall high-level NRID process is covered in Enclosure B - Requirements Management Process Flow. This section provides step-by-step instructions on how to submit a CN in addition to offering tips on writing an actionable requirement (e.g., a clear, concise, well-understood CN giving a developer a detailed perspective on what is required).

a. Submitting an NRID Input. This is the initial step for getting a CN into the Joint C2 requirements management process. The key factor in reducing the time it takes for a CN to get from the submission to the development and fielding stages is greatly dependent on how well the CN is written. NRID submitters require an Interlink Passport ID to submit a Joint C2 CN. Users can obtain the ID at https://passport.intelink.gov/passport/Welcome. With the Intelink Passport ID, users can navigate to the NRID to enter the CN. The "Sign In" link is in the upper right portion of the web page. Once a user is signed in, a CN can be entered via the following steps:

(1) Select the link: "Click here to create a new Capability Need."

(2) Fill in all mandatory fields outlined in red with an asterisk (*) next to field name.

(3) Provide as much detail as possible in the non-mandatory fields. A more complete requirement contains as much detail as possible and describes the need, the operational context, the role of the users, etc.

(4) Attach any necessary documents to the CN using the "Attach File" button at the top of the page.

(5) Select "Submit" when complete and approved/endorsed by an O6-level representative.

b. Writing an Actionable Requirement. Several years of NRID experience indicates the most critical determinant of how quickly a CN is acted upon is how well the need is defined by the user. This expedites the verify/assess steps when the CN becomes an actionable requirement. An actionable requirement begins with well-written CN clearly stating the user's specific problem, the functionality desired and the measurable conditions, constraints and contextual factors used in developing a solution. Specifically, to become an actionable requirement a CN must be:

(1) Described from a "user" point of view

(2) Achievable within realistic or definable budgets

(3) Measurable and testable

(4) Verifiable (i.e., use specific terms such as “exactly” and “no less than,” rather than “sufficient,” “excessive” or “reasonable”)

(5) Unambiguous (e.g., have only one possible meaning)

(6) Expressed in terms of need, not solution

(7) Consistent with other requirements

(8) Documented/expressed in language understandable to all

(9) Provide context including actor, location, process being accomplished, and desired outcome

(10) Keep sentences and paragraphs short using proper grammar, spelling, and punctuation

(11) Ask “why” and “what” questions rather than “how”

(12) Use words directive in nature and use active voice

(13) Use tolerances (≤, ≥, range, ±) to help the developer/designer

(14) Never use “and/or” in a requirement statement

The degree a requirement meets these parameters determines how much additional detail the CCD must solicit from the user to decompose the requirement to CDP/CP level.

c. Tracking NRID Submissions. Once the CN is submitted, the submitter receives a confirmation email containing a direct link to the need. The submitter can visit the NRID at any time to check the status of a CN. NRID CNs are tracked in several ways. On the NRID home page, users can browse CNs by using the “Quick View - CNs by Status” or by using the “Quick View - CNs by Working Group” web parts. The user also has the option of viewing all of the CNs using the “All Capability Needs” tab near the top of the page. As the NRID is hosted on SharePoint, common SharePoint features are available such as the ability to sort and filter CNs using column headers. Users also can view data using any available list views. Quick views allow NRID users to see CNs by status and WG. All of the CNs resident in the NRID can be viewed by clicking on the “All Capability Needs” tab near the top of the page. Users can also set up a SharePoint Alert on their CN so an email is automatically generated every time an update is made to the CN. Submitters are contacted by a CCD SME who will follow up on the submission and gather any additional details. The following CN attributes are assigned by CCD SMEs:

(1) Status

(2) CN ID

(3) CCD Point of Contact

(4) WG

d. Additional Considerations**.** Many users have more than one Intelink Passport ID since Intelink allows login via Common Access Card. For more information, including how to look up multiple Passport accounts, visit https://intellipedia.intelink.gov/wiki/Intelink_Passport

e. NRID Help. Direct specific NRID questions or improvement suggestions to the CCD.

ENCLOSURE D

CAPABILITY DEFINITION PACKAGE (CDP)/CAPABILITY PACKAGE (CP) TEMPLATE

1. Pages D-2 through D-13 of this enclosure provide the template for developing a CDP or CP. This template supersedes "The Executive Guide for Production of the Joint C2 CDP and Capability Package (CP)" and will continue to evolve in order to take into account changes in requirements development ensuring continued agility and flexibility in providing responsive CNs to materiel developers. The template will be updated, as required, and in coordination with the C2 community.

2. Following is the link located on NIPRNET to the CCD Intelink external portal page: https://intelshare.intelink.gov/sites/ccd/ext/default.aspx. To access the Joint C2 CDD or Joint C2 CDPs and CPs, under "All Documents," select either "Joint C2 CDD" or "Joint C2 CDPs and CPs."

3. Below is the link located on NIPRNET to reference b and approved CDPs and CPs:
https://intelshare.intelink.gov/sites/ccd/ext/Public%20Requirements%20Documents%20CDD%20CDPs%20CPs/JROCM%20073-13%20Joint%20C2%20CDD%209%20April%202013.pdf.

XXXXXXXXXX

Capability Definition Package (CDP) or

Capability Package (CP)

Joint Staff (JS) J6
Deputy Director, Command and Control Integration (DD C2I)
Combat Capability Developer (CCD) Division

Address

Dissemination Statement:
This document has been approved by J6 for release to
NATO, Australia, Canada, Great Britain, and New Zealand

For Official Use Only – Not for Public Release
Administrative/Operational Use – Date
Other requests for this document shall be referred to:
Name, email, phone number

Capability Definition Package
for
xxxxxx

Submitted by: Date:

Name, GS-xx
Joint Staff J6, Deputy Director C2 Integration
Title

Endorsed by: Date:

Name, GS-15
Joint Staff J6, Deputy Director C2 Integration
Division Chief, Combat Capability Developer (CCD)

Approved by: Date:

Name, SES
Joint Staff J6, Deputy Director C2 Integration

Capability Package
for
xxxxxx

Submitted by: Date:

Name, Grade/Rank
Organization
Title

Endorsed by: Date:

Name, GS-15
Joint Staff J6, Deputy Director C2 Integration
Branch Chief, Combat Capability Developer (CCD)

Approved by: Date:

Name, GS-15
Joint Staff J6, Deputy Director C2 Integration
Division Chief, Combat Capability Developer (CCD)

Table of Contents

Table of Figures

(As Required)

List of Tables

Executive Summary (Less than One Page)

This section provides a synopsis of the required capability. It should include a problem statement, a description of the current capability if one exists, why the proposed capability is needed, the utility it will provide and if it is a specialization and/or variant of the current capability. It should also include a brief discussion of the operational environment driving the requirements and where capability solutions will be employed. An example introductory statement for an Executive Summary is shown below:

> "The Department of Defense (DoD) lacks a capability to provide xxxx.
>
> "This capability need is derived from the Joint Requirements Oversight Council (JROC)-approved *Joint Command and Control (C2) Capability Development Document (CDD)* and operational priorities aligned with the *Joint C2 CDD*. Specifically, this capability is mapped to operational priority #xx as captured in JROC Memorandum (JROCM) xxx-xx, date, and the corresponding Requirements Prioritization and Sequence Plan (RPSP). Additionally, this capability is mapped to required operational activities, operational functions, C2 and data mission services, and C2 core-enabling services derived from joint mission threads (JMT).
>
> "The xxxx Capability Package (CP) describes the xxxx. Proposed development is based on a software-only solution integrated in an enterprise capability xxxx."

1 Purpose

This section provides a succinct, high-level description of the required capability. Discuss why this required capability best meets the warfighter's needs.

2 Scope

This section details the Joint C2 capabilities required to address operational sustainment and/or modernization needs and the requisite background to explain existing systems the capability will augment, improve or replace. If writing a CDP, identify the expected CPs and use cases, if known, satisfying the capability requirement in its entirety via subsequent CP builds.

3 Operational Context

Operational context includes an operational narrative, use cases or a vignette developed in conjunction with the warfighter. It identifies the user and presents an overarching operational scenario describing for Program Managers (PM) and developers how the capability will be used to support Joint C2. It is best understood as an operational narrative describing the environment for intended use to include linkages and dependencies, mechanisms, roles, range of military options, and users involved in performing activities the chosen solution is intended to resolve.

3.1 Operational Information

Given a national security strategy, a supporting military strategy, and defined operational objectives, military actions are approved at the operational level. Detail how the capability impacts Joint C2 at the operational level.

3.2 Tactical Information

As required, show applicability to the tactical arena. An example for tactical-level situational awareness (SA) follows:

"Tactical-level SA feeds the common tactical picture (CTP) and common operational picture (COP); as such, the CTP/COP is only as accurate as the information generated and/or forwarded up-channel from the tactical level. The accuracy and timeliness of CTP/COP information, if retransmitted to other operational and tactical forces, can increase SA and reduce the risk of fratricide."

4 Requirements/Use Cases

This section details requirements developed from capability needs statements contained in the Joint C2 CDD, Net-Enabled Requirements Identification Database (NRID), Integrated Priority Lists (IPL), Joint Urgent Operational Needs (JUON) and other sources under the purview of the CDP/CP authoring organization. The requirements identified through this process and later binned to a CDP/CP are linked to the Joint C2 CDD as parent-child relationships down to the third tier if developing a CP. Additionally, Joint C2 capability gaps have been identified and prioritized to assist in determining annual Operational Priorities providing the demand signal for the Office of the Under Secretary of Defense for Acquisition, Technology & Logistics (OUSD(AT&L))-led Joint C2 Plan/Build and Sustainment and Modernization Plan development processes. Within this section, CDP authors should outline specific operator or system (functional) use cases.

4.1 Operator Use Cases

This section focuses on the specific actors within the system. The intent is to show 1) who the actors are, 2) where they fit within the context of the mission, 3) what information they need, 4) what they do with the information/what function they accomplish, 5) what product(s) they produce and 6) who then uses the products. It may also include stakeholders, who may or may not have direct input into the system.

4.2 Functional Requirements

The following System Requirements Table for XXXX was developed from requirements and capability needs statements contained in the *Joint C2 CDD,*[1] NRID capability needs and other key supporting documents, such as previous CDPs and CPs to include xxxxx. These requirements support, and in some instances, define use cases previously described in Section 3. A full list of pedigree documents is in Appendix B. In the example below, each of the following example Initial Minimum Requirement statements has been linked to the *Joint C2 CDD* and cross-walked to NRID capability needs. The Table 1 requirements listing does not imply the required capabilities are developed within or specifically for xxxxx; however, xxxxx must, at minimum, possess the ability to access and use extant capabilities to satisfy these requirements. Key Performance Parameters (KPP) are delineated in the *Joint C2 CDD*. Related Key System Attributes (KSA) are listed in the CDP. The statements with a tan shaded background were extracted verbatim from the *Joint C2 CDD* or the NRID. The statements with a gray shaded background were derived from the higher-level *Joint C2 CDD*/NRID requirements. The non-shaded statements are the minimum xxxx capabilities extrapolated from and detailed to amplify the higher-level required capabilities.

[1] *Joint C2 CDD*, 9 Apr 2013, JROCM 073-13.

Table 1 XXXX Initial Minimum Requirements

Req ID	**xxxxx Initial Minimum Requirements** **Tan = CDD/NRID Requirement Gray = Derived Requirement White = xxxx Minimum Capability**
CDD 1.1	CDD 1.1 Situational Awareness – The warfighter requires specific capabilities to support situational awareness. These capabilities include: • The ability to monitor, understand, collaborate and share situational awareness with traditional and nontraditional mission partners across various mission sets. • These mission partners include, but are not limited to appropriate US government agencies; foreign governments and their militaries; international organizations (IO); regional organizations (RO); nongovernmental organizations (NGO); state, local and tribal authorities and members of the public and private sectors. • Shared SA by accessing and integrating data/information from authoritative data sources to display a fused, accurate, timely, integrated, and complete battlespace picture. • The ability to tailor dissemination of Shared SA based on the clearance level and role of recipients.
NRID 337	Unclassified COP
NRID 337.1	On an unclassified network, share location/disposition data of DoD/non-DoD organizations supporting Homeland Defense (HLD) and Military Assistance to Civilian Authorities (MACA) missions.
	Example - The xxxx software segment shall share xxxx data across multiple security clearance levels at U.S. and coalition locations in accordance with theater security agreements.
CDD 1.1.1	CDD 1.1.1 Situational Awareness Data The warfighter requires the capabilities to develop situational awareness through timely access to Authoritative Data Sources (at all classification levels) to include: • 1.1.1.1 Position, movement and amplifying data, to include current/future tasking, operational area (OPAREA)/movement area (MOVEAREA) assignment, weapon/weapon system status, communications status • 1.1.1.2 Current and historical position and associated movement data for hostile, neutral, and friendly, including interagency, forces and capabilities of interest, to include air, land, maritime, space and cyberspace, within a user-defined area of responsibility.
NRID xxx	Xxxxxxx
NRID xxx	Xxxxxxx

4.3 KPP linkage

Table 2 Applicable Joint C2 Key Performance Parameters (KPP)

Name	Key Performance Parameter	Initial Minimum
Command and Control - Understand	**1. Information Visualization.** Mission: Provide timely access to and standardized display of relevant information via net-centric services describing the current and predicted operational environments, including PMESII conditions, operationally-relevant nodes and centers of gravity; the location and disposition of friendly, enemy, neutral, and unknown forces; and the plan itself, including the commander's intent and operational approach.	

NR-KPP and interoperability performance requirements will be included as part of the information exchange specification process and are posted to the external CDD website.

Table 3 Net-Ready Key Performance Parameter Attribute Elements

NR-KPP Attribute	Key Performance Parameter	Initial Minimum
Support net-enabled military operations	Mission: Provide C2 planning and force employment information and capabilities in support of joint C2 operations from the NMCS through the JFC.	
Enter and be managed in the network	Network: DISN Data Networks, CENTRIXS and FMN	Defined in Joint C2 requirements
Exchange Information	Information Element: Defined in Joint C2 requirements	Defined in Joint C2 requirements architectures (OV-2, OV-3, OV-5, SV-2 and SV-6)

4.4 KSA development (CDPs only)

This section outlines KSA development. KSAs further define system operational effectiveness and technical performance as required by the program sponsors. KSAs must be measurable, testable, and quantifiable.

4.5 Metrics

This section takes the KSAs from Section 4.4 and decomposes them into Measures of Effectiveness (MOE) and Measures of Performance (MOP). MOEs measure the ability of the capability to accomplish mission objectives and achievement of desired results. MOPs measure the capability's technical performance expressed in quantifiable statistical objectives using ratios, percentages, and quantities. Measures of Suitability (MOS) may also be developed. MOSs are the measure of a capability's ability to be supported in its intended operational environment. MOSs typically relate to readiness or operational availability, reliability, maintainability and the item's support structure such as documentation and training. A capability's interoperability and integration with existing services and systems is an example of an MOS. Measurement metrics will be traceable to the KPPs as required by the *Joint C2 CDD* or KSAs if additional key attributes are needed in lieu of or to support a KPP. Program sponsors will develop metrics based on the recommendations from the CDP/CP developers. CDP/CP developers should ensure metrics are developed with economy, determining the viability and "good enough" effectiveness of a capability.

5 Core-Enabling / Cross-Functional Capabilities

5.1 Cyber Security

Information assurance capabilities will be fielded in accordance with enterprise information environment standards to ensure the security architecture supports future integration of Joint C2 capabilities. This section highlights cyber security needs and threat matrix related to the capability to ensure the right level of information protection is addressed.

5.2 Training and Training Support

The warfighter requires web service modeling and simulation capabilities to establish/reinforce Joint C2 skill sets and training management tools for distributed simulation-based training exercises recording and assessing performance, training metrics, training skill certification/accreditation and scheduling. This section highlights training needs related to the capability for both system administrators and operators.

5.3 Mission Partner Interoperability

The warfighter requires the ability to access and disseminate time-critical information with mission partners (cross-Command/Service/Agency, Multinational, Interagency, and/or Intergovernmental). Interoperability must be leveraged through common standards, protocols (e.g., the National Information Exchange Model (NIEM)) and procedures. The warfighter requires timely, relevant, and secure interoperable capabilities. This section provides the interoperability specifications as well as mission partner specifications.

5.4 Virtual Collaboration (Visualization, Communication & Synchronization)

The warfighter requires capabilities to support a collaborative information environment with both user-to-user, users-to-machine, user-to-virtual, as well as machine-to-machine interaction in synchronous, asynchronous, concurrent and emergent mission environments. The warfighter requires capabilities to assist the supported and supporting staffs in transient and distributed groups with the collaborative management and sharing of information throughout the enterprise. This section provides virtual collaboration (visualization, communication, and synchronization) specifications.

5.5 Information Management/Workflow Management

Within the information management arena, the warfighter requires the capability to 1) collaboratively manage, assess, monitor, execute and adjust plans and operational outcomes in an interdependent enterprise services network to achieve integrated mission operations; 2) support commanders' and their staffs' enterprise information requirements in a disconnected, intermittent connectivity and limited bandwidth (DIL) environment; and 3) process, maintain and deliver data (bi-directional enterprise cross-domain services -- low-to-high) to supported and supporting commanders in a tailorable format to provide relevant critical information to support key decision points. The warfighter requires a workflow management system to 1) manage and define a multiple series of tasks within and across organizational boundaries in accordance with doctrinally-established processes and procedures; 2) allow users to define a unique workflow for tailored jobs or processes based on theater, combatant command (CCMD) or operational need to deviate from a doctrinally established process flow; 3) allow users to develop executable processes with no familiarity with formal programming concepts; 4) support virtual team collaboration with both human-to-human and human to non-person entity as well as machine-to-machine interaction in synchronous, asynchronous, concurrent and emergent environments; and 5) assist the supported and supporting staff members in transient groups with the collaborative management and sharing of information threads throughout the enterprise. This section, as required, also contains cross-domain needs.

5.6 Scalability/Portability

This section provides scalability/portability specifications for the capability.

5.7 Hosting

This section contains information on where the solution will be hosted based upon the need to satisfy DIL operations. The solutions may be hosted locally, regionally, Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC)/Core Data Center, etc.

6 Architectures

The architecture products and data provided in this section of the CDP/CP (Appendix A) define the operational environment and context for capability implementation. Just as the capabilities and requirements of a CDP/CP are a sub-set of those in the supported ICD/CDD, the architectural products of a CPD/CP should be derived from the supported ICD/CDD architectural products with an additional degree of decomposition or granularity. The types of architecture products and data include: 1) operational activities and associated processes, 2) information and data exchanges, 3) appropriate services and systems, and 4) applicable standards and measures of effectiveness/performance/suitability (MOE/MOP/MOS) should clearly inform materiel developers of the required operational capability to be developed. The architectures and other products will align with the capabilities as defined in the Joint C2 CDD operational environment/context and comply with the goals, principles, rules, and standards as defined by the Joint C2 Reference Architecture. The architectural products will be driven by the focus, scope, and complexity of the proposed operational capability, and in compliance with all applicable governing directives/guidance. Consideration should be given to the development of All View, Operational View (OV), and Capability View (CV) products, as needed. Service Views, (SV), Data and Information Viewpoint (DIV), Project Viewpoint (PV), Services Viewpoint (SvcV), and Standard Viewpoint (StdV) should be considered based on their ability to capture system, service, data layers and web and enterprise standard functionality needed to support operational activities. Of particular importance are the annotated Information Exchange Requirements (IERs) within the OVs and DIVs.

7 Data

This section describes the data and information needed (consumed) to achieve the capability described in the CDP/CP. The types of data needs include 1) known authoritative data sources (ADS) planned to be exposed as web services, 2) data needs required but not currently planned for exposure by the data producer or 3) ones not yet provided in any manner by any provider. Interfaces built within the Joint C2 will optimize the exposure of data from recognized ADSs. Data sources are authoritative within operational context (e.g., Joint CA, and JP 3.0 Phases of Military Operations, etc.). C2 ADSs shall be leveraged to indicate what data is currently or projected to be available in time to support the products described by the CDP/CP. Exposed authoritative data sources support a planned capability and are maintained in the CCD's Decision Support Toolkit (DST). All authoritative data sources are registered in the DoD Data and Services Environment (DSE) (https://metadata.ces.mil/dse/).

If the capability is also a producer of authoritative data, as well as a consumer of authoritative data, the CDP/CP must: indicate the data requirement is to register the capability in the DSE by the publication of an operational endpoint; articulate creation of a Web Service Description Language (WSDL) or other web services standards identified and confirmed in the DISR; and identify transparent identity and access management policies and requirements consumers must implement to readily access and use an ADS.

The information exchange requirements needed to achieve the capability described in the CDP/CP will be reviewed for National Information Exchange Model (NIEM) conformance or exception to policy approval from DoD CIO IAW references (f), (o), and (p). All DoD organizations shall first consider NIEM conformance for their information sharing solutions when deciding the data exchange standards or specifications meeting their mission and operational needs. Every effort shall be made to ensure a rigorous analysis of NIEM be conducted as part of this consideration.

Key Data & Services Attributes (KDSA) are characteristics required for all capabilities and all solutions should exhibit. These attributes/characteristics are objective and verifiable and directly support references (q), (p) and (f). Capability solutions exhibiting these characteristics decrease the barriers to data, information, and information technology (IT) service sharing between capabilities, within the department, with our mission partners and between federal agencies. The KDSA's will increase the re-use of data, information, and IT services by warfighters and material developers. Examples of KDSA are: a) non-proprietary interfaces between capability activities, registered in the DSE, and provide policy, process, and technical access instructions; b) structural metadata required to exchange data and information between interfaces is registered in the DSE and compatible with the appropriate standards and specifications.

8 Mission Services

This section includes articulation of operational context-driven capability needs for logical mission and shared/common services from JS J6 CCD's Mission Services list, mapped to the Joint C2 CDD, describing common and mission unique functionalities derived from examining multiple Joint Mission Threads (JMTs) and other capability analysis, related to the CDP/CP as derived. Specifically, this section analyzes and documents functions in the context of "collect, display, process, store, & disseminate" – aligning operational activities to operational functions (information exchanges) to logical C2 Mission Services to C2 data services to C2 Common/Shared Services to leverage Enterprise Services. Inclusion of mission services functionality enables a cleaner description and understanding of specific use cases and user stories; articulation of operational and technical behavior and performance parameters; definition of linkages to enterprise service requirements; and enabling of feedback to refine and improve architectures, common systems functions (e.g., Joint Common Systems Functions List (JCSFL), etc.), requirements documentation and identification of consumer-driven data needs. CDPs/CPs should also indicate capability services are required to be registered once developed in the DSE, per ref (q), to ensure warfighter use and developer re-use. JS J6 CCD Mission Service List can be found at: https://intelshare.intelink.gov/sites/ccd/ext/SitePages/Mission%20Services%20Map.aspx.

9 DOT_LPF Implications

This section articulates the nature of non-materiel (and some materiel) concerns and issues identified in the research and staffing of the CDP/CP.

10 Appendix A – Acronyms

11 Appendix B – Reference

(INTENTIONALLY BLANK)

ENCLOSURE E

REFERENCES

a. CJCSI 3265.01 Series, "Command and Control Governance and Management"

b. JROCM 073-13, 9 April 2013, "Joint Command and Control Capabilities Development Document"

c. JROCM 051-13, 5 March 2013, "Adaptive Planning and Execution (APEX) Initial Capabilities Document (ICD)"

d. JROCM 114-10, 15 July 2010, "Charter for Joint Command and Control (C2) Capability Requirements Governance"

e. JROCM 158-11, 1 December 2011, "Joint Command and Control (Joint C2) Capabilities Development Document (CDD)"

f. DoD CIO Memorandum, 28 March 2013, "Adoption of the National Information Exchange Model within the Department of Defense"

g. Capstone Concept for Joint Operations: Joint Force 2020, 10 September 2010

h. FY 14-18 Defense Planning Guidance (DPG), 11 April 2012

i. Title 10, U.S.C., section 181, "Joint Requirements Oversight Council"

j. CJCSI 3170.01 Series, "Joint Capabilities Integration and Development System"

k. JCIDS Manual, 19 January 2012, "Manual for the Operation of the Joint Capabilities Integration and Development System," NIPRNET at https://www.intelink.gov/wiki/JCIDS_Manual; SIPRNET at http://www.intelink.sgov.gov/wiki/JCIDS_Manual

l. CJCSI 6285.01 Series, "Multinational and Other Mission Partner (MNMP) Information Sharing Requirements Management Process"

SUPPORTING DOCUMENTATION

CJCSI 5123.01 Series, "Charter of the Joint Requirements Oversight Council"

JROCM 008-08, 14 January 2008, "Leveraging Technology Evolution for Information Technology System"

Minutes of the 25 June 2010 Command and Control (C2) Joint Capabilities Board, 25 June 2010

Joint Command and Control (C2) Capability Development Document (CDD), Version 1.4, 9 April 2013

JSI 5711.01E, 24 May 2013, "Action Processing"

DJ-6 memorandum, 12 April 2013, "DoD Adoption of the National Information Exchange Model (NIEM) and establishment of the NIEM Military Operations Domain"

DoDI 8320.02, 5 August 2013, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense"

GLOSSARY

PART I - ABBREVIATIONS AND ACRONYMS

ADS	Authoritative Data Sources
AFROC	Air Force Requirements Oversight Council
AROC	Army Requirements Oversight Council
C2	Command and Control
C2I	Command and Control Integration
C4	Command, Control, Communications, and Computers
CA	Capability Area
CCD	Combat Capability Developer
CCMD	Combatant Command
CD	Capability Drop
CDD	Capability Development Document
CDP	Capability Definition Package
CENTRIXS	Combined Enterprise Regional Information Exchange System
CGA	Capability Gap Assessment
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJCSM	Chairman, Joint Chiefs of Staff Manual
CN	Capability Need
CNWG	Capability Needs Working Group
CoC	Council of Colonels
CP	Capability Package
CR	Change Request
C/S/A	Combatant Commands, Services, and Agencies
DDC2I	Deputy Director Command and Control Integration
DIV	Data and Information Viewpoint
DJ-6	Director for Command, Control, Communications, Computers, and Cyber
DoD	Department of Defense
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy
DSD	Data and Services Division
DSE	Data and Services Environment
DST	Decision Support Toolkit
ESC	Executive Steering Council
FCB	Functional Capabilities Board
FoP	Family of Programs
FY	Fiscal Year

FYDP	Future Years Defense Program
IAW	In Accordance With
IER	Information Exchange Requirements
IPL	Integrated Priority List
IT	Information Technology
JCB	Joint Capabilities Board
JCIDS	Joint Capabilities Integration and Development System
JFC	Joint Force Commander
JMT	Joint Mission Thread
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JS	Joint Staff
JSAP	Joint Staff Action Processing
JSI	Joint Staff Instruction
JTF	Joint Task Force
KPP	Key Performance Parameter
KSA	Key System Attribute
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOS	Measure of Suitability
MPE	Mission Partner Environment
MROC	Marine Requirements Oversight Council
NGB	National Guard Bureau
NIPRNET	Non-Classified Internet Protocol Router Network
NMCS	National Military Command System
NROC	Navy Requirements Oversight Council
NRID	Net-Enabled Requirements Identification Database
ORA	Operational Risk Assessment
OSD	Office of the Secretary of Defense
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
OV	Operational View
PM	Program Manager
PM-CESG	Program Manager-Chief Engineer Steering Group
PR	Problem Report
PSA	Principal Staff Assistant
RDP	Requirements Definition Package
RMD	Resource Management Directives

RPSP	Requirements Prioritization and Sequencing Plan
SA	Situational Awareness
SIPRNET	Secure Internet Protocol Router Network
SME	Subject Matter Expert
SMP	Sustainment and Modernization Plan
SMPP	Sustainment and Modernization Planning Process
SRS	System/Software Requirements Specifications
SSG	Senior Steering Group
SSG-A	Senior Steering Group for Acquisition
WG	Working Group

GLOSSARY

PART II – TERMS AND DEFINITIONS

capability need (CN) -- a NRID input from the operational user.

change requests (CR) -- CRs address changes to existing functions to enhance or provide additional capability. CRs are assessed and processed via the NRID.

modernization -- The migration of the existing Joint and Service C2 systems to an agile, joint C2 FoP environment.

Net-Enabled Requirements Identification Database (NRID) -- The NRID is the primary mechanism used by JS and C/S/As to submit CNs. Inputs to the NRID require O-6 level approval/endorsement before they may be submitted. The NRID is located on SIPRNET at https://intelshare.intelink.sgov.gov/sites/nrid for classified inputs. Unclassified NRID inputs are located on the NIPRNET at https://intelshare.intelink.gov/sites/ccd/ds/NRID-U. The NRID allows the warfighter to submit and track the status of CNs throughout the Joint C2 requirements / capability development lifecycle. The NRID will evolve to ensure congruency with other Joint Staff, C/S/A requirements management systems to the maximum extent feasible.

problem report (PR) -- A PR addresses problems with existing functionality not meeting the capability requirements they were designed to meet. Generally, PRs are not entered into the NRID but processed via the JS Support Center Help Desk for issue correction. When a PR represents a CN or correction of an issue requiring additional unique development beyond the current program scope, a CR should be entered into the NRID.

requirement -- A capability required to meet an organization's roles, functions, and missions in current or future operations.

sustainment -- This includes the process, procedures, people, materiel, and information required to operate, support, and maintain currently deployed C2 systems.

synchronization -- The process of modifying currently deployed C2 systems to adapt to a changed environment (e.g., hardware/software compatibility, interoperability), correct deficiencies, or adjust for and align to dependencies upon other systems/capabilities.

warfighters -- Warfighters are organizations or individuals who use C2 to oversee, conduct, and support warfighting activities. In the context of this manual, principal users are the Joint Staff, C/S/As, and NGB.

(INTENTIONALLY BLANK)