MANUAL FOR THE OPERATION OF THE JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM (JCIDS)

References: See Enclosure H.

1. Purpose

a. This manual is not intended to stand alone – readers are encouraged to become familiar with the Joint Requirements Oversight Council (JROC) Charter and the JCIDS Instruction, references a and b, before reviewing this manual.

b. This manual augments references a and b with detailed guidelines and procedures for the JCIDS process, and interactions with several other departmental processes to facilitate robust capability requirement portfolio management, and the timely and cost effective development of capability solutions for the warfighter.

c. This manual provides information regarding activities including mandatory training for personnel involved in the requirements processes, capability requirement portfolio management, identification of capability requirements and associated capability gaps, development of capability requirement documents, gatekeeping, and staffing procedures.

2. Cancellation. The JCIDS Manual, 19 January 2012, "Manual for the Operation of the Joint Capabilities Integration and Development System," is hereby cancelled, along with any alternative/interim/optional document formats previously authorized for use.

3. Applicability. This manual applies to the Joint Staff, Services, Combatant Commands (CCMDs), and other DOD Components.

4. Procedures. This manual provides procedural guidance for the overall JCIDS process as well as other requirements-related processes and activities.

a. The JROC is implemented by reference a, to satisfy the statutory responsibilities shown in Figure 1. Reference a also outlines the structure of the JROC's subordinate boards, and identifies other organizations involved in JROC activities.

b. The JCIDS process is established by reference b as the primary means for the JROC to fulfill its statutory responsibilities to the Chairman of the Joint Chiefs of Staff (CJCS) shown in Figure 1. The JCIDS process activities described in reference b and this manual are based upon the JROC structures and organizations described in reference a.

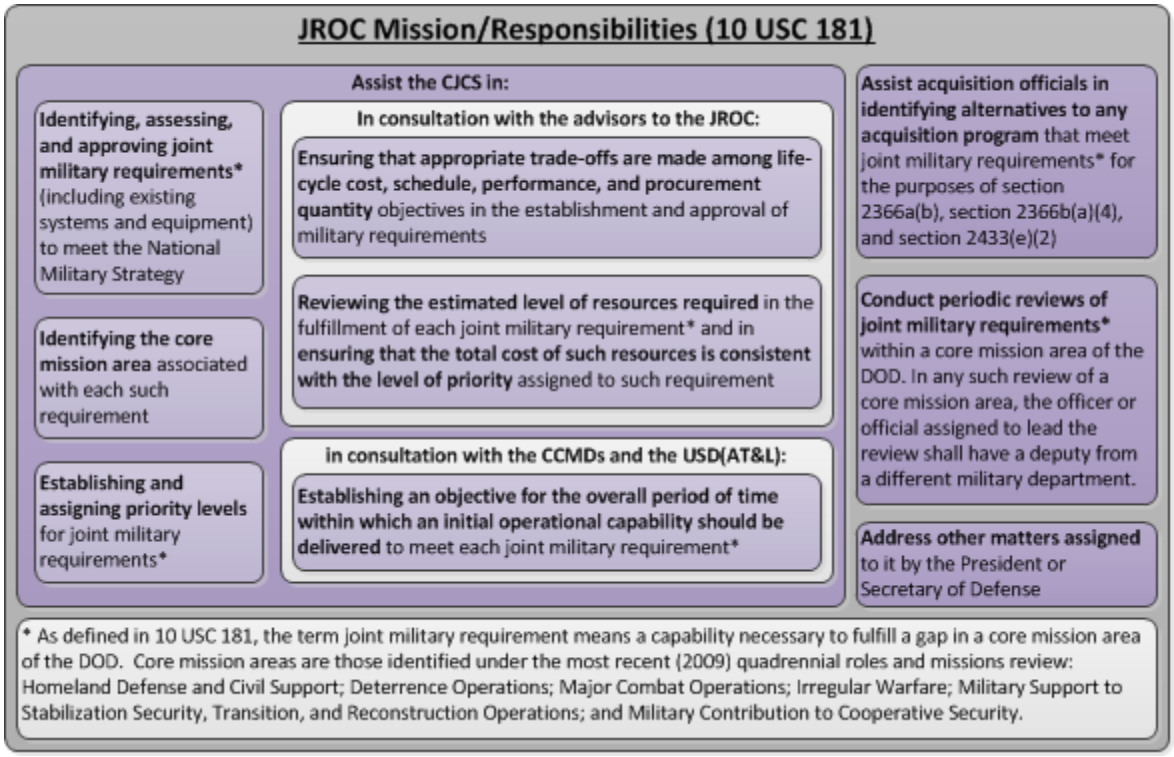

Figure 1. JROC Title 10 Responsibilities

(1) The description of the JCIDS process in reference b provides a high level overview of the detailed information contained in this manual, which is organized into logical subsections shown in Figure 2.

(2) Reference c provides Uniform Resource Locators (URLs) for the JCIDS Wiki sites. In addition to other process-related information, the wiki sites include errata identified between official releases of the JCIDS Manual and points of contact (POCs) for suggesting future refinements to the JCIDS process or identifying additional errata.

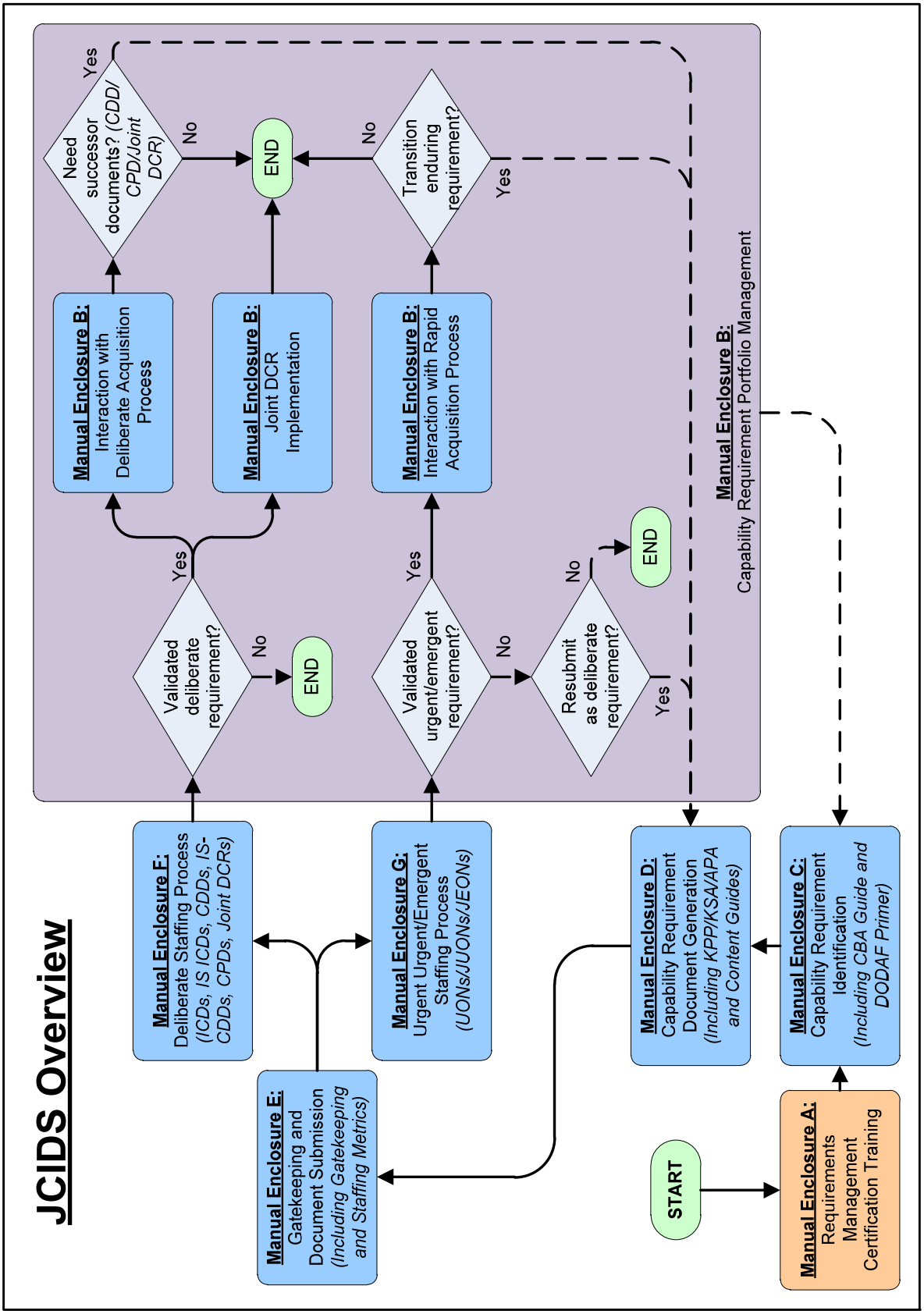

Figure 2. Overview of JCIDS Process and JCIDS Manual Enclosures

c. Requirements Training and Portfolio Management

(1) Enclosure A outlines mandated training for personnel involved in the requirements processes.

(2) Enclosure B provides detail of capability requirement portfolio management activities performed by the Functional Capabilities Boards (FCBs) and other stakeholders. An outline of the Capability-Mission Lattice (CML) is provided as an integrating construct for identification of capability requirements, and maintaining traceability to strategic guidance, missions of the joint force, Service and joint concepts, Concepts of Operations (CONOPS), and other departmental activities involved in developing and sustaining capability solutions. This enclosure also discusses the critical interaction between capability requirements validated in JCIDS and implementation of non-materiel capability solutions, deliberate and rapid acquisition activities conducted through the Defense Acquisition System (DAS), and other DOD processes.

d. Capability Requirement Identification and Document Generation

(1) Enclosure C outlines the various processes which capability requirement Sponsors use to identify their capability requirements, associated capability gaps, and proposed materiel and non-materiel capability solutions for submission into the JCIDS process for review and validation. The enclosure also includes discussion of Capabilities-Based Assessments (CBAs) and other studies, as well as means for notifying stakeholders of study initiation and posting of study results and related data.

(2) Enclosure D outlines the different capability requirement documents which are used to articulate capability requirements, associated capability gaps, and other related data for initial review and validation, as well as to provide more refined capability requirements related to specific materiel and non-materiel capability solutions for review and validation. The enclosure also includes detailed content guides for the mandatory Key Performance Parameters (KPPs), and other sections of documents which require more in-depth discussion.

e. Document Staffing and Validation

(1) Enclosure E outlines the gatekeeping processes for all incoming capability requirement documents prior to deliberate or expedited staffing and validation.

(2) JCIDS staffing is adaptable depending upon the timeliness of the operational requirement, as shown in Figure 3.

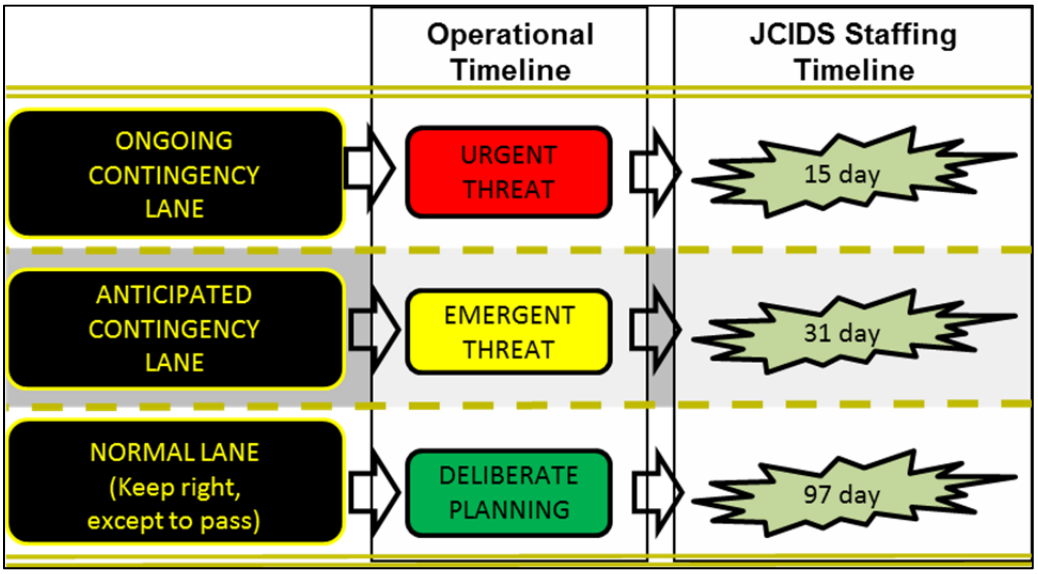

Figure 3. Three JCIDS Process Lanes

(a) Enclosure F outlines the deliberate staffing process used for the review and validation of the majority of capability requirements, associated capability gaps, and proposed materiel and non-materiel capability solutions, ensuring appropriate rigor and assessment by a wide range of stakeholders across DOD. This enclosure also provides guides for certifications and endorsements required during staffing of capability requirement documents.

(b) Enclosure G outlines the urgent/emergent staffing process for expedited review and validation of urgent or emergent capability requirements, and associated capability gaps, which if unmitigated would result in unacceptable loss of life or critical mission failure in ongoing or anticipated contingency operations. Use of these expedited processes is only appropriate when the deliberate process cannot be tailored to address the capability requirements in a timely fashion.

f. Requests for exceptions or variances to reference b or the document formats and processes described in this manual must be directed to the Joint Staff Gatekeeper.

(1) The Joint Staff Gatekeeper will work in coordination with the document Sponsor and the appropriate FCB(s) to ensure any exceptions or variances meet the needs of the validation authority while allowing for appropriate flexibility in the capability requirements process.

(2) Waivers granted by the Joint Staff Gatekeeper shall be documented in memo format, and attached to associated documents in the KM/DS system to provide traceability in future staffing and validation activities.

5. Summary of Major Changes

a. Streamlines capability requirement document formats providing more logical flow within each document, enhancing consistency between document types, and clarifying intent for each document section through a "purpose" subparagraph in the guidance. As modified in this revision of the JCIDS Manual, the July 2012 alternate/optional document formats are adopted as the baseline document formats.

b. Adds Content and Certification Guides for Intelligence Supportability as partial consolidation of CJCS Instruction (CJCSI) 3312.01B. Remaining content from CJCSI 3312.01B related to roles and responsibilities is consolidated into CJCSI 5123.01G. These changes also incorporate the proposed revisions in the draft CJCSI 3312.01C.

c. Adds a Certification Guide for the Net-Ready KPP (NR KPP) and expands the Content Guide for the NR KPP with the majority of the content from CJCSI 6212.01F. Remaining content from CJCSI 6212.01F related to roles and responsibilities is consolidated into CJCSI 5123.01G.

d. Introduces a content guide for weapon safety assurance, and updates the guide to the Weapon Safety Endorsement (WSE) to reflect the consolidation of the Joint Weapon Safety Technical Advisory Panel (JWSTAP) Charter into CJCSI 5123.01G.

e. Introduces the CML as an integrating construct to ensure traceability to strategic guidance, missions of the joint force, Service and joint concepts, CONOPS, and other departmental activities – both in the identification of capability requirements and their associated capability gaps, and for capability requirement portfolio management.

f. Reorganizes the CBA Guide for more logical flow, incorporates applicable DOD Architecture Framework (DODAF) data and views in the CBA discussion, and adds a DODAF Primer in a new appendix.

g. Changes the values associated with operational attributes in Initial Capabilities Documents (ICDs) from "Minimum Values," implying no operational utility below the specified value, to "Initial Objective Values, with associated operational context," allowing more robust follow-on analysis and trade-off decisions.

h. Adds Science and Technology (S&T) content to ICD recommendations section, and in capability requirement portfolio management, to facilitate greater leverage of innovative technologies and prioritization of S&T efforts.

i. Clarifies intent of setting and changing quantities in Capability Development Documents (CDDs), Capability Production Documents (CPDs), Joint Urgent Operational Needs (JUONs), Joint Emergent Operational Needs (JEONs), and DOD Component Urgent Operational Needs (UONs).

j. Clarifies scope limitations for the Information Technology (IT)-Box construct used in Information Systems ICDs (IS-ICDs) and Information Systems CDDs (IS-CDDs).

k. Clarifies that Technology and Manufacturing readiness assessments in CDDs and CPDs must include discussion of how (or if) workarounds or flexibility are available for high risk areas to allow the program to continue in the event that risks are realized.

l. Deletes the requirement to document alternatives considered in preparing Joint Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P) Change Recommendation (DCRs), as these should be documented in the CBA or other studies or analyses, and not required in the document itself.

m. Aligns affordability paragraphs of capability requirement documents with affordability information required for following acquisition decision points, ensuring JCIDS and DAS processes consider cost, performance, schedule, and quantity trades from similar baselines.

n. Adds a validation page behind the cover page of each capability requirement document, ensuring that validated documents – new or updated – will have authoritative validation memos attached.

o. Splits the table of required DODAF views in the NR KPP Content Guide, moving DODAF views required for all documents to a new table in general document guidance, and streamlining the NR KPP guidance to only those DODAF views applicable to NR KPP evaluation.

p. Adds a Content Guide for DOTmLPF-P, and moves non-materiel Training related requirements content in CDDs and CPDs from the Training KPP to the DOTmLPF-P section.

q. Renames the mandatory Survivability KPP to System Survivability KPP to clarify the distinction between this KPP and aspects of human “survivability” addressed in the mandatory Force Protection KPP.

r. Eliminates the Joint Staffing Designator (JSD) of Independent, while retaining specified DOD Component validation authority and discretion over certifications and endorsements.

s. Clarifies cases where the Joint Staff Gatekeeper may reject capability requirement documents submitted for staffing, if documents are incomplete and do not enable substantive discussion of the capability requirements and associated tradeoffs in life cycle cost, schedule, performance, and procurement quantities in the setting of capability requirements.

t. Clarifies that reviews of capability requirements, individually or as part of capability requirement portfolio management, will include access, by properly cleared individuals, to all data relevant to the reviews, ensuring robust assessments of the entirety of the capability requirement portfolios.

u. Introduces common Gatekeeping between JCIDS and the requirements validation aspects in the process for acquisition of Defense Business Systems (DBS), ensuring visibility and ability for Joint Capabilities Board (JCB) or JROC to review DBS when appropriate.

v. Expands Gatekeeping and Staffing section guidance to ensure greater stakeholder understanding of expectations and roles in the process.

w. Clarifies that the JCB and JROC typically delegate authority to the Sponsor to make non-KPP changes after validation, but retain change authorities when required.

x. Highlights flexibilities and encouragement for a Sponsor, in coordination with the Milestone Decision Authority (MDA), to request KPP or other capability requirements changes due to knowledge gained during the acquisition process, ensuring cost, performance, schedule, and quantity trades are maintained in the best interest of the joint force.

y. Reorganizes post-validation processes and prioritization enclosures into a single Capability Requirement Portfolio Management enclosure, including further clarification of Integrated Priority List (IPL)/Capability Gap Assessment (CGA) activities and how capability requirements inform and are informed by activities under the Joint Strategic Planning System (JSPS).

z. Updates the JROC/JCB Tripwire review process to better articulate the monitoring of ongoing acquisition programs. A new figure is provided to clarify the overall JROC/JCB Tripwire review process.

aa. Deletes reference to the Capabilities Development Tracking and Management tool due to its retirement.

6. Releasability. This manual is approved for public release; distribution is unlimited.

7. Effective Date. This manual is effective upon promulgation.

INDEX

A REQUIREMENTS MANAGEMENT CERTIFICATION TRAINING A-1

Overview A-1
Training Mandate A-1
Certification Levels A-1
RMCT Management and Reporting..... ..... A-2
Component Appointed Representatives and Functional Integrated Process Team Representatives A-2
Requirements Workforce Status Reports A-3
Training Courses A-3
Core Courses A-4
CLR 101 – Introduction to JCIDS A-4
RQM 110 – Core Concepts for Requirements Management A-4
RQM 310 – Advanced Concepts and Skills for Requirements Managers. A-4
RQM 403 – Requirements Executive Overview Workshop A-4
RQM 413 – Senior Leader Requirements Course A-5
Core Plus Courses A-5
CLR 151 – Analysis of Alternatives A-5
CLR 250 – Capabilities Based Assessment A-5
CLR 252 – Key Performance Parameters A-5
Course Attendance Guidelines A-5
Resident Course Attendance A-6
Pre-course Work A-6
Walk-in Students A-6
Course No-shows A-7
Short Notice Cancellations A-7
Course Failures A-7
Additional Academic Policies A-8

B CAPABILITY REQUIREMENT PORTFOLIO MANAGEMENT B-1

Overview B-1
Purpose B-1
Capability Requirement Portfolios B-1
Capability-Mission Lattice B-4
Strategic Guidance B-6
Planning/Operations B-6
Global Context and Threats/Intelligence B-7
Capability Requirements B-8
Materiel and Non-Materiel Capability Solutions B-8
Budgets/Funding B-9
Portfolio Management Tools B-9
Portfolio Reassessments B-10

Executing Capability Requirement Portfolio Management B-10
Periodic Reviews B-11
Capability Gap Assessment B-11
Munition Requirements Process B-11
Program and Budget Review B-12
Other Capability Requirement Portfolio Assessments B-15
Interactions with the Joint Strategic Planning System B-16
Comprehensive Joint Assessment B-16
Joint Strategy Review B-16
Joint Intelligence Estimate B-16
Joint Concept Development B-16
Joint Logistics Estimate B-16
Joint Personnel Estimate B-16
Chairman's Risk Assessment B-17
Operational Availability Studies B-17
Continuous Assessment Processes under JSPS B-17
Joint Combat Capability Assessment B-17
Chairman's Readiness System B-17
Global Force Management B-17
Chairman's Advice and Direction B-18
Chairman's Program Recommendation B-18
Chairman's Program Assessment B-18
National Military Strategy B-18
Joint Strategic Capabilities Plan B-19
Joint DCR Implementation B-19
Implementation Plan Refinement B-19
Implementation Progress Monitoring B-20
Documenting Joint DCR Completion B-20
Interaction with Deliberate Acquisition Activities B-20
Overview of Deliberate Acquisition B-20
Planned Requirement Reviews B-20
ICD Validation B-21
Post-AoA (or Similar Study) Review B-21
CDD Validation B-22
CPD Validation B-23
Event Driven Requirement Reviews B-24
Changes to Validated Capability Requirements B-24
JROC/JCB Tripwire Reviews B-24
Critical Intelligence Parameter Breach Review B-26
Nunn-McCurdy Unit Cost Breach Review B-27
Major Automated information System Critical Change Review B-27
Upgrades and End of Service Life Decisions B-27
Interaction with Rapid Acquisition Activities B-29
Overview of Rapid Acquisition B-29
Periodic and Transition Review of Urgent and Emergent

Capability Requirements B-30

Appendix A – Capability Gap Assessment B-A-1
Introduction B-A-1
Inputs to the CGA Process B-A-2
Synthesis of CGA Inputs B-A-3
Stratification of Capability Gaps B-A-3
Outputs of the CGA B-A-4

C INITIAL IDENTIFICATION OF CAPABILITY REQUIREMENTS AND ASSOCIATED CAPABILITY GAPS C-1

Overview C-1
Fundamental Goal C-1
Use of Certified Requirements Managers C-1
Relation to Functions, Roles, Missions, and Operations C-1
Leverage of Prior Efforts C-2
Approaches to Identifying Capability Requirements C-2
Considerations C-2
Solution Independence C-3
Primary Types of Approaches C-3
CBAs and Other Studies C-3
Operational Planning C-5
Exercise/Warfighting Lessons Learned C-6
Joint Capability Technology Demonstrations and Other Experiments C-7
Transition of Rapidly Fielded Capability Solutions C-7
Business Process Reengineering C-8
Determination of Appropriate JCIDS Action C-9
Issues not Requiring JCIDS Action C-9
Issues Requiring JCIDS Action C-9
Documentation of Studies/Analyses and Associated Data C-11
Purpose C-11
Submission of Studies and Associated Data C-12
Study Initiation Notices C-12

Appendix A – Example Operational Attributes C-A-1
Purpose C-A-1
JCA Specific Examples C-A-1

Appendix B – Capabilities Based Assessment Guide C-B-1
Overview C-B-1
Purpose C-B-1
Traceability C-B-1
Level of Rigor C-B-2
Additional Guidance C-B-2

CBA Process Steps C-B-3
Study Initiation Notice C-B-3
CBA Focus C-B-3
Strategic Context C-B-3
Missions and Scenarios C-B-3
Joint Lessons Learned C-B-3
Use of DODAF Views C-B-3
Operational Context C-B-5
Timeframe C-B-5
Threats C-B-6
Concepts and CONOPS C-B-7
Identification of Operational Tasks C-B-8
Level of Detail C-B-9
Capability Requirement and Capability Gap Identification .. C-B-9
Risk Assessment C-B-11
Non-materiel Approaches C-B-12
Materiel Approaches C-B-14
Documentation C-B-14

Appendix C – DOD Architecture Primer C-C-1
Introduction C-C-1
Architecture Products C-C-1
Architecture Discovery and Accessibility C-C-8
Architecture Discovery C-C-8
Use of Enterprise Services C-C-8
Architecture Repository Types C-C-9
Accessibility of Architectures C-C-10
Warfighter Mission Area - Architecture Federation and Integration Portal C-C-10

D CAPABILITY REQUIREMENT DOCUMENT GENERATION D-1

General Document Guidance D-1
Purpose D-1
Coordination of Intelligence Community Capability Requirement Documents D-1
Coordination of DBS Problem Statement and Business Case Documents D-2
Types of Capability Requirement Documents D-2
ICD (includes the IS-ICD variant) D-2
DCR D-2
CDD (includes the IS-CDD variant) D-2
CPD D-3
JUON, JEON, and DOD Component UON D-3
Limitation on IS-ICD and IS-CDD Variants D-3
Support to the Acquisition Process D-3

Deliberate Acquisition D-3
ICD Validation..... D-4
Post-AoA (or Similar Study) Review..... D-4
CDD Validation D-4
CPD Validation..... D-6
Rapid Acquisition D-7
Document Sequences and Variations..... D-7
Capability Requirement Document Updates/Revisions D-11
Situations Not Requiring New Capability Requirement Documents.....D-13
Precedence of Recommended Approaches D-14
Required DODAF Views D-14
Formatting Standards D-15
Classification and Releasability D-16
Initial Capabilities Document D-17
Background D-17
Format D-17
Cover Page D-17
Validation Page D-18
Executive Summary D-18
Document Body.....D-19
Operational Context D-19
Threat Summary D-20
Capability Requirements and Gaps/Overlaps D-21
Assessment of Non-Materiel Approaches.....D-25
Final Recommendations D-25
Appendices.....D-27
Information Systems – Initial Capabilities Document D-29
Background D-29
Format Changes.....D-31
Cover Page D-31
Validation Page D-31
Executive Summary D-32
Differences from ICD in Document Body.....D-32
Capability Requirements and Gaps/Overlaps D-32
Final Recommendations D-32
Appendices.....D-33
Example of Managing an IS Program Using the IT Box Construct from an IS-ICD or IS-CDD D-33
Joint DOTmLPF-P Change Recommendation D-37
Background D-37
Format D-38
Cover Page D-38
Validation Page D-38
Executive Summary D-39
Document Body.....D-39

DRAFT

Operational Context D-39
Threat Summary D-40
Capability Discussion D-41
Change Recommendations D-42
Implementation Plans D-43
Appendices D-45
Capability Development Document D-47
Background D-47
Format D-47
Cover Page D-47
Validation Page D-48
Executive Summary D-49
Document Body D-49
Operational Context D-49
Threat Summary D-50
Capability Discussion D-51
Program Summary D-53
Development KPPs, KSAs, and APAs D-54
Other System Attributes D-56
Spectrum Requirements D-57
Intelligence Supportability D-57
Weapon Safety Assurance D-58
Technology Readiness D-58
DOTmLPF-P Considerations D-59
Program Affordability D-60
Appendices D-62
Information Systems – Capability Development Document D-63
Background D-63
Format Changes D-64
Cover Page D-64
Validation Page D-64
Executive Summary D-65
Differences from CDD in Document Body D-65
Program Summary D-65
Development KPPs, KSAs, and APAs D-65
Program Affordability D-65
Appendices D-66
Capability Production Document D-67
Background D-67
Format D-67
Cover Page D-67
Validation Page D-68
Executive Summary D-69
Document Body D-69
Operational Context D-69
Threat Summary D-70

DRAFT

Capability Discussion D-71
Program Summary D-73
Production KPPs, KSAs, and APAs D-74
Other System Attributes D-76
Spectrum Requirements D-77
Intelligence Supportability D-78
Weapon Safety Assurance D-78
Manufacturing Readiness D-78
DOTmLPF-P Considerations D-79
Program Affordability D-80
Appendices D-82
Joint Urgent Operational Need, Joint Emergent Operational Need, and DOD Component UON D-84
Background D-84
Format D-85
Document Body D-85
Administrative Data D-85
Operational Context and Threat Analysis D-86
Required Capability D-86
Flexibility D-86
Potential Non-Materiel Capability Solutions D-86
Potential Materiel Capability Solutions D-86
Required Quantities D-87
Constraints D-87

Appendix A – Development of Key Performance Parameters, Key System Attributes, and Additional Performance Attributes D-A-1
Overview D-A-1
KPPs D-A-1
KSAs D-A-1
APAa D-A-1
Threshold and Objective Values D-A-1
Designating Measures of Performance D-A-1
Tradespace D-A-2
Mandatory KPPs D-A-2
Force Protection KPP D-A-2
System Survivability KPP D-A-2
Sustainment KPP D-A-3
Net-Ready KPP D-A-3
Energy KPP D-A-3
Training KPP D-A-4
Required Certification or Endorsement of Mandatory KPPs D-A-4
Waiving Mandatory KPPs D-A-4
CONOPS Update and/or OMS/MP Documentation D-A-5
Additional Data Required D-A-5
Data Submission D-A-5

Follow-on Usage D-A-5
Development of KPPs, KSAs, and APAs D-A-5
Initial Questions D-A-6
KPP Change Authority D-A-7
Test and Evaluation Considerations D-A-7
Example Development Methodology D-A-7
Refinement of Threshold and Objective Values D-A-8
Requesting KPP Relief D-A-11
Changing Context over Time D-A-11
Budgetary Considerations D-A-11
Potential KPP, KSA, or APA Performance Attributes D-A-11
Command and Control D-A-12
Battlespace Awareness D-A-13
Fires D-A-16
Movement and Maneuver D-A-17
Protection D-A-18
Sustainment D-A-18

Appendix B – Content Guide for the Force Protection KPP D-B-1
Overview D-B-1
Purpose D-B-1
Synergy/Overlap with System Survivability KPP D-B-1
Exclusion of Offensive Capabilities D-B-1
Tailoring of Standards D-B-1
Force Protection Attributes D-B-1
Protection from Kinetic Fires D-B-1
Protection from Non-kinetic Fires (other than CBRN) D-B-2
Protection from CBRN Effects D-B-2
Protection from Environmental Effects D-B-2
Protection from Crash Events D-B-3
Proponent D-B-3

Appendix C – Content Guide for the System Survivability KPP D-C-1
Overview D-C-1
Purpose D-C-1
Synergy/Overlap with Force Protection KPP D-C-1
Exclusion of Offensive Capabilities D-C-2
Tailoring of Standards D-C-2
Potential Attributes or Considerations D-C-2
For Reduced Probability of Hit D-C-2
For Reduced Vulnerability if Hit D-C-2
For Increased Resiliency of the Force D-C-3
Proponent D-C-4

Appendix D – Content Guide for the Sustainment KPP D-D-1
Introduction D-D-1

Purpose D-D-1
Sustainment as a Key Component of Performance D-D-1
Value D-D-1
Background D-D-1
Overview of the Sustainment KPP Development D-D-1
Derivation of the Sustainment KPP D-D-2
Operational Framework D-D-2
Elements of the Sustainment KPP D-D-2
Materiel Availability and Operational Availability D-D-2
Reliability KSA D-D-3
O&S Cost KSA D-D-4
Sustainment KPP for Complex Systems D-D-5
Documentation D-D-5
Development Guide D-D-5
Proponent D-D-5

Appendix E – Content Guide for the Net-Ready KPP D-E-1
Overview D-E-1
Usage D-E-1
Purpose D-E-1
Summary D-E-2
Attribute Characteristics D-E-3
Support Military Operations D-E-3
Entered and Managed on the Network D-E-3
Effective Information Exchanges D-E-4
NR KPP Summary Table D-E-4
Platform Integration Information Table Alternative D-E-5
NR KPP Functions D-E-7
Requirements D-E-7
Information Exchanges D-E-7
MOEs and MOPs D-E-7
Interoperability Issues D-E-7
Compliance D-E-8
Spectrum Requirements D-E-8
NR KPP Development D-E-8
Primary Questions D-E-8
NR KPP Example D-E-8
NR KPP Architecture Development Methodology D-E-9
Background D-E-11
DODAF Use for NR KPP D-E-11
Architecture Tools D-E-12
Submitting Architectures D-E-12
DOD IEA Alignment D-E-13
Architecture Alignment D-E-13
Activity Models D-E-13
NR KPP Information and Architecture Views D-E-13

DRAFT

Proponent D-E-13

Appendix F – Content Guide for the Energy KPP D-F-1
Introduction D-F-1
Purpose D-F-1
Operational Implications of Energy D-F-1
Applicability D-F-2
Energy Supportability Analysis D-F-2
General Considerations D-F-2
Three Part Methodology D-F-3
Energy Performance Attributes D-F-6
Categories of Systems D-F-6
Provider Systems D-F-6
Receiver Systems D-F-7
Drop-in/Bolt-on Systems D-F-7
Relationship with Other Performance Attributes D-F-8
Testability D-F-8
Proponent D-F-8

Appendix G – Content Guide for the Training KPP D-G-1
Overview D-G-1
Purpose D-G-1
Applicability D-G-1
Situations Requiring Training KPP Content D-G-1
Specific Materiel Performance Requirements D-G-1
Mission of the System is Training D-G-1
Proponent D-G-2

Appendix H – Content Guide for DOTmLPF-P D-H-1
Overview D-H-1
Purpose D-H-1
Usage D-H-1
Applicability D-H-1
Coordination with Other Processes D-H-1
Section Content D-H-1
Doctrine D-H-1
Organization D-H-2
Training D-H-2
“Little-m” Materiel D-H-4
Leadership and Education D-H-4
Personnel D-H-5
Facilities D-H-5
Policy D-H-5
Proponent D-H-5

Appendix I – Content Guide for Intelligence Supportability D-I-1

Overview D-I-1
Purpose D-I-1
Review D-I-1
Certification D-I-1
Category Descriptions D-I-1
Intelligence Manpower Support D-I-1
Intelligence Resource Support D-I-2
Intelligence Planning and Operations Support D-I-2
Planning and Direction D-I-2
Collection D-I-3
Processing and Exploitation D-I-5
Analysis and Production D-I-6
Dissemination and Integration D-I-6
Evaluation and Feedback D-I-7
Targeting Support D-I-7
Intelligence Mission Data Support D-I-9
Warning Support D-I-10
Space Intelligence Support D-I-11
Counterintelligence Support D-I-11
Intelligence Training Support D-I-11
Document Content Guidance D-I-12
General D-I-12
CDD and CPD Content D-I-13

Appendix J – Content Guide for Weapon Safety D-J-1
Overview D-J-1
Purpose D-J-1
Designation of Weapons as Joint Systems D-J-1
Tailoring of Weapon Safety Requirements D-J-1
Baseline Weapon Safety Requirements D-J-1
System Safety D-J-2
Insensitive Munitions D-J-2
Fuze Safety D-J-2
Explosive Ordnance Disposal D-J-2
Laser Safety D-J-2
E3 Ordnance Safety D-J-2
Weapon Packing, Handling, Storage, and Transportation D-J-2
Other Considerations D-J-2
Proponent D-J-3

E GATEKEEPING E-1

Joint Staff Gatekeeper E-1
Purpose E-1
IC Common Gatekeeping E-1
DBS Common Gatekeeping E-1

DRAFT

Sponsor Organization Gatekeepers E-1
Additional Activities E-1
Managing Submissions with Special Protections E-1
Monitoring of Validated JUONs and JEONs E-2
Managing the KM/DS System E-2
Generating JCIDS Process Metrics E-2
Document Submission Guidance E-2
Staffing Process and Validation Authority Determination E-2
Use of DOD Component Gatekeepers E-3
Recommendation for Parallel Staffing E-3
Document and Data Submission E-3
Classified SECRET and Below E-4
Classified Above SECRET E-4
Protected by SAP/SAR Designation E-4
Protected by ACCM Designation E-5
Sequence for Document Submissions E-5
ICD or CDD Waiver Requests E-6
Other Format or Process Waiver Requests E-6
Joint Staff Gatekeeper Activities E-7
Initial Review E-7
Actions for ICDs, CDDs, CPDs, and Joint DCRs E-8
FCB Assignment E-8
JSD Assignment E-8
Determine Certification/Endorsement Authority E-10
Other Pre-Staffing Activities E-13
Pre-Validation Activities E-14
Actions for JUONs, JEONs, and DOD Component UONs E-14
Actions for Other Submissions E-15

Appendix A - Gatekeeping and Staffing Metrics E-A-1
Overview E-A-1
Gatekeeping Metrics E-A-1
Deliberate Staffing/Validation Metrics E-A-1
Urgent/Emergent Staffing/Validation Metrics E-A-2
Post Validation Metrics E-A-2

F DELIBERATE STAFFING PROCESS F-1

Overview F-1
Purpose F-1
Staffing Timelines F-2
Draft Documents F-2
Tailored Staffing F-2
JCB and JROC Procedures F-2
Pre-Staffing F-3
Initiation F-3

Initial Review F-3
Early engagement with stakeholders F-3
Staffing of Draft/Initial ICDs, Joint DCRs, CDDs, and CPDs F-3
Document Review and Commenting Stage F-3
Comment Adjudication Stage F-6
FCB Working Group and FCB Review Stage F-7
Validation Stage F-10
Post-Validation Documentation F-12
Staffing of Changes to Previously Validated Documents F-14
Abbreviated Staffing F-14
Staffing for Certifications and Endorsements F-14
Full Staffing F-14
Focus of Staffing for Proposed Changes F-14
Staffing of Post-AoA (or Similar Study) Reviews F-14
Abbreviated Staffing F-14
Focus of a Post-AoA (or Similar Study) Review F-15
Staffing of JROC/JCB Tripwire and CIP Breach Reviews F-16
Overview F-16
Initiation F-18
Review F-18
Waiver F-19
Other Review Authority F-20
Staffing of Nunn-McCurdy Unit Cost Breach and
MAIS Critical Change Reviews F-20
Statutory Basis F-20
Initiation F-20
Criteria F-21
Review Teams F-21
JROC Participation F-21
Staffing of Other Reviews or Issues F-22
Tailored Staffing F-22
Examples F-22

Appendix A – Endorsement Guide for Weapon Safety F-A-1
Purpose F-A-1
Weapon Safety Review F-A-1
JWSTAP Review Process F-A-2
Proponent F-A-5
Attachment A – Example WSE Recommendation Memorandum . F-A-A-1

Appendix B – Endorsement Guide for the Force Protection KPP F-B-1
Purpose F-B-1
Review Process F-B-1
Review Criteria F-B-1
Proponent F-B-2

DRAFT

Appendix C – Endorsement Guide for the System Survivability KPP F-C-1
Purpose F-C-1
Review Process F-C-1
Review Criteria F-C-1
Proponent F-C-2

Appendix D – Endorsement Guide for the Sustainment KPP F-D-1
Purpose F-D-1
Review Process F-D-1
Review Criteria F-D-1
Proponent F-D-5

Appendix E – Certification Guide for the Net-Ready KPP F-E-1
Overview F-E-1
Types of NR KPP Certifications F-E-1
Process relationships F-E-1
NR KPP Certification Process F-E-2
NR KPP Staffing F-E-3
Failure to Meet NR KPP Certification Requirements F-E-3
Recommendations F-E-4
Resources F-E-4
Spectrum Requirements Compliance F-E-4

Appendix F – Endorsement Guide for the Energy KPP F-F-1
Purpose F-F-1
Review Process F-F-1
Review Criteria F-F-1
Waiver Process F-F-3
Proponent F-F-3

Appendix G – Endorsement Guide for the Training KPP F-G-1

Appendix H – Endorsement Guide for DOTmLPF-P F-H-1
Purpose F-H-1
Review Process F-H-1
Review Criteria and Endorsement Memorandum F-H-2
Proponent F-H-3

Appendix I – Certification Guide for Intelligence Supportability F-I-1
Overview F-I-1
Intelligence Certification Procedures F-I-5
ISSA F-I-10
Attachment A – Intelligence Certification Summary and Letter F-I-A-1

G URGENT/EMERGENT STAFFING PROCESSES G-1

Overview G-1
Purpose G-1
Compromises to Facilitate Timeliness G-1
Staffing Timelines for JUONs and JEONs G-2
Follow-on Activities G-2
Staffing of JUONs and JEONs G-3
Initiation G-3
Joint Staff Gatekeeper Review G-3
FCB Review G-3
Validation Authority G-4
Validation Decision G-4
Validation Duration G-5
Validation Documentation G-5
Modifications to Validated JUONs and JEONs G-6
Modification Review G-7
Validation Recommendation G-7
Validation Decision G-7
Exceptions G-7
Periodic Validation Reviews G-7
Quarterly Review G-7
Biannual Review G-7
Assessment of Operational Utility G-8
Timing G-8
Intent G-8
Tailorability G-8
Disposition G-9
Archiving G-10
Example Assessment Content G-10

H REFERENCES H-1

GLOSSARY GL-1

Part I – Acronyms GL-1
Part II – Definitions GL-9

DRAFT

(INTENTIONALLY BLANK)

DRAFT

ENCLOSURE A

REQUIREMENTS MANAGEMENT CERTIFICATION TRAINING (RMCT)

1. Overview

a. Training mandate. In accordance with reference d, members of the Armed Forces and employees of DOD with authority to generate capability requirements must successfully complete a DOD Component certification training program, including training courses executed by the Defense Acquisition University (DAU) as outlined in this enclosure.

(1) The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), in consultation with DAU, developed a training program for DOD personnel with responsibility for generating requirements, and defined the target population for the training program.

(2) As personnel have varying degrees of responsibility within the requirements process, and correspondingly variable training needs, each DOD Component determines what specific steps are needed to certify their personnel as Requirements Managers. Completion of the DAU training courses corresponding to the levels described herein is a prerequisite to any DOD Component certification.

(3) DOD Components, and their gatekeeper personnel, are ultimately responsible for ensuring that capability requirement documents are in compliance with guidance in references a and b, and this manual. RMCT training provides essential knowledge for:

(a) Personnel preparing, reviewing, and approving capability requirement documents.

(b) Personnel participating as members, stakeholders, or advisors in the FCB Working Groups (FCB WGs), FCBs, JCB, and JROC.

(c) Personnel submitting comments related to capability requirement documents, and associated certifications or endorsements.

b. Certification levels. Individuals filling positions/billets within a DOD Component whose responsibilities are commensurate with the guidelines below will be trained to the level associated with those responsibilities.

(1) Level A – Contribute to the capability requirement generation and development process in various capacities. Duties may include administrative support, analysis, provision of subject matter or domain expertise, and JCIDS document development, staffing, and/or coordination.

(2) Level B – Significantly involved with capability requirement generation and development in specific capacities. Duties may include study leadership, planning, writing, adjudicating comments, and facilitating inter-organizational development and coordination of JCIDS documents.

(3) Level C – Designated by organizational leadership for advanced requirements instruction. Duties may include leadership and supervisory roles in capability requirement generation and development, and organizational representation in pertinent program management and JCIDS forums to include the FCB WGs, FCBs, JCB and JROC.

(4) Level D – General Officer/Flag Officer (GO/FO) and Senior Executive Service (SES) only. Duties may include approval of draft documents for submission into JCIDS, senior leadership and oversight of analysis and staffing of JCIDS documents, enforcement of requirements standards and accountability, and if holding independent authority, validation of JCIDS documents.

2. RMCT Management and Reporting

a. Component Appointed Representatives (CARs) and Functional Integrated Process Team (FIPT) representatives.

(1) Each Component designates a Primary and Alternate CAR – typically O-4/O-5 or civilian equivalent – for day-to-day RMCT management activities. CAR oversight duties include, but are not limited to:

(a) Identifying and tracking all billets/positions within the Component requiring training and certification in accordance with this enclosure.

(b) Participating in FIPT working groups on behalf of the Component.

(c) Encouraging all personnel developing capability requirement documents to participate in recurrent training in order to increase their skills and knowledge of the requirements process. Also encouraging participation in training related to other Defense Acquisition Workforce Improvement Act (DAWIA) career fields and functional areas detailed in reference e, to gain wider breadth of knowledge and understanding.

(2) In addition, each Component designates a Functional Integrated Process Team (FIPT) representative – typically O-6, GS-15, or equivalent grade – to represent the Component at RMCT leadership events. FIPT Representative

duties include, but are not limited to, participating in RMCT leadership events, such as FIPTs, on behalf of the Component.

(3) When designating or replacing a Primary and/or Alternate CAR or FIPT representative, send updated information to RMCT@dau.mil, Subject: CAR and/or FIPT Representative. Include first and last name, rank, Component, office name/symbol, email address, phone number, and specifically identify the individual(s) as the primary or alternate CAR or FIPT representative. Upon designation, a message will be sent from DAU to the individual with RMCT program details and expectations.

b. Requirements workforce status reports. When notified by a Joint Staff Action Processing (JSAP) task, not to exceed every 6 months, the CAR will submit a requirements workforce status report in accordance with the directions in the JSAP. The consolidation of JSAP responses will be briefed to the JCB and/or JROC by the J-8/DDR and the Director, Joint Operations Support within the Office of the USD(AT&L). The JSAP responses will be used to inform Congressional and DOD decision-makers on the status of the requirements workforce, allowing for informed future training and resource allocation decisions. The JSAP responses will provide at least the following information:

(1) Number of RMCT Level 'B' Billets (Military/Civilian)

(2) Number of RMCT Level 'C' Billets (Military/Civilian)

(3) Number of RMCT Level 'D' Billets (Military/Civilian)

(4) Number of Level 'B' Billets filled - trained/certified (Military/Civilian)

(5) Number of Level 'C' Billets filled - trained/certified (Military/Civilian)

(6) Number of Level 'D' Billets filled - trained/certified (Military/Civilian)

(7) Estimated number requiring Level 'C' training in current and next Fiscal Year (new fills and replacement)

(8) Estimated number requiring Level 'D' training in current and next Fiscal Year

3. Training Courses. Courses created and administered by DAU for RMCT fall into two general categories.

a. Core courses. The core courses, required for specific certification levels, are shown in Table A-1, with additional detail provided at the URL in reference f.

TRAINING COURSE NUMBER/ TITLE	**CLR 101** Introduction to JCIDS	**RQM 110** Core Concepts for Requirements Management	**RQM 310** Advanced Concepts and Skills	**RQM 403** Requirements Executive Overview Workshop	**RQM 413** Senior Leader Requirements Course
ESTIMATED TIME TO COMPLETE	4-6 hours	24-30 hours	5 days	1 day	Tailored (no longer than 1 day)
CERTIFICATION LEVEL	A, B, C	B, C	C	D (1-3 Star/ Civilian Equivalent	D (4-Star / Agency Director)

Table A-1: DAU-Administered RMCT Core Course Overview

(1) CLR 101, Introduction to JCIDS. This on-line course provides an overview of the DOD capabilities analysis and requirements development process. The course focuses on terms, definitions, basic concepts, processes, and roles and responsibilities of personnel involved in executing the JCIDS process. Mandatory instruction for position categories A, B, & C. Prerequisites: none.

(2) RQM 110, Core Concepts for Requirements Management. This on-line course covers both the requirements manager role and requirements management within the "Big A" acquisition construct. The course examines the capability development process from an end-to-end perspective, highlighting the interactions among JCIDS, DAS, and Planning, Programming, Budgeting, and Execution (PPBE) processes. Mandatory instruction for position categories B & C. Prerequisites: CLR 101.

(3) RQM 310, Advanced Concepts and Skills for Requirements Managers. This in-residence course is held at the DAU campus, Defense Systems Management College (DSMC), Fort Belvoir, VA. The course takes an in-depth look into the interactions among JCIDS, DAS, and PPBE processes. Mandatory instruction for position category C. Prerequisites: RQM 110.

(4) RQM 403, Requirements Executive Overview Workshop. This in-residence course, for GO/FO and SES personnel, provides an executive-level understanding of requirements management within the "Big A" acquisition construct. The course examines the capability development process from an end-to-end perspective, highlighting the interactions among JCIDS, DAS, and PPBE processes, as well as the role of the requirements manager. Mandatory instruction for GO/FO and SES's in position category D. Prerequisites: none.

(5) RQM 413, Senior Leader Requirements Course. This one-on-one course, focused on the 4-star Service Chief, Service Vice-Chief, CCMD Commander, Agency Director audience, provides senior leaders with an executive-level understanding of the interactions among JCIDS, DAS, and PPBE processes to meet the warfighters needs. The presentation length and scope of the course is tailored to meet the needs of each senior leader. Prerequisites: none.

b. Core Plus courses. Core Plus courses, not required for RMCT certification unless directed by a DOD Component, are shown in Table A-2, with additional detail provided at the URL in reference f.

TRAINING COURSE NUMBER / TITLE	**CLR 151** Analysis of Alternatives	**CLR 250** Capability Based Assessment	**CLR 252** Key Performance Parameters
ESTIMATED TIME TO COMPLETE	3-5 hours	3-5 hours	3-5 hours

Table A-2: DAU-Administered RMCT Core Plus Course Overview

(1) CLR 151, Analysis of Alternatives (AoA). This on-line course provides professionals who lead or directly support AoAs with a comprehensive introduction to conducting AoA activities. Sponsors use the AoA to assess and prioritize potential materiel solutions and trade space in support of validated military capability requirements. Prerequisites: none, but CLR 101 is recommended for those without previous requirements experience.

(2) CLR 250, Capabilities-Based Assessment (CBA). This on-line course provides professionals who lead or directly support CBAs with a comprehensive introduction to conducting CBA activities. Sponsors use the CBA to identify military capability requirements and associated capability gaps, as well as potential non-materiel and materiel approaches to close or mitigate capability gaps. Prerequisites: none, but CLR 101 is recommended for those without previous requirements experience.

(3) CLR 252, Key Performance Parameters (KPPs). This on-line course provides professionals who develop KPPs and other requirements for inclusion in capability requirement documents with an overview of how to develop KPPs, details of the mandatory KPPs, and the relationship of KPPs to measures of effectiveness (MOEs), measures of performance (MOPs), and measures of suitability. Prerequisites: none, but CLR 101 is recommended for those without previous requirements experience.

4. Course Attendance Guidelines

a. Resident course attendance

(1) DAU receives funding to teach a number of students considered necessary to provide the requirements community with training directed by DOD senior leadership and reference d. Each DOD Component receives a limited number of seats per year, and should strive to fill all allocated seats with students in need of requirements training.

(2) CARs will enroll prospective students in a course or add them to a course's official wait list only after verification that course pre-requisites have been completed by reviewing either/or:

(a) Copy of student's DAU transcript

(b) Official DAU Course completion certificates for all pre-requisites

b. Pre-course work. Any student scheduled to attend a DAU resident course should thoroughly review the recommended and/or required preparatory pre-course work. Supervisors should ensure that their employees have sufficient time during the duty day to complete the pre-course work and provide assistance, if needed.

c. Walk-in students

(1) Documenting pre-requisite courses. Walk-in students NOT on the course waiting list will be required to provide documentation citing successful completion of prerequisite DAU course(s) as noted above for course enrollment. Walk-in students who are on the course waiting list do not need to provide documentation of pre-requisites, as they have already been verified.

(2) Contractor attendance. Per reference g, contractors will be accepted into resident courses only on a walk-in basis, per DAU's walk-in regulations. Contractors may accomplish DAU on-line training as needed, subject to guidance and/or limitations in their specific contracts.

(3) Priorities for filling open seats. Class seats remaining open due to low registration, short-notice cancellations, or course no-shows will be filled in the following priority order:

(a) Military and DOD civilian students who work in requirements related billets and are on the course's official waiting list.

(b) Military and DOD civilian students who work in non-requirements related billets, taking the course as a DAWIA Core-Plus or other knowledge broadening opportunity, and are on the course's official waiting list.

(c) Military and DOD civilian students who work in requirements related billets and are walk-ins at the beginning of the course.

(d) Military and DOD civilian students who work in non-requirements related billets, taking the course as a DAWIA Core-Plus or other knowledge broadening opportunity, and are walk-ins at the beginning of the course.

(e) Contractor personnel who work in requirements related billets and are walk-ins at the beginning of the course.

(f) Contractor personnel who are in non-requirements related billets, taking the course as a DAWIA Core-Plus or other knowledge broadening opportunity, and are walk-ins at the beginning of the course.

d. Course no-shows. Students who are enrolled in a resident course and fail to attend the class, impose a potential negative impact on the Component and seat allocations for future DAU courses.

(1) Any no-show requirements community member(s) will remain ineligible to apply for future DAU courses for a period of four (4) months starting on the last day of the scheduled resident course for which they failed to appear.

(2) The individual's supervisor and the first O-6, GS-15, or equivalent grade in the chain-of-command will sign a memorandum acknowledging the individual's no-show status. No later than five (5) business days after first day of intended course, email the memorandum, Subject: No-Show, to the Dean for Requirements Management, DSMC at RMCT@dau.mil.

e. Short notice cancellations. Cancellation within 14 days of the scheduled start date for resident courses is considered to be short notice. If a student cancels within the short notice timeframe, the student must inform his/her CAR as soon as possible. The CAR is responsible for filling the vacated slot with another student.

f. Course failures. A course failure can occur for numerous reasons including, but not limited to, students failing a graded event within a resident course, or students missing more than 5% of instructional time.

(1) If such an instance occurs, the student must inform his/her supervisor and the first O-6, GS-15, or equivalent grade in the chain-of-command.

(2) A memorandum acknowledging the individual's course failure must be written and signed by both the individual's supervisor and the first O-6, GS-

15, or equivalent grade in the chain-of-command. Provide the memorandum to the Dean for Requirements Management, DSMC, by sending the memorandum to RMCT@dau.mil, Subject: Course Failure.

h. Additional academic policies

(1) Reference g provides DAU's student academic policies and information for additional insight on DAU student matters not covered in this enclosure.

(2) The Dean for Requirements Management, DSMC, in consultation with the CAR, may waive rules as they pertain to DAU's RMCT courses, curriculum, and the stipulations therein.

DRAFT

ENCLOSURE B

CAPABILITY REQUIREMENT PORTFOLIO MANAGEMENT

1. Overview

a. Purpose. The key objective of the JCIDS process is to facilitate the JROC and its subordinate boards, as informed by other stakeholders in the capability requirements process, to:

(1) Manage and prioritize capability requirements within and across the capability requirement portfolios.

(2) Inform other assessments, processes, and activities within the Joint Staff and across DOD.

(3) Enable the JROC and CJCS to meet their statutory responsibilities outlined in reference a.

b. Capability Requirement Portfolios

(1) Capability requirement portfolios are established using Joint Capability Areas (JCAs) as an organizing construct. This provides the FCBs with capability requirement portfolios of similar DOD capabilities, across all organizations and at all classification levels, functionally grouped to support capability analysis, strategy development, investment decisions, capability requirement portfolio management, and capabilities-based force development and operational planning.

(a) Capability requirement portfolios include capability requirements validated by the JCB or JROC as well as those validated by independent validation authorities. They also include capability requirements validated under the urgent or emergent process lanes in addition to those validated under the deliberate process lane.

1. Note that visibility within a portfolio should include both the capability requirements which are the primary focus of documents reviewed by the particular FCB, as well as capability requirements which align with the JCA but are part of documents reviewed by a different FCB. For example, a system being reviewed by the Force Application (FA) FCB due to its primary capabilities, may also have radar/sensor capabilities which are applicable to the Battlespace Awareness (BA) FCB portfolio.

2. Sub-portfolios may be organized by the FCB Chairs in cases where the breadth of the capability requirement portfolio makes analysis and decision support efforts cumbersome without further subdivision.

3. Information related to validated capability requirements is available via the Knowledge Management / Decision Support (KM/DS) system at the URL in reference h, with additional information available from the wiki site at the URL in reference i.

(b) Each validated capability requirement should align with one of three categories shown in Figure B-1:

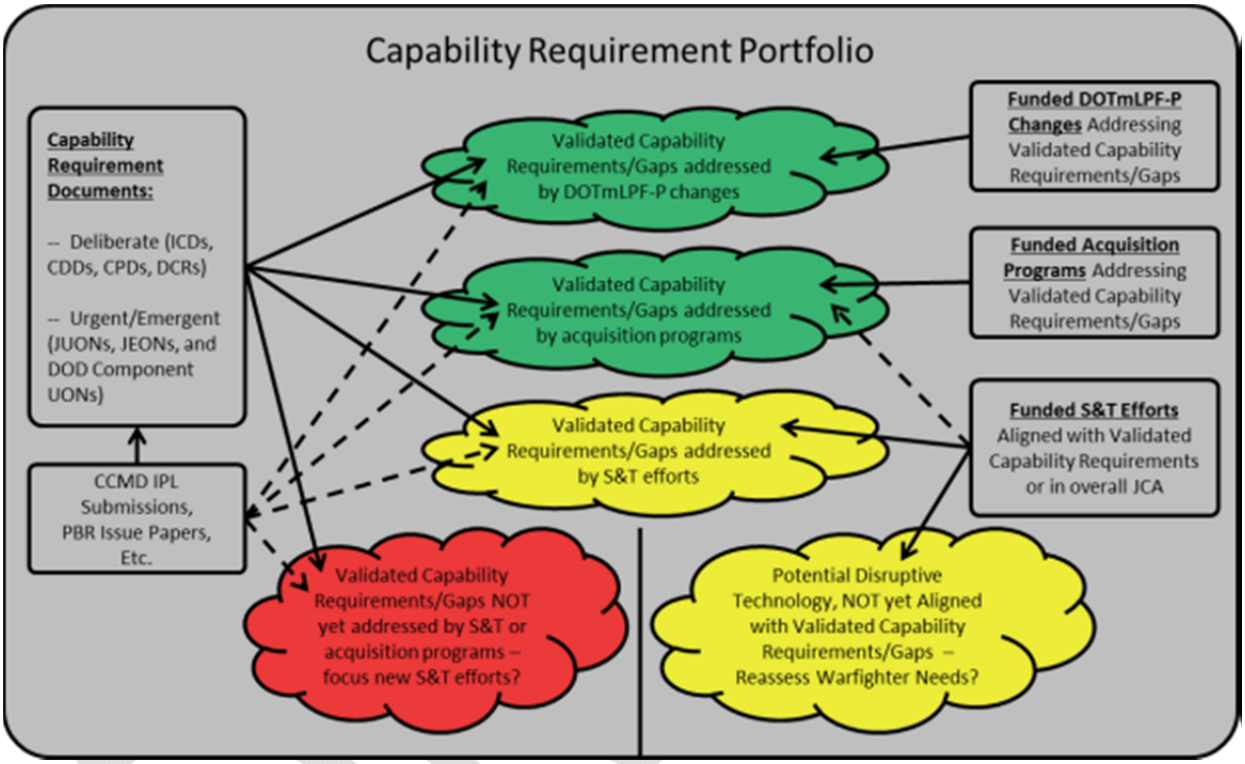

Figure B-1: Notional Capability Requirement Portfolio

1. Validated capability requirements being addressed by an acquisition program or implementation of DOTmLPF-P changes.

a. FCBs and other stakeholders should maintain awareness of progress toward satisfying validated capability requirements to ensure potential changes to programs or implementation timelines can be assessed for their impact to the capability requirement portfolio, and to ensure that newly proposed capability requirements are not unnecessarily duplicative of efforts already underway.

b. S&T organizations should maintain awareness of technology challenges within and across acquisition programs for potential alignment of independent S&T efforts.

c. Information related to acquisition programs is available via the Defense Acquisition Management Information Retrieval system at the URL in reference j, or Sponsor equivalent databases. Information related to implementation of DOTmLPF-P changes resulting from validated Joint DCRs is available from the Joint Staff Gatekeeper.

2. Validated capability requirements not (yet) being addressed by an acquisition program or implementation of DOTmLPF-P changes, but aligned with ongoing or recently completed S&T efforts at a Technology Readiness Level (TRL) of three or greater. Visibility into S&T efforts potentially addressing warfighter needs leverages a key aspect of the DOD scientific and technical information program outlined in reference k.

a. FCBs and other stakeholders should maintain awareness of S&T efforts potentially applicable to validated capability requirements to ensure proper advocacy for execution and timely transition of S&T efforts when applicable to satisfying validated capability requirements.

b. Program Managers (PMs) should maintain awareness of S&T efforts where incorporation of technologies matured outside of specific acquisition programs could improve cost, schedule, and/or performance.

c. Information related to ongoing and recently completed S&T efforts is available via the Defense Technical Information Center's Unified Research and Engineering Database at the URL in reference l.

3. Validated capability requirements not (yet) being addressed by an acquisition program, implementation of DOTmLPF-P changes, or ongoing or recently completed S&T efforts.

a. S&T organizations should maintain awareness of validated, but unaddressed, capability requirements for potential alignment of future S&T efforts.

b. Information related to validated capability requirements is available via the KM/DS system at the URL in reference h.

(c) To enable technological innovation, FCBs and other stakeholders must maintain visibility into funded S&T efforts which align with the general capability requirement portfolio but not with any specific validated capability requirement, as shown in Figure B-1. This visibility can potentially enable disruptive technology changes through reassessment of previously validated requirements in light of emerging technologies.

(d) Knowledge of past requirements, acquisition, and budgetary decisions and rationale, is also critical for making informed decisions on

validation of new capability requirements, or conducting periodic assessments of the capability requirement portfolios.

1. Specifically, this awareness should include information from the past several cycles of the CGA and PBR, and what rationale was behind the recommendations and decisions. Note that some IPLs introduced for the CGA, or issue papers introduced for PBR, identify issues that are not already captured as a validated capability requirement, and must be documented and validated through the JCIDS process.

2. Reassessment of the capability requirement portfolio, including potential changes to previous validation decisions to better close or mitigate capability gaps, may also be necessary to adapt to changing global context, threats, or strategic guidance. Decisions must be with awareness of how more recent context differs from that informing the original decisions.

3. In cases where programs developing capability solutions to satisfy validated capability requirements are reduced or cancelled, the FCBs and other stakeholders must assess the impact to the capability requirement portfolios. See the JROC/JCB Tripwire review activities later in this enclosure.

(2) Capability requirements and other issues which cross capability requirement portfolios will be handled by teaming between FCBs and other organizations.

(a) For issues lying primarily within a lead FCB and requiring support from one or more supporting FCBs, the lead FCB will coordinate with the supporting FCBs as required.

(b) For issues with significant cross-cutting impact, leadership may designate the Joint Staff J-8, Joint Requirements Assessment Division (J-8/JRAD) to coordinate analysis efforts, with participation from the appropriate FCBs, J-8/JRAD, Joint Staff J-8, Capabilities and Acquisition Division (J-8/CAD), Joint Staff J-8, Program and Budget Analysis Division (J-8/PBAD), and invite participation of other stakeholders of the issue under review.

(c) The O-6 and GO/FO Integration Groups provide discussion forums for oversight of cross-cutting issues before being elevated to the JCB or JROC.

c. Capability-Mission Lattice (CML). The CML, shown in Figure B-2 and described in the following paragraphs, provides an integrating construct for articulating the dependencies between capability requirements as well as the traceability between related processes and activities across the department as shown in Figure B-3.

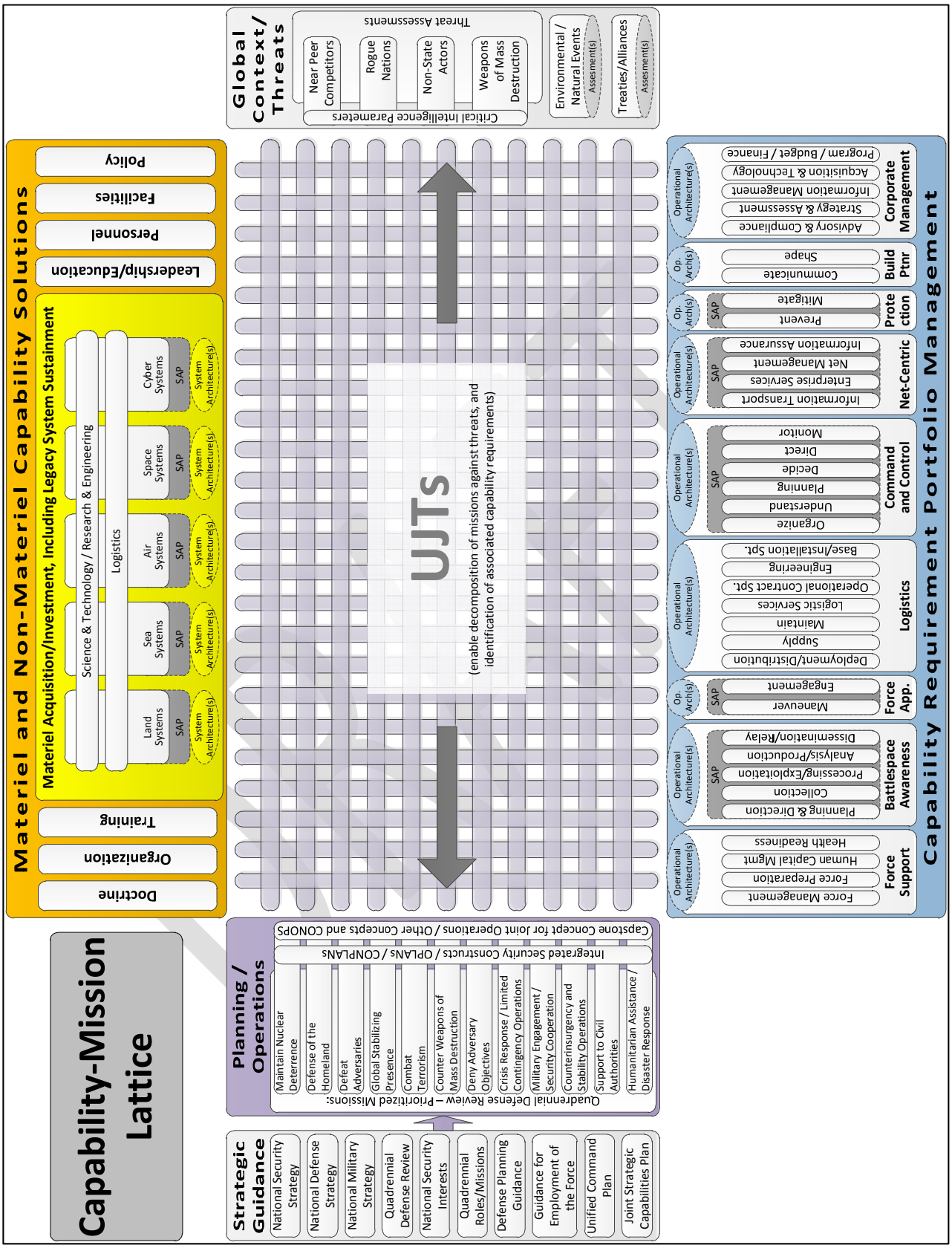

Figure B-2. Capability-Mission Lattice

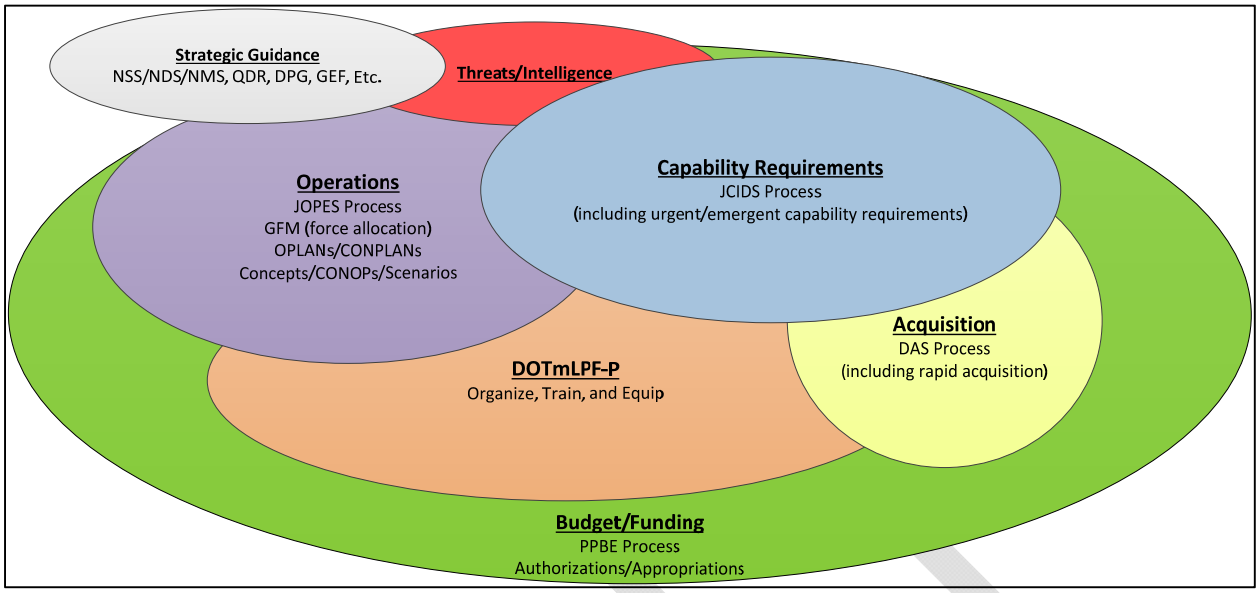

Figure B-3. Process Interactions

(1) Strategic Guidance. Guidance from many sources influences military operations, intelligence activities, development and validation of capability requirements, acquisition activities, and DOTmLPF-P associated with organizing, training, and equipping forces. It also influences the budgetary process which provides funding for all of these activities.

(a) An organization's roles, missions, or tasks, and any associated planning or operations must be consistent with strategic guidance.

(b) The National Security Strategy (NSS), the National Strategy for Homeland Security, the National Defense Strategy (NDS) or the most recent Quadrennial Defense Review (QDR) Report, and the National Military Strategy (NMS) provide the overarching description of the Nation's defense interests, objectives, and priorities. In addition, the Defense Planning Guidance (DPG), the Guidance for the Employment of the Force (GEF), the Chairman's Risk Assessment (CRA), the Joint Strategic Capabilities Plan (JSCP), and other documents contain further guidance for objectives and priorities.

(c) The above list of strategic guidance documents should be considered as a starting point. The dynamic nature of strategic guidance requires that Sponsors ensure the latest strategic guidance is considered, including guidance which may have superseded documents listed above.

(2) Planning/Operations. Current and planned operations, as well as other roles, missions, and functions which direct an ability to perform certain activities, are the most direct driver of capability requirements, in the context of the strategic guidance and threats/intelligence. Capability requirements

associated with operations, which are not already available from the joint force, may result in capability gaps with associated operational risk if not mitigated by a new materiel or non-materiel capability solution.

(a) An organization's operations, roles, missions, or functions can be organized in terms of the Department's top level mission areas. Service and joint concept(s) or CONOPS will articulate how the organization plans to accomplish its roles, missions, or functions, which may be further decomposed into lower levels of the Universal Joint Task List (UJTL). While Sponsors may use other constructs, such as Joint Mission Threads (JMTs), kill chains, etc., to facilitate decomposition or assessment of their roles, missions, or functions, they must ultimately be captured in terms of UJTs. These lower level decompositions express the activities in terms of operational capabilities required to accomplish the activity.

(b) Operational capabilities are articulated in terms of operational attributes rather than system specific parameters. For example, if communications are part of a task, the operational attributes might specify what must be communicated, where, under what conditions, and with what reliability or latency parameters. Specific frequencies, technical specifications, etc. are generally not appropriate for use as operational attributes.

(c) Identified operational capabilities must be traceable to approved Service and joint concepts developed in accordance with reference m, Support for Strategic Analysis (SSA) products developed in accordance with references n and o, and/or other JROC approved guidance. SSA products include current and future baselines, scenarios, and CONOPS developed in conjunction with an approved operation plan (OPLAN) or contingency plan (CONPLAN). SSA products may also be organized into Integrated Security Constructs (ISCs) to aid in the analysis process. CONOPS must be endorsed by the JROC, a CCMD, a Service, or a defense agency.

(3) Global Context and Threats/Intelligence. Intelligence activities identify and quantify threats which may drive or impact military operations, and inform the setting of performance levels in capability requirements. The need to collect intelligence also drives capability requirements, often worked collaboratively between military and intelligence requirements processes when there are shared equities in the capabilities.

(a) The level of performance required for each capability requirement derived from the UJTs is generally driven by a pacing threat or some other global context. FCBs and other stakeholders must also understand the relationship and traceability of the capability requirements to the Universal Joint Tasks (UJTs) they enable and the missions they support.

(b) Threat data must be traceable to DIA- or Service-approved threat products, including but not limited to Defense Intelligence Agency (DIA) validated Capstone Threat Assessments (CTAs), the Multi-Service Force Deployment (MSFD), the Joint Country Forces Assessments, and the CRA.

(4) Capability Requirements. Based upon strategic guidance, threats/intelligence, and military operations, the JROC, or an independent validation authority, reviews and validates proposed new capability requirements and performs periodic assessments of the capability requirement portfolios. Validated capability requirements which lack a materiel or non-materiel capability solution may be recommended for developing a new materiel or non-materiel capability solution to mitigate the operational risk associated with the capability gap.

(a) Validated capability requirements for legacy and planned future capabilities are organized using JCAs. This provides the FCBs with capability requirement portfolios of similar DOD capabilities, across all organizations and at all classification levels, functionally grouped to support capability analysis, strategy development, investment decisions, capability requirement portfolio management, and capabilities-based force development and operational planning.

(b) Capability requirement portfolios also include capability requirements protected by Special Access Program (SAP), Special Access Required (SAR), or Alternative Compensatory Control Measure (ACCM) designation. Appropriately cleared analysts provide FCB Chairs and other senior decision makers with the context of how the SAP, SAR, or ACCM protected capability requirements contribute to the overall capability requirement portfolios.

(c) Efforts identifying potential new capability requirements must be considered in the context of previously generated architectures for capabilities in that JCA, particularly when there is an enterprise architecture (EA) established, to ensure interoperability and integration within and across JCAs. Related architecture data and associated artifacts/views can be found at the URLs shown in references p and q. Additional detail on enterprise architectures and the architecture federation is available in Appendix C to this enclosure.

(d) Proposal of completely new capability requirements and related architectures is discouraged when adaptation of previously validated capability requirements and previously generated architectures can be re-used or adapted to address changing roles, missions, or functions.

(5) Materiel and Non-Materiel Capability Solutions

(a) There is generally a many-to-many mapping between validated capability requirements and capability solutions, requiring both materiel and non-materiel solutions to address a single requirement. A single multi-function system, with its associated DOTmLPF-P enablers, may also address many capability requirements across multiple capability requirement portfolios.

(b) DOTmLPF-P

1. Organizing, training, and equipping of the DOD Components encompass the DOTmLPF-P activities and provide forces ready to conduct military operations. In cases where a new non-materiel capability solution is recommended to close or mitigate a capability gap, one or more aspects of DOTmLPF-P may be changed to deliver a non-materiel capability solution.

2. Non-materiel capability solutions addressed by changes to DOTmLPF-P, as well as DOTmLPF-P enablers to materiel capability solutions, are organized in parallel with the materiel system portfolios.

(c) Materiel Acquisition

1. In cases where a non-materiel capability solution is not practical or sufficient, and a new materiel capability solution is recommended to close or mitigate a capability gap, DOD Components with acquisition authority may develop new materiel capability solutions to deliver the capability. Typically, there will also be DOTmLPF-P changes associated with the introduction of new materiel capability solutions.

2. Materiel capability solutions, including both legacy systems and those in development, are organized into areas of similar systems. These areas include systems from all organizations and all classification levels, and may have one or more roadmaps for development of similar classes of systems across the department. System architectures are also collected for each system in these areas.

3. Supporting or enabling efforts, such as S&T, Research and Engineering, and Logistics, are also captured as they are critical enablers for the capability solutions in each of the domains.

(6) Budgets/Funding. Execution of the processes or activities in the other areas requires appropriate funding, which is best justified by being able to articulate the interactions and traceability between each area.

(7) Portfolio Management Tools. Tools which leverage the CML shown in Figure B-2 and integrate data available from applicable databases are being developed by the Joint Staff for use by the FCBs and other capability requirement stakeholders. Contact the Joint Staff Gatekeeper for further

information or access to prototype portfolio tools. The portfolio tools in development specifically allow queries against and integrate information related to:

(a) Mapping defense planning scenarios to UJTs. This data is managed by the Joint Staff J-8.

(b) Mapping UJTs to JCAs. This data is managed by the Joint Staff J-7.

(c) Mapping validated capability requirements to JCAs. This data is provided by Sponsors in their capability requirement documents and associated DODAF views.

(d) Mapping current and recently completed S&T efforts to JCAs. This data is managed by the Defense Technical Information Center (DTIC).

(e) Mapping validated capability requirements to acquisition programs. This data is managed by USD(AT&L).

(f) Mapping acquisition programs to budget data. This data is managed by OSD CAPE.

d. Portfolio reassessments. Changes within any of the related processes or activities may require reassessment of the capability requirement portfolios to ensure that any impacts are identified and appropriate actions taken to reprioritize and reshape the capability requirement portfolios to best serve the joint force. These actions may include, but are not limited to:

(1) Review of previously validated capability requirements for potential adjustment in light of the updated guidance.

(2) Initiating studies or analyses to assess identified gaps or overlaps in the capability requirement portfolios.

(3) Using capability requirement portfolio assessments to inform other Departmental processes or decision making, such as in Program and Budget Review (PBR).

2. Executing Capability Requirement Portfolio Management. Fundamentally, FCB Chairs and other stakeholders must be advocates for changes to the capability requirement portfolio which are in the best interest of the joint force, and not necessarily advocate for every capability requirement proposed by Sponsors. They must ensure that EA products are updated to reflect how new or modified capability requirements, and associated materiel and non-materiel capability solutions, impact their capability requirement portfolios without

introducing unnecessary redundancy in capability or capacity. To facilitate capability requirement portfolio management, a number of periodic and event driven reviews may be applicable to each capability requirement portfolio.

a. Periodic Reviews

(1) Capability Gap Assessment (CGA)

(a) The CGA is an annual assessment, coordinated by the Joint Staff Gatekeeper, which examines CCMD identified priorities, along with other issues and perspectives from the Services and other DOD Components, groups similar gaps, assesses on-going efforts to close or mitigate capability gaps, and recommends programmatic and/or non-programmatic actions to close or mitigate capability gaps. The CGA process is general in nature and may be modified as necessary based on senior leader direction. See Appendix A to this enclosure for more detail of the CGA process.

(b) The CGA provides a key opportunity to adjust and reprioritize capability requirements within each capability requirement portfolio to better serve the needs of the joint force, as articulated by the CCMDs in their IPLs.

1. CCMDs annually submit IPLs for capability requirements, assessed across DOD Component and functional lines, which represent capability gaps limiting CCMD assigned mission accomplishment.

2. The FCBs and other stakeholders involved in the CGA process must consider the priorities of the CCMDs in context of the capability requirement portfolios in present and future timeframes. Any potential mitigation strategies for a capability gap must also be considered in terms of its impact to other capabilities and dependencies within and across capability requirement portfolios.

3. Where appropriate, the output of the CGA will recommend mitigation strategies for the identified capability gaps which better prioritize the efforts to improve the capability requirement portfolios.

4. In cases where the CGA identifies new capability gaps that are not already supported by validated capability requirements, the FCBs will provide recommendations to the JROC to facilitate Sponsor development of the appropriate capability requirement document for review and validation.

(2) Munitions Requirements Process (MRP). The MRP is an annual review of near-year and out-year total munitions requirements, in accordance with reference r, identifying total munition inventories required to enable execution of CCMD assigned missions. Analysis conducted as a part of MRP is

a key aspect of managing the munitions portfolio and supporting capability requirement decision making.

(3) Program and Budget Review (PBR). The PBR is an annual review coordinated by the Office of the Under Secretary of Defense, Comptroller (USD(C)) and the Office of the Secretary of Defense (OSD) Cost Assessment and Program Evaluation (CAPE) to facilitate the consolidation of program objective memorandum (POM) and budget estimate submissions (BES) from the Services and other DOD Components, and adjudication of any outstanding issues before presenting the overall DOD input to the President's budget submission.

(a) Overview. PBR is one part of the larger PPBE process. The Deputy Secretary of Defense manages PPBE as the primary process for enabling the funding of the various JCIDS and DAS activities which develop, field, and sustain effective capability solutions to the warfighters. Details of the PPBE processes are in reference s. See Figure B-4 for an overview of the resource allocation process and its interaction with the PPBE process.

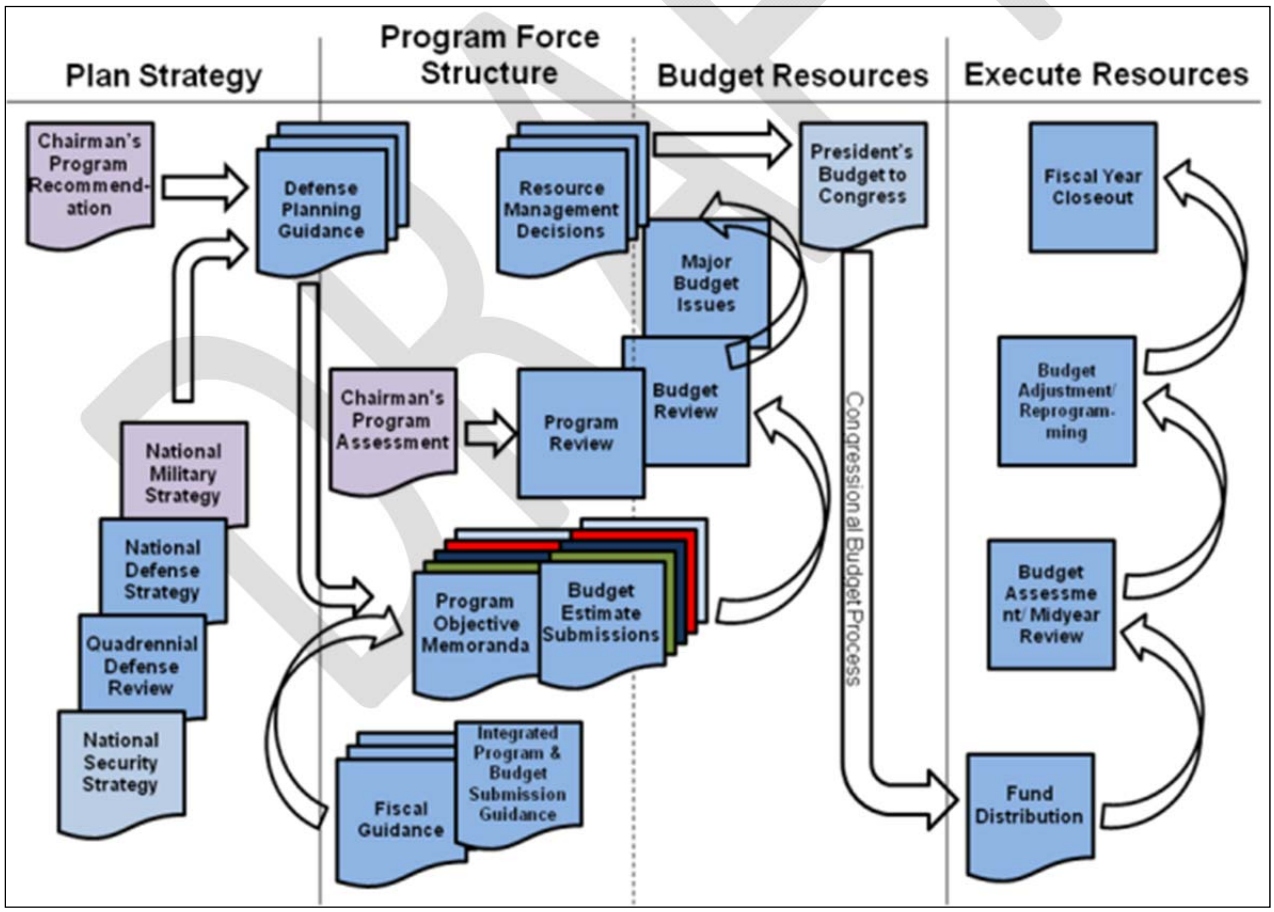

Figure B-4. Overview of the Resource Allocation Process and Interaction with PPBE

1. Planning

a. Planning examines U.S. defense posture and the DOD in the global context, considering national security objectives and the need for efficient management of defense resources. The focus of planning is to define the national defense strategy necessary to maintain national security and support U.S. foreign policy, and to provide the Secretary of Defense with strategic decision options. These options are informed by relevant joint operational concepts and analysis of current and programmed forces in relation to the demands of the primary missions defined by the defense strategy. Results of the planning phase inform the development of proposed programs by the DOD Components.

b. Planning utilizes the same strategic documents which inform the JCIDS process. The DPG, along with fiscal guidance from the Office of Management and Budget (OMB), informs the Services, CCMDs, and other DOD Components in the development of their POMs.

2. Programming

a. DOD Components develop proposed programs, which in the aggregate form their POMs, consistent with planning guidance, programming guidance, and fiscal guidance. These programs reflect analysis of missions and objectives to be achieved, alternative methods of accomplishing them, and the effective allocation of resources. The Chairman's Program Assessment (CPA) provides an assessment of the adequacy of DOD Component POMs and may be considered in refining the Defense program and budget. OSD conducts an annual PBR to adjudicate program and budget issues and better align the overall DOD budget prior to submission to OMB. The result of PBR is a Resource Management Decision, which directs changes to the POMs as they are consolidated into the overall DOD budget submission to OMB.

b. Validated capability requirements from the JCIDS process are the driver for a large portion of the POMs, including both development of new capability solutions and sustainment of fielded capability solutions. Robust capability requirement portfolio management and the exercise of JROC Title 10 authorities ensures that validated capability requirements represent an appropriate balance across the joint force.

3. Budgeting

a. DOD Components develop and submit detailed budget estimates for their programs in accordance with fiscal guidance, programming guidance, and DOD financial management regulations in reference t. A budget review is conducted as part of PBR to ensure that programming and budgeting are aligned to the priorities of the joint force. Since the DOD budget is only a

portion of overall government expenditures, OMB consolidates the budget submissions from all of the government departments and agencies, and produces the President's Budget for submission to Congress. Through a number of committees and legislative procedures, and informed by the President's Budget and testimony of various DOD officials, Congress authorizes and appropriates funds as it sees fit for the execution of DOD programs.

b. As with the programming stage, validated capability requirements must inform budgetary decisions, since changes to budget may impact ability to develop capabilities on a particular schedule or affect quantities of capability solutions to be purchased, and thus impact the operational risk accepted by the joint force.

4. Execution Review

a. Using the funding provided by Congress, the Services, CCMDs, and other DOD Components execute their programs and interact directly or indirectly with the JCIDS process with activities including study, identification, validation of new capability requirements with associated capability gaps, development and acquisition of new capability solutions, and Operations and Support (O&S) of fielded capability solutions.

b. The DOD Components conduct annual execution reviews to determine how well programs and financing have met joint warfighting needs. OSD, in coordination with CJCS, assess the findings of the DOD Components and recommend program and budget adjustments where applicable.

(b) Requirements context for PBR decision making

1. Following POM/BES submissions, OSD CAPE organizes issue teams as needed to review program issues, while the Office of the USD(C) conducts budgetary pricing, execution and executability reviews. Both OSD CAPE and the Office of the USD(C) recommend potential adjudication for senior decision makers. Issue team membership includes representatives from across the Joint Staff and OSD as well as the DOD Components, to assure that joint equities are properly represented.

2. As close coordination of JCIDS, DAS, and PPBE processes is critical, the FCB Chairs, supported by representatives from the FCBs, J-8 JRAD, J-8/CAD, and J-8/PBAD, participate in issue teams to provide the warfighter capability requirement perspective.

(c) The PBR provides a key opportunity to ensure that budgetary decisions are fully informed by the priorities of the validated capability requirements of the joint force. Ongoing capability requirement portfolio

management and prioritization, as well as the output of the most recent CGA and MRP provide essential context to discussions during PBR.

1. As part of robust capability requirement portfolio management, FCBs and other stakeholders should be ready to introduce issue papers into the PBR where the POM submissions are not aligned with the priorities within the capability requirement portfolios, or where earlier decisions as part of the review and validation of capability requirements are not reflected in the POM submissions.

2. FCBs and other stakeholders should also review issue papers submitted to PBR from other sources in the context of the impact they may have on the capability requirements and priorities within the capability requirement portfolios, dependencies within and across capability requirement portfolios, and potential impact to operational risk for the joint force.

3. At the end of PBR, as a result of the budgetary decisions made, assessments should be updated to reflect the latest decisions relating to funding (or not) of capability solutions addressing the capability requirements within each capability requirement portfolio.

(d) In cases where PBR directs funding be made available to address issues not already supported by validated capability requirements, the FCBs will provide recommendations to the JROC to facilitate Sponsor development of the appropriate capability requirement document for review and validation.

(4) Other Capability Requirement Portfolio Assessments. The FCB chairs also have responsibility for monitoring ongoing activities impacting their capability requirement portfolios, such as progress of AoA efforts and other acquisition activities, implementation of Joint DCRs, progress in satisfying JUONs, JEONs, and DOD Component UONs, etc. The FCB chairs may have the need to assess their capability requirement portfolios at other times throughout the year for a number of different reasons, including but not limited to:

(a) The Vice Chairman of the Joint Chiefs of Staff (VCJCS) or other senior leadership may request an assessment of a capability requirement portfolio or sub-portfolio to inform their decision making on a particular topic, or to potentially identify new opportunities in a particular area.

(b) The FCB chair may direct a capability requirement portfolio baseline assessment to better inform annual reviews such as CGA, PBR, or MRP.

(c) A change in strategic guidance or other event may have such a significant impact on the content or priorities of a capability requirement portfolio that a reassessment is needed to adjust the focus of efforts related to that capability requirement portfolio.

(5) Interactions with the JSPS. Management and prioritization of the capability requirement portfolios can provide robust support to, as well as be impacted by, activities of the JSPS outlined in reference u.

(a) Comprehensive Joint Assessment (CJA). This annual survey is used in part as the means by which the CCMDs provide their IPL inputs to initiate the annual CGA conducted in accordance with references a, b, and this manual.

(b) Joint Strategy Review (JSR). The JSR has several components which impact the management and prioritization of the capability requirement portfolios.

1. Joint Intelligence Estimate (JIE), Joint Strategic Assessment (JSA), and JSR Report. The JIE, JSA, and JSR provide important context for the evaluation of capability requirement portfolios and contribute to the left and right sides of the CML.

2. Joint Concept Development (JCD). JCD considers CJA and other inputs to assess progress in the implementation of approved joint concepts. These concepts provide a basis for Sponsors to develop implementation plans, identifying new or modified capability requirements for consideration in the JCIDS process. Details of JCD activities are in reference m.

3. Joint Logistics Estimate (JLE). The JLE evaluates how well the joint force can project, support, and sustain itself in the near-, mid-, and long-term, in support of the full range and number of missions called for in the NMS and JSCP. It should be informed by the capability requirement portfolio managed by the Logistics FCB, and may also identify new capability requirements and associated gaps for submittal into the JCIDS process.

4. Joint Personnel Estimate (JPE). The JPE evaluates how well the joint force develops and employs human capital over time, in support of the full range and number of missions called for in the NMS and JSCP. It should be informed by all stakeholders in Personnel issues in DOTmLPF-P across all capability requirement portfolios, and may identify issues which impact the ability to fully implement and sustain capabilities in the capability requirement portfolios.

5. Chairman's Risk Assessment (CRA). The CRA is the CJCS's assessment of the nature and magnitude of strategic and military risk in executing the missions called for in the NMS, and may include recommendations for mitigating risk, including changes to strategy, development of new Service or joint concepts, evolving capabilities, increases in capacity, or adjustments in force posture or employment.

a. The CRA informs the review and validation of capability requirements in the capability requirement portfolios during normal staffing activities as well as during CGA, PBR, and other periodic reviews.

b. The CRA should also be informed by the capability requirements and priorities in the capability requirement portfolios, and the acquisition activities underway to satisfy those capability requirements and reduce risk in conducting the missions called for in the NMS.

6. Operational Availability Studies. Operational availability study findings provide insights to draw inferences and establish linkages between current operations and the future. They may also identify capacity issues related to capabilities in the capability requirement portfolios, informing decision making related to quantities of systems required to support of the full range and number of missions called for in the NMS and JSCP.

(c) Continuous Assessment Processes under JSPS

1. Joint Combat Capability Assessment (JCCA). The JCCA is the near-term analysis of readiness and ability to execute required priority plans, and informs Global Force Management (GFM) sourcing decisions and CJCS risk assessments in accordance with reference v. In cases where GFM cannot source the required capabilities and resulting risks are unacceptable, the JCCA may serve as the basis for quantity adjustments or new capability requirements being introduced into the JCIDS process.

2. Chairman's Readiness System (CRS). The CRS provides a common framework for conducting commanders' readiness assessments and enables leadership to gain greater visibility on readiness issues across the CCMDs, Services, and Combat Support Agencies (CSAs) in accordance with reference w. The CRS is also supplemented by CSA Review Team assessments performed in accordance with reference x.

3. Global Force Management (GFM). The GFM process provides near term sourcing solutions while providing the integrating mechanism between force apportionment, allocation, and assignment in accordance with references y and z. In cases where GFM cannot source the required capabilities and resulting risks are unacceptable, the JCCA may serve as the

basis for quantity adjustments or new capability requirements being introduced into the JCIDS process.

a. Interaction between the GFM and JCIDS processes is essential to ensure the optimum balance between validated capability requirements, force structure quantities, and allocation to address joint force priorities.

b. An instance of the GFM process not sourcing the forces requested does not necessarily imply that additional quantities of capability solutions are required, or new capability requirements should be submitted to the JCIDS process. However, significant or repetitive shortfalls in GFM sourcing may be reason to reassess capability requirement portfolios and, if required, adjust priorities and/or quantities of capability solutions.

(d) Chairman's Advice and Direction

1. Chairman's Program Recommendation (CPR). The CPR provides the CJCS's personal recommendations to the Secretary of Defense, and informs the DPG and influences resource decisions and development of the President's Budget.

a. The CPR articulates issues the CJCS deems important enough for the Secretary to consider when identifying DOD strategic priorities in the DPG. The CPR is informed by the annual CGA activities executed under the JCIDS process, and the assessment and prioritization of the capability requirement portfolios.

b. Since the CPR is personal correspondence to the Secretary of Defense, the document is not presented to the JCB and JROC for approval.

2. Chairman's Program Assessment (CPA). The CPA provides the CJCS's personal assessment to the Secretary of Defense on the adequacy of DOD Component POMs submitted in the most recent cycle and may be considered in refining the Defense program and budget.

a. The CPA addresses risk associated with the programmed allocation of Department resources and evaluates the conformance of POMs to the priorities established in strategic plans and CCMD priorities for capability requirements.

b. The CPA also assesses the recommendations and execution of those issues highlighted in the CPR. FCBs, together with J-8/JRAD, J-8/CAD, and J-8/PBAD, assist in the development of the CPA by

identifying and articulating candidate issues, conducting supporting research and assessments, and developing summaries of the candidate issues.

c. Since the CPA is personal correspondence to the Secretary of Defense, the document is not presented to the JCB and JROC for approval.

3. National Military Strategy (NMS). The purpose of the NMS is to prioritize and focus military efforts while conveying the Chairman's advice with regard to the security environment and the necessary military actions to protect vital national interests. The NMS provides military ends, ways, and means that inform development of the GEF and the development of joint force capabilities. As such, it serves as a key piece of strategic guidance when assessing and prioritizing the capability requirement portfolios.

4. Joint Strategic Capabilities Plan (JSCP). The JSCP provides guidance to accomplish tasks and missions based upon near-term military capabilities, and implements campaign, campaign support, contingency, and posture planning guidance reflected in the GEF.

a. Assessment and prioritization of the capability requirement portfolios should align with the guidance and assumptions of the JSCP.

b. The planning efforts executed under the JSCP may lead to identification of new or modified capability requirements, which may then be documented and submitted to JCIDS for review and validation.

b. Joint DCR Implementation

(1) Implementation plan refinement. The Sponsor of a Joint DCR or designated lead organization, together with the chair of the lead FCB and the affected Joint DOTmLPF-P Functional Process Owners (FPOs) identified in Table D-5, shall refine implementation plan(s) and associated POCs within each OPR to address the tasks identified in the validated Joint DCR within the timeline delineated in the validation JROC Memorandum (JROCM).

(a) The Sponsor or designated lead organization, with the support of the FCBs and the affected Joint DOTmLPF-P FPOs, ensures that each task is completed in accordance with the timeline, and provides status of, and visibility into, the process to senior leaders.

(b) The Sponsor or designated lead organization, with the support of the FCBs and the affected Joint DOTmLPF-P FPOs, also makes recommendations to the validation authority for modifications to timelines, as needed, based upon the synchronization of tasks.

(2) Implementation progress monitoring. As Joint DCRs are the means to implement non-materiel capability solutions – either independently or in conjunction with materiel capability solutions – the FCB Chair must maintain awareness of implementation progress, and associated impact to their capability requirement portfolio.

(a) In cases where a Sponsor or designated lead organization proposes an altered timeline or approach to implementing the Joint DCR, the FCB chair must assess changes to operational risk from the proposed changes, as well as impact of the change upon enabling or enabled capability solutions related to the capabilities being implemented by the Joint DCR.

(b) The FCBs are responsible for coordinating assigned tasks with the Sponsor or designated lead organization via FCB processes, and for providing periodic updates on implementation progress to the O-6 and GO/FO Integration Groups. If unresolved issues occur, and cannot be adjudicated at the O-6 or GO/FO Integration Groups, the validation authority will provide appropriate resolution.

(3) Documenting Joint DCR completion. When the lead FCB determines that all tasks associated with a Joint DCR have been completed, the FCB Chair shall document completion in a memorandum to be posted with the original Joint DCR and validation memorandum in the KM/DS system.

c. Interaction with Deliberate Acquisition Activities

(1) Overview of deliberate acquisition. Deliberate acquisition begins when an appropriate MDA considers, along with other pertinent information, a validated ICD, CDD, or CPD, identifying one or more capability requirements which may be best addressed with a new materiel capability solution, and documents a positive Materiel Development Decision (MDD) in an Acquisition Decision Memorandum (ADM) in accordance with references aa and bb. The ADM may also direct entry at the appropriate acquisition phase, depending upon the maturity of potential capability solutions for the validated capability requirements.

(2) Planned requirement reviews. Each of the planned reviews below are key aspects of ensuring that appropriate tradeoffs are made among life cycle cost, schedule, performance, and procurement quantities in the establishment and approval of military requirements in accordance with reference cc. See Figure B-5 for the nominal process overview, and see Enclosure D of this manual for additional detail related to documents and sequence variations.

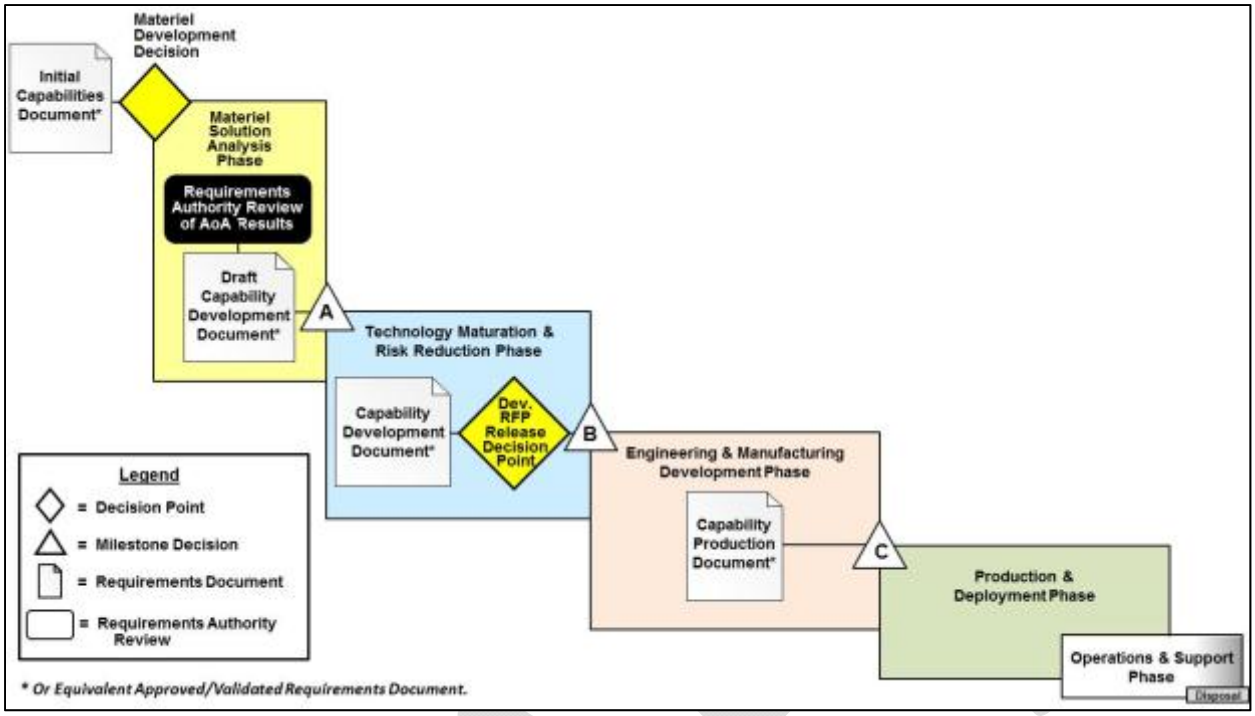

Figure B-5: JCIDS and DAS Process Interactions (Deliberate Process)

(a) ICD validation

1. Prior to validation, the draft ICD provides the validation authority and other stakeholders the opportunity to assess how the identified capability requirements, associated capability gaps, and other supporting data, impact the capability requirement portfolios. During staffing, the validation authority and other stakeholders have the opportunity to recommend modifications to the document, including the operational attributes and initial objective values which make up the capability requirements, to best address the needs of the joint force and to manage and prioritize the capability requirement portfolios.

2. The validated ICD is a critical entry criterion for the MDD, and guides the Sponsor activities during the Materiel Solution Analysis (MSA) phase of acquisition, assessment of potential materiel solutions through an AoA or similar studies, identifies associated DOTmLPF-P changes, and guides development of other acquisition information required for the Milestone (MS) A review.

(b) Post-AoA (or similar study) review

1. Following Sponsor completion of the AoA, or similar study conducted in place of an AoA, this review provides the validation authority and other stakeholders the opportunity to assess how the different alternatives address the validated capability requirements and associated capability gaps,

to ensure that critical dependencies/enablers and assumptions have been considered, and to understand the associated life cycle costs. It also provides the opportunity to review the results of other activities completed during the MSA phase of acquisition, and the proposed KPPs, key system attributes (KSAs), and additional performance attributes (APAs) for the recommended alternative(s).

a. The review considers all alternatives for not only highest performance in meeting validated capability requirements, but for cost-effectiveness and associated risk in meeting incrementally fewer or lesser requirements - determining the 'knee in the curve' of diminishing return on investment with acceptable risk.

b. The review is not a validation of the results, but rather informs the validation authority's advice to the MDA on the results, recommended alternative(s), and proposed KPPs, KSAs, and APAs consistent with the updated CONOPS and/or Operational Mode Summary/Mission Profile (OMS/MP) documentation. The validation authority may recommend alternative(s) different from those recommended by the sponsor when such a recommendation would better serve the management and prioritization of the capability requirement portfolio.

2. The review shall be completed in sufficient time to permit Sponsor preparation and approval of a draft CDD to inform both the development of the Request for Proposals (RFP) in support of the Technology Maturation and Risk Reduction (TMRR) phase of acquisition and the MS A decision. The draft CDD, prepared and approved by the Sponsor but not submitted to the Joint Staff Gatekeeper for staffing and validation at that time, is a critical entry criterion for the MS A.

3. In cases where MS A is not required, the review by the validation authority shall be completed before the next directed MS or the release of the RFP for the subsequent phase of acquisition, whichever comes first. If a formal AoA or similar study is not appropriate, the MDA will coordinate with the validation authority to ensure that the validation authority has the proper information to advise the MDA.

(c) CDD validation

1. Prior to validation, review of the CDD provides the validation authority and other stakeholders the opportunity to assess how the proposed capability solution, its associated development KPPs, KSAs, and APAs, and other supporting data, address the validated capability requirements. During staffing, the validation authority and other stakeholders have the opportunity to recommend modifications to the document, including the development KPPs, KSAs, and APAs and associated threshold/objective values, to best address the

needs of the joint force and to manage and prioritize the capability requirement portfolios.

a. The development KPPs, KSAs, and APAs set in the CDD do not necessarily need to achieve 100% of the initial objective values of operational attributes validated in the ICD, although the validation authority and other stakeholders will assess the operational risk and impact to the capability requirement portfolios of performance above or below the previously validated values.

b. Establishing development KPPs, KSAs, and APAs which represent a cost effective "knee in the curve" with respect to the initial objective values of operational attributes validated in the ICD is a key aspect of incorporating knowledge gained during the MSA and TMRR phases of acquisition. This ensures that appropriate tradeoffs are being made among life cycle cost, schedule, performance, and procurement quantities to manage and prioritize the capability requirement portfolios.

2. The validated CDD is a critical entry criterion for the development RFP release and MS B decision points, and guides the Sponsor in activities during the Engineering and Manufacturing Development (EMD) phase of acquisition. The validated CDD is a key factor in the MDA decision to initiate an acquisition program at MS B. In cases where MS B is not required, but an EMD phase of acquisition will be conducted, the CDD shall be validated ahead of the release of the RFP for the EMD phase of acquisition or the beginning of the EMD phase of acquisition, whichever comes first.

(d) CPD validation

1. Prior to validation, the draft CPD provides the validation authority and other stakeholders the opportunity to assess how the capability solution, its associated production KPPs, KSAs, and APAs, and other supporting data, address the validated capability requirements. During staffing, the validation authority and other stakeholders have the opportunity to recommend modifications to the document, including the production KPPs, KSAs, and APAs and associated threshold/objective values, to best address the needs of the joint force and to manage and prioritize the capability requirement portfolios.

a. The production KPPs, KSAs, and APAs set in the CPD do not necessarily need to be a 100% match to the development KPPs, KSAs, and APAs validated in the CDD, although the validation authority and other stakeholders will assess the operational risk and impact to the capability requirement portfolios of any proposed deviations from the previously validated values.

b. Proposing adjusted production KPPs, KSAs, and APAs from the validated development KPPs, KSAs, and APAs is a key aspect of incorporating knowledge gained during the EMD phase of acquisition, and to ensure that appropriate tradeoffs are being made among life cycle cost, schedule, performance, and procurement quantities to manage and prioritize the capability requirement portfolios.

2. The validated CPD is a critical entry criterion for the MS C, and guides the Sponsor in activities during the Production and Deployment (P&D) phase of acquisition. The validated CPD is a key factor in the MDA decision to initiate production of the capability solution at MS C. In cases where MS C is not required, the CPD shall be validated ahead of the release of the RFP for the P&D phase of acquisition or the beginning of the P&D phase of acquisition, whichever comes first.

(3) Event Driven Requirement Reviews

(a) Changes to validated capability requirements

1. There may be cases where it is necessary to change KPPs, KSAs, APAs, or other aspects of a validated capability requirement document, due to factors related to life cycle cost, technology, production, development, or other issues that prevent meeting performance thresholds.

a. When the JCB or JROC is the validation authority, except within the scope of specific change authorities delegated by the JCB or JROC to the Sponsor, the Sponsor may request changes through the Joint Staff Gatekeeper. When a Sponsor proposes such a change, the updated document will be submitted for review and revalidation by the appropriate validation authority.

b. When the Sponsor is the validation authority, or within the scope of specific change authorities delegated by the JCB or JROC, the Sponsor may make changes as they deem appropriate. The updated document and its associated change approval memorandum are provided to the Joint Staff Gatekeeper for archiving.

c. Any changes potentially impacting certifications or endorsements will be reviewed by the applicable certification or endorsement authorities outlined in Enclosure E of this manual.

2. Changes to previously validated capability requirement documents will be assessed for operational risk and other impact to the management and prioritization of the capability requirement portfolios.

(b) JROC/JCB Tripwire Reviews

1. The JROC/JCB Tripwire review is a JCIDS activity for JROC and JCB Interest programs which enable re-examination of validated capability requirements, and the balance between performance levels and operational risk, to mitigate challenges in acquisition programs. Tripwire reviews are triggered by deviations from program acquisition unit cost (PAUC) or average procurement unit cost (APUC), schedule, or quantity targets established at the time of validation.

a. The JROC/JCB Tripwire review applies to capability requirements identified in CDDs or CPDs, as well as information systems ICDs.

b. The JROC/JCB Tripwire review also applies in cases of program cancellation, as this represents an extreme case of schedule and quantity change.

2. In considering programs under JROC/JCB Tripwire review, the FCB chair and other stakeholders involved in the review and validation of the capability requirements evaluate the operational risk or other impact to the capability requirement portfolio and priorities if changes to cost, schedule, or quantity persist, or whether a lower level of one or more KPPs, KSAs, or APAs can be accepted at reasonable risk or impact to help mitigate the trigger conditions.

3. The following trigger values apply unless tailored by the validation authority:

a. Cost. Programs must return to the JROC or JCB for re-validation if they experience a PAUC or APUC growth equal to or greater than 10 percent over their current baseline or 25 percent over their original baseline as defined in the Acquisition Program Baseline (APB).

b. Schedule. Programs must return to the JROC or JCB for re-validation if they experience a schedule slip for IOC or FOC equal to or greater than 12 months from IOC and FOC targets set in the validation JROCM.

c. Quantity. Programs must return to the JROC or JCB for re-validation if they experience a reduction in operational inventory quantities equal to or greater than 10 percent from the quantity target set in the validation JROCM.

(1) Changes to production quantities intended solely to accommodate unexpected attrition, or expenditure in the case of munitions and other expendables, and maintain the required operational inventory, do

not trigger JROC/JCB Tripwire reviews and do not require re-validation of the capability requirements.

(2) Changes to production quantities which result in changes to the operational inventory, or lack of changes to production quantities necessary to maintain operational inventory when expenditure rates change, will trigger JROC/JCB Tripwire reviews, and require revalidation of required operational inventory quantities and/or acceptance of the altered operational risk.

4. See Enclosure F of this manual for details of the JROC/JCB Tripwire review process.

(c) Critical Intelligence Parameter (CIP) Breach Review

1. A CIP breach review is a collaborative assessment of the relationship between a changing CIP - specific quantity, type, system capabilities, and technical characteristics or performance threshold of a particular foreign capability such as radar cross-section, armor type or thickness, or acoustic characteristics - and the related KPPs, KSAs, and/or APAs validated in a CDD or CPD for one or more capability solutions.

2. The review is conducted by a risk mitigation team comprised of program office, capability Sponsor, capability developer, FCB representatives, and other applicable stakeholders.

3. When the supporting military Service Intelligence center determines a CIP has been breached, notification of the breach will be made to appropriate offices in DoD, and the program office(s) and FCB(s) impacted by the breach.

4. The purpose of the CIP breach review is to:

a. Assess the impact of changes to adversary capabilities related to the CIP and determine if the breach compromises mission effectiveness of current or future capability solution(s).

b. Assess whether other current or future capability solutions, within and across the capability requirement portfolios, are impacted by the CIP breach.

c. Determine appropriate responses and/or risk mitigation efforts which balance potential increase in operational risk or costs with decisions to pursue (or not pursue) potential non-materiel and materiel changes.

5. CIP Breach Reviews may use review procedures similar to JROC/JCB Tripwire reviews, as shown in Enclosure F of this manual but focusing on CIP parameter changes rather than cost, schedule or quantity changes.

(d) Nunn-McCurdy Unit Cost Breach Review

1. The Nunn-McCurdy Unit Cost Breach review activity is an USD(AT&L) process implemented to meet statutory review requirements in reference dd. More detail on Nunn-McCurdy Unit Cost Breach procedures are in references aa and bb.

2. In considering programs under Nunn-McCurdy Cost Breach conditions, the FCB chair and other stakeholders involved in the review and validation of the capability requirements evaluate the essentiality of the program to national security. For programs deemed essential to national security, they also evaluate operational risk or other impact to the capability requirement portfolio and priorities from potential changes to one or more KPPs, KSAs, APAs, schedule, or quantity, if such a change would to help mitigate the unit cost breach conditions. See Enclosure F of this manual for details of JROC/JCIDS interaction with the Nunn-McCurdy Unit Cost Breach procedures.

(e) Major Automated Information System (MAIS) Critical Change Review

1. The MAIS Critical Change review activity is an USD(AT&L) process implemented to meet statutory review requirements in reference ee. More detail on MAIS Critical Change review procedures are in references aa, bb, and ff.

2. In considering programs under MAIS Critical Cost Change conditions, the FCB chair and other stakeholders evaluate the essentiality of the program to national security. For programs deemed essential to national security, they also evaluate operational risk or other impact to the capability requirement portfolio and priorities from potential changes to one or more KPPs, KSAs, APAs, schedule, or quantity, if such a change would to help mitigate the critical change conditions. See Enclosure F of this manual for details of JROC/JCIDS interaction with the MAIS Critical Change Review procedures.

(f) Upgrades and end of service life decisions

1. For incremental improvements to fielded capability solutions, through more capable production increments and/or retrofit of previously fielded systems, the need for a new or updated ICD, CDD, and/or CPD will be

determined by the validation authority after Joint Staff Gatekeeper and lead FCB review of the Sponsor proposed changes. If new capability requirement documents are not directed, the FCB Chair and other stakeholders will still assess the impact of the proposed capability improvements to the capability requirement portfolios in terms of reduced operational risk, opportunity cost of the upgrades which could otherwise be spent on other capabilities, etc.

2. For sustainment of previously fielded capability solutions, a new ICD, CDD, or CPD is not required to retain or restore capabilities or perform technology refresh of fielded systems that have a validated Operational Requirements Documents (ORD), ICD, CDD, or CPD. For example, subsystems that have approved performance parameters but are no longer able to meet those parameters can be updated or replaced to meet production threshold/objective values under the authority of the previously validated capability requirement document.

3. When a capability solution is approaching end of service life, there are three courses of action as shown in Figure B-6:

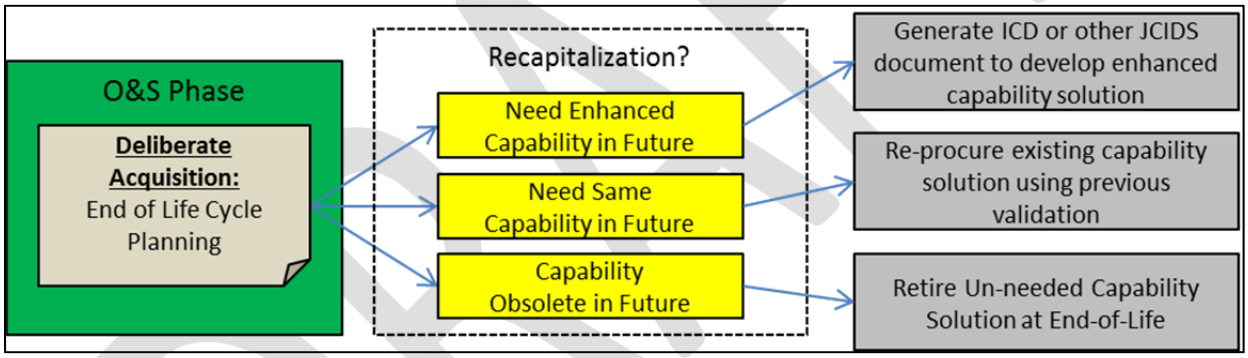

Figure B-6. End of the O&S Phase of (Deliberate) Acquisition

a. If the capability is obsolete or otherwise not required in the future, the validation authority will rescind the validation and the Sponsor will dispose of the capability solution. The capability requirement portfolio will be updated to reflect the removal of the capability requirements, and any associated changes to capability requirement portfolio priorities.

b. If the originally validated capability requirements remain valid, then a replacement capability solution can be acquired to meet the same performance attributes under the authority of the originally validated document. The capability requirement portfolio will be updated to reflect the continued satisfaction of the capability requirements through a replacement capability solution.

c. If adversary threats, strategic guidance, or other operational context have changed such that upgraded capabilities are required

for the replacement system, a new capability requirement document will be generated by the Sponsor. FCB Chairs and other stakeholders will assess impact to the capability requirement portfolios during staffing of the document.

d. Interaction with Rapid Acquisition Activities

(1) Overview of Rapid Acquisition. Rapid acquisition of a capability solution in response to a validated JUON, JEON, or DOD Component UON is accomplished in accordance with references bb and gg, with additional guidance for DOD Component UONs in references hh through oo. DoD Components use all available authorities to expeditiously fund, develop, assess, produce, deploy, and sustain these capabilities, and will delegate approval for those authorities to a level that promotes rapid action.

(a) Responding to validated JUONs, JEONs, and DOD Component UONs occurs in two steps after validation, which are overseen, prioritized, and facilitated, as necessary, by the Warfighter SIG.

1. Identification of a feasible capability solution that resolves or substantially mitigates the validated requirement.

2. Execution of a capability solution, including identification and prioritization of funding, and completion of any development, acquisition, training, and fielding.

(b) The PM, under the authority, direction, and control of the MDA, is responsible for all phases of the rapid acquisition process. The PM ensures that supporting actions during the O&S phase of acquisition are accomplished. The PM also ensures that funding requirements to accomplish all actions, and any shortfalls thereof, are quickly identified and elevated as necessary to appropriate DOD Component officials for resolution. See Figure B-7 for an overview of the rapid acquisition process.

DRAFT

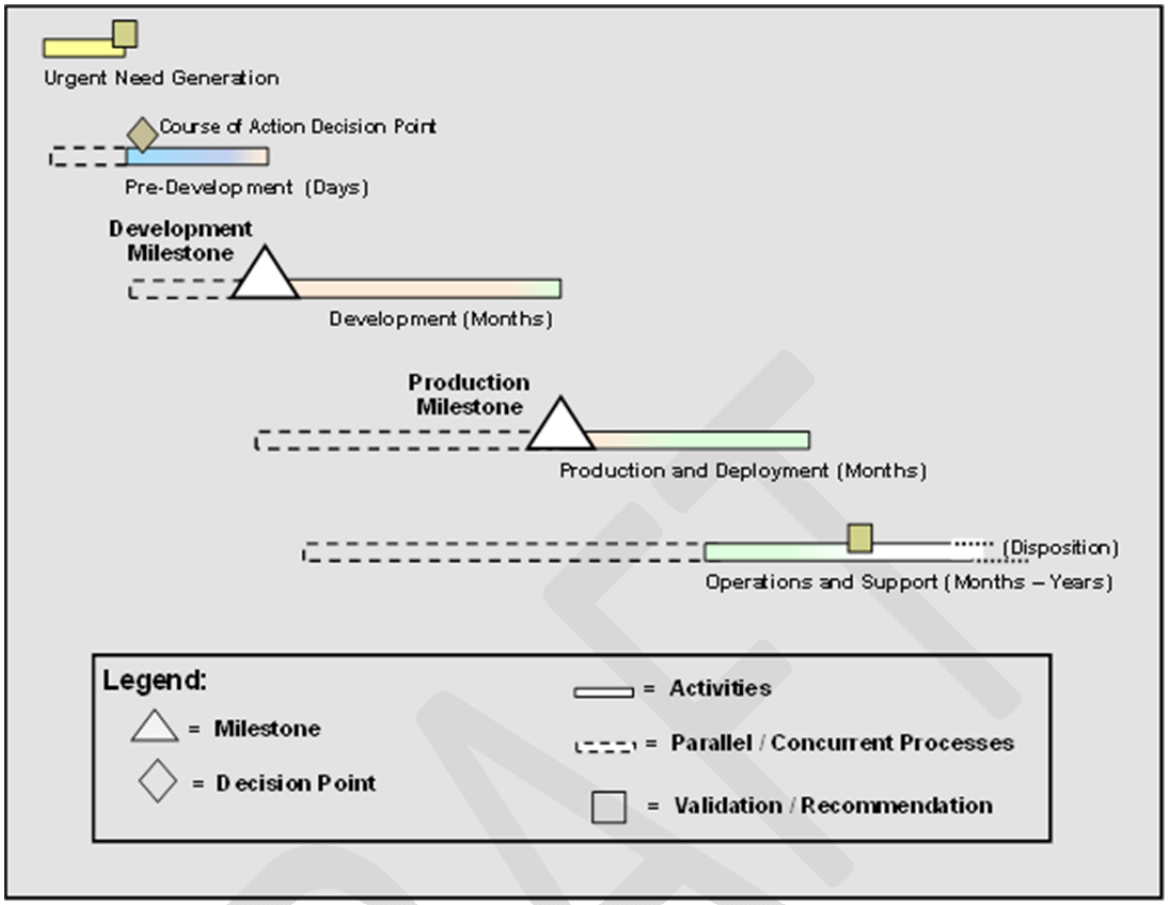

Figure B-7. Overview of the Rapid Acquisition Process.

(2) Periodic and Transition Review of Urgent and Emergent Capability Requirements.

(a) Post-fielding assessments of DOD Component UONs are at the discretion of the Sponsor.

(b) Validated JUONs and JEONs are reviewed quarterly by the Joint Staff Gatekeeper and the JRAC to assess progress toward fielding capability solutions in a timely manner. Progress reviews of validated DOD Component UONs are at the discretion of the Sponsor. See Enclosure G of this manual for more detail on periodic reviews.

(c) Once a capability solution has been fielded in response to a JUON or JEON, an Assessment of Operational Utility will be conducted in accordance with Enclosure G of this manual, resulting in one of the recommendations shown in Figure B-8. This assessment enables the validation authority to maintain visibility on the closure of urgent and emergent capability gaps, provide timely changes to previously validated JUONs or JEONs, and where applicable, validate enduring capability

requirements to support transition of rapidly fielded capability solutions to programs of record (PORs).

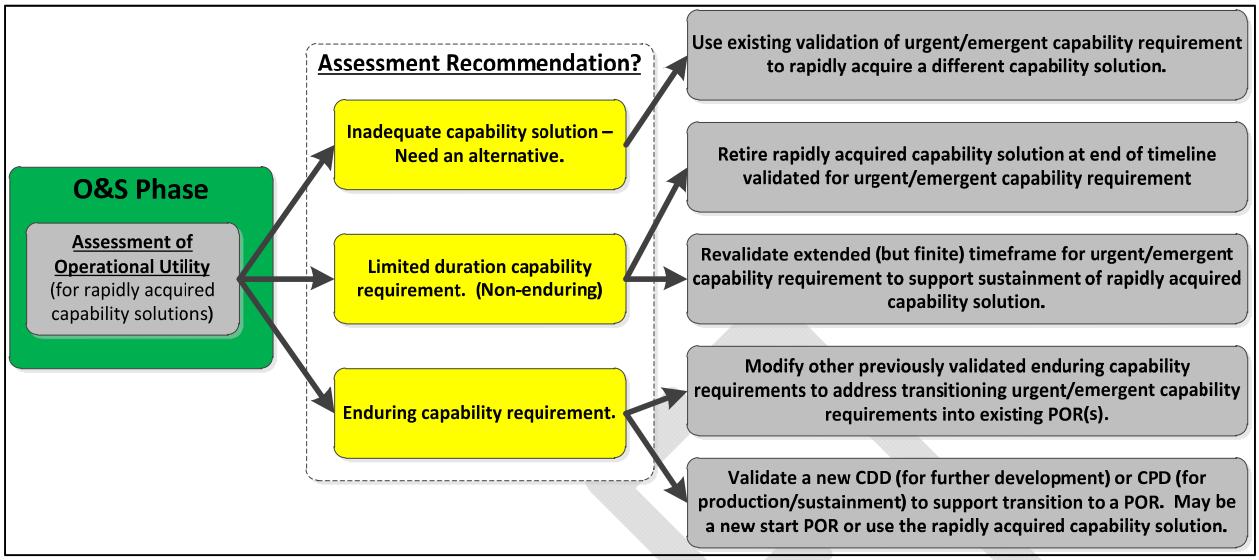

Figure B-8. End of the O&S Phase of (Rapid) Acquisition

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX A TO ENCLOSURE B

CAPABILITY GAP ASSESSMENT

1. Introduction

a. The CGA is a deliberate assessment by which the CJCS and JROC carry out statutory responsibilities outlined in references cc, and pp through rr. Responsibilities supported by the CGA include:

(1) Providing advice to the Secretary of Defense on the effect that critical force capability deficiencies and strengths will have on accomplishing national security objectives.

(2) Providing advice on program recommendations and budget proposals to conform to priorities established for the CCMDs and in strategic plans.

(3) Submitting to the congressional defense committees a report on the requirements of the CCMDs.

(4) Conferring with and obtaining information from the CCMDs and evaluating and integrating that information into his advice to the President and the Secretary of Defense.

(5) Assisting the Secretary of Defense with funding proposals for the CCMDs.

(6) Identifying and assessing the priority of joint military requirements and assigning joint priority among previously fielded and future programs meeting valid requirements.

b. The CGA is conducted in the context of capability requirement portfolio management described in Enclosure B of this manual, and may consider previously validated capability requirements as well as propose new capability requirements, and associated capability gaps, for review and validation.

c. The CGA examines identified capability gaps in the joint force from various perspectives, groups “like” capability gaps, assesses ongoing efforts to close or mitigate capability gaps, and recommends programmatic and/or non-programmatic approaches to close or mitigate capability gaps. See Figure B-A-1.

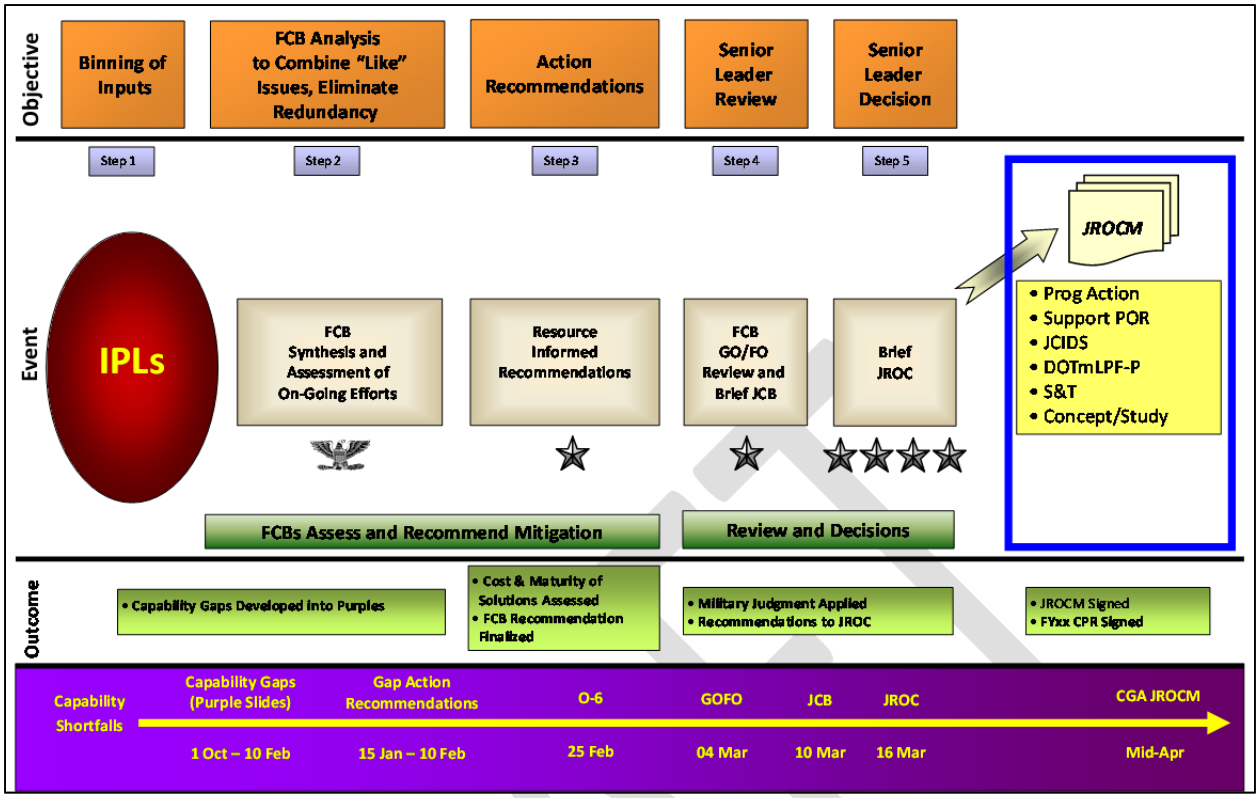

Figure B-A-1. CGA Storyboard.

2. Inputs to the CGA Process. The CGA process begins with the receipt of the IPLs provided by the CCMDs in response to the CJA and the Chairman's request for assessment of critical warfighter capability gaps linked to their top priority risk mitigation measures. Additional inputs include lessons learned, JCD needs, JUONs, JEONs, and Chief, National Guard Bureau (CNGB) issues. Since some inputs are received throughout the year, a "snapshot" of these inputs will be taken at the beginning of the CGA process to capture those issues to evaluate during assessment.

a. CCMD IPLs. Annually, the CCDRs submit a prioritized list of their most pressing capability gaps to the CJCS and the Secretary of Defense for inclusion in the Chairman's Annual Report to Congress. IPLs are intended to provide visibility for those few key problem areas which, in the judgment of the CCDR, require the highest priority attention by the DOD in finding capability solutions. The IPLs should include identification of the impacted UJTs and JCAs to tier 3 (or lower) in order to properly categorize the issues

b. Lessons learned. Lessons learned, in accordance with reference ss, are the discovery, validation, integration, evaluation, and dissemination of lessons from joint operations, training events, exercises, experiments, Title 10 wargames, and other activities in peacetime and war. Lessons learned

influence the CGA process by identifying capability gaps with the goal of delivering the best military capability solutions in support of national security.

c. JUONs and JEONs. JUONs and JEONs are evaluated to determine the extent to which they address any of the CCMD IPLs, or might be leveraged to address capability gaps identified by different CCMDs.

d. CNGB Issues. In response to the CJA, CNGB provide input to the CCMDs for inclusion in their IPLs high priority capability gaps, prioritized across Service and functional lines, risk area, and determining long-term strategic planning issues.

e. Non-CGA IPL Issues. Certain issues submitted within CCMD IPLs are not capability gaps and are outside the responsibilities of the JROC. Resolution or mitigation of these issues is handled outside the CGA process.

3. Synthesis of CGA Inputs

a. Synthesized Capability Gaps. FCBs may combine "like" capability gaps into a "synthesized capability gap." These synthesized capability gaps can be used to better manage the sheer number of capability gaps received. Combining "like" capability gaps also helps identify multiple stake holders with identical or similar issues, and allows both issues and potential capability solutions to be evaluated in a holistic approach.

b. Single Issue Capability Gaps. In many cases, analysis of a single IPL or input from a single CCMD will provide greater clarity in the analysis of operational risk and identification of ongoing efforts, which in turn will more easily identify the capability gap as a candidate for investing additional resources, maintaining current levels of resources, or accepting additional risk. Additionally, if the JROC recommends investment of additional resources, a focus area (e.g. CCMD of interest) can be more clearly identified in the recommended approach for a capability solution.

4. Stratification of Capability Gaps. As a deliberate assessment, the CGA indicates whether DOD efforts and resource investments are aligned with warfighter capability requirements, joint concepts, and strategic guidance.

a. In conducting the CGA, the FCBs review CJA inputs to develop a comprehensive list of the most pressing capability gaps.

b. This list of capability gaps is compared to the greatest risk drivers and events as articulated in the CRA. This framework provides a standardized approach to consistently portray risk across capability gaps and allows the JROC a qualitative prioritization of capability requirements.

c. FCBs categorize the capability gaps by risk and recommend risk mitigation if warranted.

d. The JROC is the final decision authority in the CGA and ensures that the timing of the output is sufficient to influence Service POM builds and the PBR.

5. Outputs from the CGA

a. As a result of the CGA, the JROC prioritizes and recommends approaches for mitigating capability gaps, with the resulting list published in a JROCM as a basis for follow-on actions.

(1) The CGA JROCM by itself does not replace the need for a validated capability requirement, but rather assigns priorities and recommends means for satisfying validated capability requirements.

(2) In cases where a capability gap identified in the CGA is not based upon a previously validated capability requirement, the CGA JROCM may be the basis for generation of the appropriate capability requirement documents for review and validation in accordance with this manual.

b. The CGA JROCM includes a list of capability gaps that require the DOD to invest additional resources, and will include the recommended actions for those capability gaps. It also includes a list of other capability gaps which are recommended to maintain current level of resources or to accept additional risk, and their respective recommendations. Generally there are six proposed strategies that the JROC may recommend to close or mitigate capability gaps:

(1) Programmatic Action. Additional resources applied to current or new programs that may close or mitigate the capability gap.

(2) Capability Development. Actions are required to assist in identification and development of a capability solution that may close or mitigate the capability gap.

(3) S&T. Current and possible new areas of research and development with recommended attributes of potential technologies that may contribute to capability solutions to close or mitigate the capability gap.

(4) JCD. Current and possible new areas of JCD that may provide or enable capability solutions to close or mitigate the capability gap.

(5) Study. A defined problem, scope, and expected process or organization the study will inform.

(6) DOTmLPF-P. Recommended non-materiel changes that should be made to close or mitigate the capability gap. Materiel portions of this recommendation are restricted to commercial or non-development items, which may be purchased commercially, or by purchasing more quantity of a previously fielded capability solution.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

ENCLOSURE C

INITIAL IDENTIFICATION OF CAPABILITY REQUIREMENTS AND ASSOCIATED CAPABILITY GAPS

1. Overview

a. Fundamental goal. The fundamental goal of any approach outlined in this section is for a Sponsor to derive and refine capability requirements and associated capability gaps – for which a capability solution must be provided either organically or leveraged through the joint force – to accomplish assigned functions, roles, missions, and operations.

b. Use of certified requirements managers. Sponsors will use certified requirements managers, as described in Enclosure A, to monitor and evaluate capability requirement identification, including but not limited to the identification of capability gaps due to changes in threats, missions, or aging of legacy weapon systems throughout their life cycle.

c. Relation to functions, roles, missions, and operations. Before any action can be taken in the JCIDS process related to reviewing and validating capability requirement documents, Sponsors must first identify capability requirements related to their functions, roles, missions, and operations.

(1) Sponsors may pursue a variety of approaches to determine their organizational capability requirements, depending upon the timeliness of the assessment and the scope of the activities being reviewed. Due to the wide array of issues that may be considered, the breadth and depth of each approach must be tailored to suit the issue. The approach must be sufficient to develop coherent and well-supported recommendations, which the validation authority will then use to validate the capability requirements and associated capability gaps to support possible follow-on actions.

(2) While Sponsor activities may examine various aspects of their capability requirements in significant levels of detail, the key for JCIDS is to identify the high level operational capability requirements, establish quantifiable attributes and metrics, and articulate the traceability from those capability requirements to the tasks, missions, threats, and overall strategic guidance. See Appendix A of this enclosure for additional guidance on selecting operational attributes for capability requirements.

(3) For each identified capability requirement, Sponsors then compare them to current and programmed future capability solutions, if any, to determine if there are any capability gaps which present an unacceptable level of risk and warrant further development of materiel or non-materiel capability solutions to mitigate or eliminate the capability gaps.

(4) When the operational risks involved with not closing the capability gaps outweigh the potential resources associated with pursuing a capability solution and potential operational risks introduced by removing the resources from other efforts, the Sponsor may recommend the most appropriate path forward to satisfy the capability requirements and reduce or eliminate any associated capability gaps.

d. Leverage of prior efforts. The Sponsor must identify and build upon any previous CBAs, studies, and other analytical products applicable to the area of interest. In addition to analytic products available within the Sponsor's organization, previous studies may also be accessible through the KM/DS system at the URL in reference h. The intent is to avoid any unnecessary repetition of prior efforts, and provide continuity between analyses for reviewers and decision makers. This does not preclude the Sponsor from applying different context or different assumptions, as appropriate for the approach being pursued.

2. Approaches to Identifying Capability Requirements

a. Considerations. Any approach taken by a Sponsor must address the following areas:

(1) Description of the mission and military problem being assessed.

(2) Identification and assessment of prior CBAs, studies, and other analytical products applicable to the area of interest.

(3) Identification of the tasks to be completed to meet the mission objectives.

(4) Identification of the capability requirements within one or more of the JCAs, described in terms of the tasks, performance, and conditions.

(5) Assessment of capability gaps between the identified capability requirements and current or programmed capabilities across the joint force.

(6) Assessment of operational risks associated with each capability gap if not addressed.

(7) Evaluation of possible non-materiel and materiel approaches to satisfy part or all of the capability requirements and close or mitigate the associated capability gaps.

(8) Evaluation of current and potential future S&T efforts which may enable a future capability solution, or future enhancements to current or proposed capability solutions.

(9) Recommendation for the most appropriate approach to be taken to close or mitigate capability gaps and reduce operational risk.

b. Solution independence. The Sponsor should not presuppose a specific capability solution or end item, but provide data related to forms and functions of potential solutions to support the development of capability requirement documents. The final recommendations should include a focused and concise justification for the proposed action.

c. Primary types of approaches. Approaches for identifying capability requirements may include, but are not limited to:

(1) CBAs and other studies

(a) The CBA provides an analytic basis to identify capability requirements and associated capability gaps prior to development and submission of capability requirement documents for review and validation.

1. Details of the CBA process are in Appendix B to this enclosure and in references tt through vv.

2. Applicable joint concepts and associated implementation plans must be considered during CBAs and other analyses. Details of JCD activities are in reference m.

(b) DOTmLPF-P analysis is part of all CBAs, but may be used independently of a CBA when the scope of an issue being studied is not likely to result in new materiel solution development. The eight DOTmLPF-P areas are:

1. Doctrine. Fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Though neither policy nor strategy, joint doctrine serves to make US policy and strategy effective in the application of US military power. Joint doctrine is authoritative guidance and will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. Joint doctrine is based on existing capabilities in accordance with reference ww. Implementation of change recommendations to joint doctrine which are validated in the JCIDS process will be coordinated with the processes established in reference ww.

2. Organization. A joint unit or element with varied functions enabled by a structure through which individuals cooperate systematically to accomplish a common mission and directly provide or support joint warfighting capabilities. Subordinate units and elements coordinate with other units and elements and, as a whole, enable the higher-level joint unit or element to accomplish its mission. This includes the joint staffing (military, civilian, and contractor support) required to plan, operate, sustain, and reconstitute joint warfighting capabilities. Implementation of change recommendations to joint organizations which are validated in the JCIDS process will be coordinated with the processes established in reference xx.

3. Training. Training, including mission rehearsals, of individuals, units, and staffs using joint doctrine or joint tactics, techniques, and procedures to prepare joint forces or joint staffs to respond to strategic, operational, or tactical requirements considered necessary by the CCMDs to execute their assigned or anticipated missions. Training also pertains to non-materiel aspects of operation and maintenance of materiel solutions. Implementation of change recommendations to joint training which are validated in the JCIDS process will be coordinated with the processes established in reference yy.

4. Materiel. All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support joint military activities without distinction as to its application for administrative or combat purposes. The letter "m" in the acronym is usually lower case since Joint DCRs do not advocate new materiel development, but rather advocate increased quantities of fielded materiel capability solutions or use in alternate applications. Implementation of change recommendations to joint existing materiel which are validated in the JCIDS process will be coordinated with the Sponsor(s) responsible for the materiel impacted by the recommended change.

5. Leadership and Education. Professional development of the joint leader is the product of a learning continuum that comprises training, experience, education, and self-improvement. Joint professional military education complements training, experience, and self-improvement to produce the most professionally competent individuals possible. Implementation of change recommendations to joint leadership and education which are validated in the JCIDS process will be coordinated with the processes established in references zz and aaa.

6. Personnel. The personnel component primarily ensures that qualified personnel exist to support capability requirements across the joint force. This is accomplished through synchronized efforts of joint force commanders and DOD components to optimize personnel support to the joint

force to ensure success of ongoing peacetime, contingency, and wartime operations. Implementation of change recommendations to joint personnel which are validated in the JCIDS process will be coordinated with the processes established in reference bbb.

7. Facilities. Real property consisting of one or more of the following: buildings, structures, utility systems, associated roads and other pavements, and underlying land. Key facilities are defined as command installations and industrial facilities of primary importance to the support of military operations or military production programs. A key facilities list is prepared under the policy direction of the Joint Chiefs of Staff. Implementation of change recommendations to joint facilities which are validated in the JCIDS process will be coordinated with the processes established in references ccc and ddd.

8. Policy. Any DOD, other US government agency/department, or international policy issues that may be changed to close or mitigate a capability gap, or if unchanged, prevent effective implementation of changes in the other seven DOTmLPF-P elemental areas. Implementation of change recommendations to joint policy which are validated in the JCIDS process will be coordinated with the Joint Staff J-5 and the Under Secretary of Defense for Policy (USD(P)), and the process established in reference eee.

(c) The DOTmLPF-P Analysis generally results in one or more DCRs without an associated ICD.

1. DCRs which impact only the Sponsor organization may be reviewed, validated, and implemented in accordance with DOTmLPF-P policies and processes of that organization.

2. DCRs which impact multiple organizations typically lead to a Joint DCR for review and validation. Details of Joint DCRs are in Enclosure D of this manual.

(d) Other studies. Organizations may conduct other forms of studies, analyses, or assessments which cover some aspects of what is typically covered in CBAs and DOTmLPF-P analysis. These other studies may be used as sources of capability requirements, but may need to be augmented or further refined through additional efforts before having sufficient data to properly quantify capability requirements and generate capability requirement documents.

(2) Operational Planning. Operational planning is performed in accordance with references fff through iii.

(a) Development of OPLANs and CONPLANs is one means to identify capability requirements related to CCMD roles and missions and the assignment or attachment of forces. Capability requirements identified during planning may require additional analysis as outlined for CBAs prior to submission of capability requirement documents for review and validation.

(b) Planning for ongoing contingency operations may identify capability requirements which represent potential for critical mission failure or unacceptable loss of life if not satisfied in a compressed timeframe impractical to address with deliberate processes. These capability requirements may qualify for submission as JUONs or DOD Component UONs for expedited validation and rapid acquisition efforts in order to satisfy the validated capability requirement in the operational timeframe. Details of JUON documents are in Enclosure D of this manual, and details of DOD Component UONs are in references hh through oo. Warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed in accordance with reference gg.

(c) Planning for anticipated contingency operations may identify capability requirements which represent potential for critical mission failure or unacceptable loss of life once operations commence, if not satisfied in a compressed timeframe impractical to address with deliberate processes. These capability requirements may qualify for submission as JEONs, or DOD Component UONs if Sponsor processes allow, for expedited validation and rapid acquisition efforts in order to satisfy the validated capability requirement in the operational timeframe. Details of JEON documents are in Enclosure D and details of DOD Component UONs are in references hh through oo. Warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed in accordance with reference gg.

(d) JUONs, JEONs, and DOD Component UONs should only be generated when other means to satisfy the capability requirement are not practical – Global Force Management (GFM) process for the allocation and assignment of forces, Joint Manpower Validation Process (JMVP) for the allocation and assignment of personnel, deliberate requirements and acquisition for development of new/additional capabilities, etc. While fielding a capability solution in less than two years is a typical goal, JUONs and JEONs may also be validated to support near-term resourcing and initiation of efforts to field capability solutions in greater than two years.

(3) Exercise/Warfighting Lessons Learned. Warfighting and exercise lessons learned may serve as a basis to establish capability requirements, if the documentation suggests that mitigation of capability gaps and reduction in operational risk is worth the resources required to implement the change. Lessons Learned may require additional analysis as outlined for CBAs prior to

development of capability requirement documents for validation in the deliberate or urgent/emergent staffing processes. See reference kk for more details of the Joint Lessons Learned Program.

(4) Joint Capability Technology Demonstrations (JCTDs) and other experiments. At a minimum, assessments of JCTDs and other completed experimentation must, if applicable, establish the operational utility of the capability solution and provide the basis for establishing an enduring capability requirement. The scope of the assessment may be tailored depending upon the level of detail available to the Sponsor and the nature of the demonstrated capability solution.

(a) An assessment may be a suitable replacement for analysis used as the basis for ICD, CDD, or CPD preparation, depending upon the maturity of the capability solution. In these cases, assessments should contain the critical elements of information that are described for CBAs and required in the capability requirement documents, including description of the capability requirements and associated gap(s); associated tasks, conditions, and operational performance standards/metrics; and how the materiel and non-materiel approaches address these factors.

1. JCTDs or other prototypes tested in the field may serve as a basis to establish capability requirements, if an assessment indicates sufficient military utility of a demonstrated capability solution. More information on JCTDs is available from the JCTD Office in reference jjj.

2. Documentation of joint or DOD Component experimentation may serve as a basis to establish capability requirements, if the documentation indicates sufficient military utility of a certain capability.

(b) If the assessment does not provide sufficient detail to fully develop capability requirement documents, additional studies or analysis as outlined for CBAs may be used to complement the data available from the assessment.

(5) Transition of Rapidly Fielded Capability Solutions

(a) JUONs, JEONs, and DOD Component UONs. Successful capability solutions for JUONs, JEONs, and DOD Component UONs may serve as a basis for validating enduring capability requirements to support transition of rapidly fielded capability solutions for sustainment and/or further development if they have a positive assessment of operational utility documented by the original requirement Sponsor.

a. See Enclosure G of this manual for details of assessments of operational utility for rapidly fielded capability solutions in support of JUONs

and JEONs. An assessment for a capability solution initiated through a JUON or JEON does not need to duplicate information already contained in the validated JUON or JEON. However, the assessment may address refinements to the original capability requirements as needed to reflect lessons learned from operating the rapidly fielded capability solution.

b. Assessment of successful DOD Component UONs intended for transition to enduring capability requirements is at the discretion of the Sponsor. Information to support the associated ICD, CDD, or CPD for validation will be consistent with other guidance in this manual.

c. If the assessment does not provide sufficient detail to fully develop capability requirement documents, additional studies or analysis as outlined for CBAs may be used to complement the data available from the assessment.

(b) Joint Improvised Explosive Device (IED) Defeat Initiative. The Joint IED Defeat Transition Packet, which is completed after the Joint IED Defeat Organization (JIEDDO) validates an initiative, may serve as a basis for establishing capability requirements. The Transition Packet will be used as the source document for developing a CDD or CPD for subsequent review, validation of capability requirements, and transition of the capability solution to a POR. See reference kkk for more detail of JIEDDO transition activities.

(7) Business Process Reengineering. Regardless of life cycle cost, IS, other than a national security system, operated by, for, or on behalf of the DOD, including financial systems, mixed systems, financial feeder systems, and IT and cybersecurity infrastructures, are DBS.

(a) DBS support business activities such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management, and generally are validated by the Investment Review Board (IRB), under the guidance of the DBS Management Committee as outlined in references bb and lll. Acquisition of DBS employs problem statements and business case documents in lieu of ICDs and CDDs to document the capability requirements and associated capability solutions.

(b) The Joint Staff representative to the Defense Business Council (DBC) will perform an initial review and forward at his/her discretion, based on an assessment of business and warfighter equity, problem statements and business case documents to the Joint Staff Gatekeeper and appropriate FCB. In those cases where the Joint Staff Gatekeeper, on the advice of the appropriate FCB, determines that JCB or JROC oversight of the DBS is required, the problem statement and business case documents will be used in

lieu of the typical capability requirement documents used in JCIDS staffing and validation.

3. Determination of Appropriate JCIDS Action. A combination of actions may represent the most appropriate means of mitigating or closing the identified capability gap(s). Figure C-1 illustrates the typical JCIDS actions related to addressing capability gaps, which are detailed in the following paragraphs.

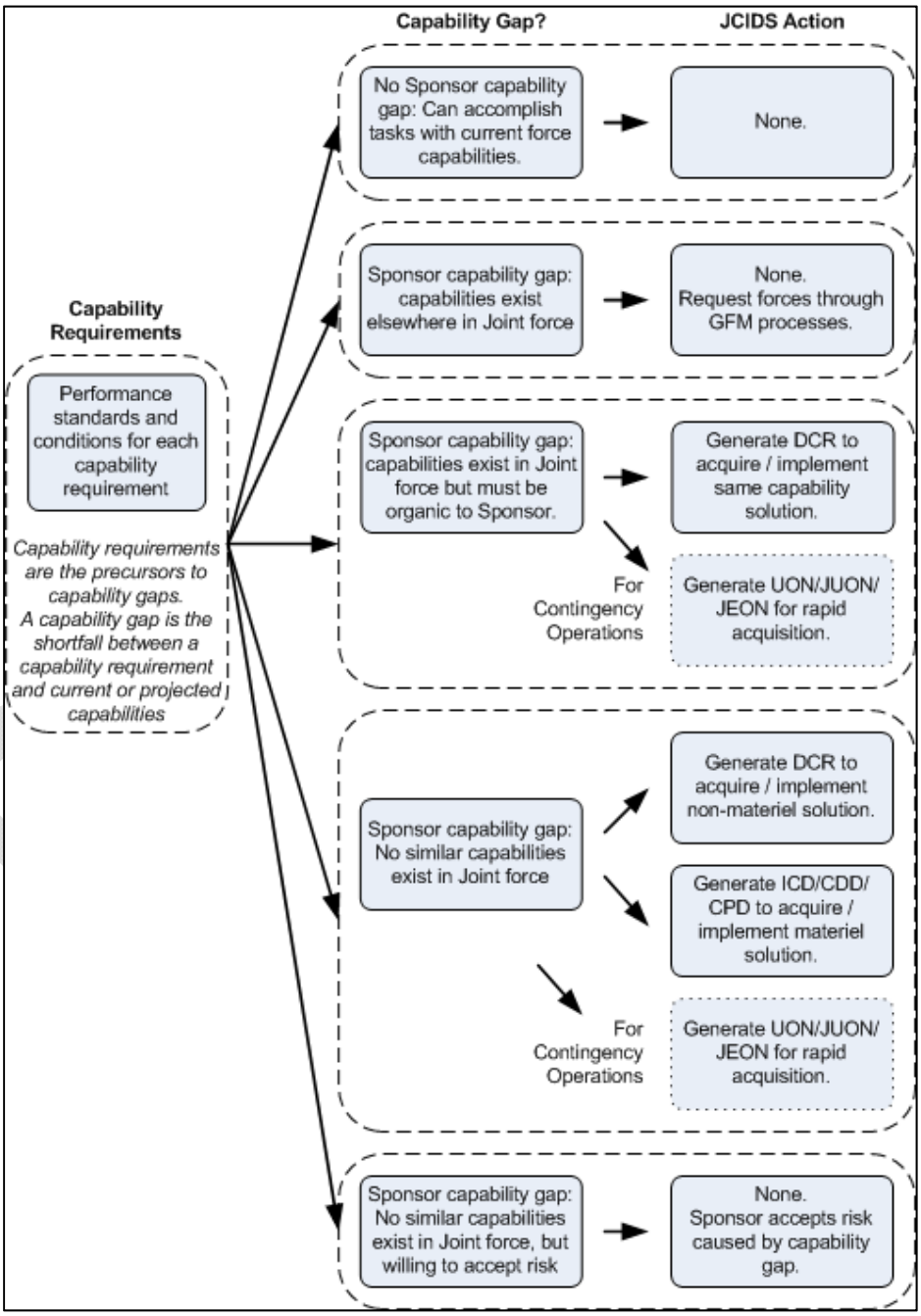

Figure C-1. Identification of Capability Gaps and Resulting JCIDS Action

a. Issues not requiring JCIDS action. Not every capability gap will result in an associated JCIDS action, as each is a balance between operational risk of the capability gap, life cycle costs associated with developing and sustaining a capability solution, and other factors.

(1) New capability requirement documents are not appropriate if the Sponsor identifies capability solutions currently available to the joint force or in development. This also applies to cases where a Sponsor elects to move within the threshold and objective trade space of a previously validated capability requirement document. I.e. – a Sponsor developing a capability solution to meet threshold KPP, KSA, or APA values later decides to pursue increased capabilities up to the previously validated objective KPP, KSA, or APA values.

(2) If capability solutions which can satisfy the Sponsor capability requirements do not exist in the joint force, but the Sponsor is willing to accept risk, then no capability requirement document is generated.

(3) If capability solutions which can satisfy the Sponsor capability requirements exist elsewhere in the joint force, the Sponsor does not create a new capability requirement document but uses a Request for Forces (RFF) or Request for Capabilities (RFC) and the GFM process to request forces and their associated capabilities in accordance with references fff and mmm.

b. Issues requiring JCIDS action. If the Sponsor identifies capability requirements which they cannot satisfy with capability solutions currently available to the joint force or in development, then they have a capability gap which may require further action.

(1) If capability solutions which can satisfy the Sponsor capability requirements exist elsewhere in the joint force, but must be organic to the Sponsor organization:

(a) To leverage entire capability solutions "off the shelf," the Sponsor may generate a Joint DCR for validation in JCIDS to establish the capability requirement for the fielded capability solution in the Sponsor organization. In urgent situations supporting ongoing or anticipated contingency operations, the Sponsor may generate a JUON, JEON, or DOD Component UON for greater expediency. Sponsors must articulate why the GFM process, and leveraging other capabilities of the joint force, is not appropriate to satisfying the Sponsor's capability requirement.

(b) To leverage only portions of fielded capability solutions, to be integrated into one or more of the Sponsor's capability solutions, the Sponsor may generate a Joint DCR for validation in JCIDS to establish the requirement to leverage part of another Sponsor's capability solution. The implementation

of the Joint DCR may involve updates to previously validated CDDs or CPDs to provide for broadened scope, and submittal for review and revalidation.

(2) If capability solutions which can satisfy the Sponsor capability requirements do not exist in the joint force, the Sponsor has three primary options:

(a) If the capability requirement can be satisfied through a non-materiel approach:

1. For non-materiel solutions which impact only the Sponsor organization, review, validate, and implement in accordance with policies and processes of that organization.

2. For non-materiel solutions which impact more than just the Sponsor organization, generate a Joint DCR for validation in JCIDS, to establish a new non-materiel solution in the Sponsor organization. Joint DCRs may also be used in a similar manner to validate capability requirements where service contracting in accordance with reference nnn provides the most appropriate capability solution.

(b) Following the CBA, if the optimal approach to satisfying the capability requirement – a non-materiel approach, a materiel approach, or a combination of the two – the Sponsor may generate an ICD for validation in JCIDS. Sponsor analyses following ICD validation, such as an AoA, additional DOTmLPF-P analysis, or other study, will determine which successor documents – Joint DCRs for non-materiel solutions and/or CDDs/CPDs for materiel solutions – should be generated and submitted to JCIDS to support follow-on efforts. For further information about the conduct of AoAs following ICD validation, see reference ooo

(c) If the capability requirements are driven by ongoing or anticipated contingency operations, and left unfulfilled would result in unacceptable loss of life or critical mission failure, the Sponsor may generate a JUON, JEON, or DOD Component UON document for expedited staffing and validation in the JCIDS or DOD Component processes. JUONs, JEONs, and DOD Component UONs should only be generated when other means to satisfy the capability requirement are not practical – GFM process, JMVP, deliberate requirements and acquisition, etc. Warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed in accordance with reference gg.

5. Documentation of Studies/Analysis and Associated Data

a. Purpose. The Joint Staff Gatekeeper maintains a studies repository within the KM/DS system to facilitate visibility into, and potential reuse of,

studies related to capability requirements and the generation of capability requirement documents. Organizations conducting studies will provide results of any studies or analyses intended to support capability requirement documents to the studies repository.

(1) Posted study results facilitate more streamlined requirements documentation, allowing capability requirement documents to refer to the study data rather than replicate information unnecessarily. Historical study data in the repository also facilitates leverage of prior studies and efforts across the joint force to reduce unnecessary duplication of prior efforts and enable shorter timelines with more focused study efforts.

(a) Sponsors will submit CBAs and other studies/data focused on identifying and assessing capability requirements to the studies repository before submitting an ICD based upon those efforts.

(b) AoA study plans, AoA final reports, and other supporting documentation for the post-AoA (or similar study) review will also be archived in the studies repository ahead of the post-AoA (or similar study) review.

(c) The studies repository is also used to capture assessments of JCTDs, fielded JUONs, JEONs, and DOD Component UONs, and other demonstrations of capability solutions in an operational environment, as well as other alternate forms of supporting documentation for capability requirements.

(d) Study initiation notices for any related activities will be posted to the study repository at the start of the respective study.

(2) To the greatest extent possible, the organizations conducting studies should leverage historical information from the studies repository and other sources, and focus CBAs and other studies only in areas which require new or updated analysis.

b. Submission of studies and associated data

(1) If details of a study, copy of an assessment, or other documentation intended to justify a capability requirement is not in the studies repository at the time the Sponsor intends to submit a related capability requirement document, the Sponsor will provide the supporting documentation before submitting the related capability requirement document for staffing and validation. Procedures for submission of studies and other data to the studies repository are outlined in Enclosure E of this manual.

(2) Results of studies indicating that there is a lack of a need to pursue new capability requirements should still be provided to the studies repository

for future reference. This "negative" conclusion can prevent unnecessary duplication of studies reaching the same negative conclusion. Altered strategic guidance, threats, or other conditions in the future, may also allow the prior study to be used to support different conclusions in a much shorter timeframe, if available for review and modification.

c. Study initiation notices. To facilitate greater visibility into ongoing studies, encourage collaboration, leverage efforts where appropriate, and reduce unnecessary duplication of current study efforts, organizations conducting studies intended for or likely to drive submission of new capability requirements in the JCIDS process will provide a study initiation notice to the studies repository.

(1) Note that while AoAs are a form of study, they do not necessarily require separate "study notice" to be sent to the Joint Staff Gatekeeper.

(a) For AoAs subject to CAPE approval of study guidance, such as for acquisition category (ACAT) ID programs, visibility into CAPE approval of AoA study guidance serves to inform JCIDS stakeholders that an AoA is underway.

(b) For AoAs or similar studies not subject to CAPE approval of study guidance, such as for ACAT II or III programs, Sponsors will submit a study initiation notice to the studies repository.

(2) Study initiation notices provided to the studies repository should be concise but provide sufficient information for a reader to determine if the scope of the study is of interest and worth contacting the POC for further information or discussion. The notice should be in memo format and contain at least the following elements:

(a) Date of the notification memo.

(b) Title of the study.

(c) Executive summary/purpose of the study.

(d) Participating organization(s).

(e) Intended completion date.

(f) Lead organization POC and contact information.

(g) Tier 1 through 3 JCAs related to primary focus of study. For broadly scoped studies where identification of tier 3 JCAs is not applicable, identify the focus of the study to the lowest appropriate JCA tier.

(3) The Joint Staff Gatekeeper will notify FCBs with potential interest in the study topic based upon their respective JCAs. FCB members and other interested stakeholders can review the study initiation notices to determine if there is any opportunity for collaboration on or leverage of study efforts. As appropriate, interested stakeholders may contact the organization conducting the study to discuss potential for collaboration and/or shared study efforts.

(4) In the event of a study being discontinued prior to providing any significant results, the organization conducting the study will provide a termination notice in the studies repository. The notice should be in memo format and contain at least the following elements:

(a) Date of the termination notice memo.

(b) Title of the study from the original initiation notice.

(c) Date of the original initiation notice memo.

(d) Purpose/reason for cancellation (i.e. – funding limitations, superseded by or consolidated into another study effort (provide reference info), or overcome by external events such as updated strategic guidance, altered threats, etc.)

(e) Lead organization POC and contact information.

DRAFT

APPENDIX A TO ENCLOSURE C

EXAMPLE OPERATIONAL ATTRIBUTES

1. Purpose

a. This appendix is intended to provide a set of example operational attributes as a common basis for definition of capabilities in each of the JCAs. They are applicable to describing capability requirements in the conduct of CBAs and other similar analyses, and in authoring of ICDs. These examples are not exhaustive, but represent the general kinds of operational attributes which should be considered in identification of operational capabilities needed to satisfy organizational roles, missions, and tasks.

b. As operational attributes generally don't provide value in isolation, they should be expressed in meaningful combinations which contribute to mission success using that capability.

c. They should also avoid presenting parameters which are system specific and would be more appropriate for KPPs, KSAs, and APAs articulated in CDDs and CPDs.

(1) For example, a sensor may provide "area coverage in a particular timeframe" which is a combination of both the field of view of the sensor and the movement speed/altitude of the host platform. That said, neither the field of view or platform speed/altitude are likely to be valid operational attributes, as they would be based upon premature assumptions of a specific capability solution. The Sponsor should focus instead on the platform/sensor agnostic operational attributes of "area coverage in a specific timeframe" and allow the AoA tradespace to determine the most appropriate combination of sensor and host platform performance to deliver the required capability.

(2) Once an AoA has been performed and a CDD is being written, the KPPs, KSAs, and APAs will include sensor and host platform performance parameters which can be traced back to these operational attributes.

2. JCA Specific Examples

a. Force Support Attributes

(1) Generic Attributes: Accuracy, Adaptability, Comprehensiveness, Credibility, Integration, Timeliness.

(2) Global Patient Movement Example (JCA 1.4.1 – Force Support, Health Readiness, Force Health Protection): Capability, with XXX hrs prior

notice; to transport XXX patients; in condition XXX requiring medical support XXX; between any two major airports; within XXX hrs of patient arrival.

b. BA Attributes

(1) Generic Attributes: Accuracy, Adaptability, Comprehensiveness, Credibility, Innovativeness, Integration, Interoperability, Persistence, Survivability, Timeliness.

(2) Anti-Submarine Wide-area Search Example (JCA 2.2 – Battlespace Awareness, Collection, Multiple Tier 3 categories): Capability to search XXX area of the ocean's surface; within XXX distance from a carrier strike group; in XXX timeframe, with XXX probability of detection; with XXX sea-state, day/night, and weather conditions; for a submerged adversary target with detectability characteristics XXX.

(a) Note that in this particular example, effective detection of the adversary is required and the Sponsor should not limit the capability requirement to a preconceived notion of the "best" phenomenology. The Sponsor would be best served by NOT specifying the Tier 3 JCA(s), since those correspond to different phenomenology and may unduly constrain the AoA and prevent selection of the most appropriate capability solution.

(b) When documenting a capability solution developed to satisfy this capability requirement, the Sponsor WILL trace KPPs, KSAs or APAs to Tier 3 or lower JCAs depending upon the specific phenomenology used to detect the target.

c. FA Attributes

(1) Generic Attributes: Accuracy, Adaptability, Capacity, Flexibility, Mobility, Persistence, Scalability, Security, Survivability, Timeliness.

(2) Penetrating Munition Example (JCA 3.2.1 – Force Application, Engagement, Kinetic Means): Capability to engage a stationary target (or target moving at speed XXX); under XXX day/night and weather conditions; through protective material/thickness XXX; delivering effect XXX to adversary personnel; within XXX distance of impact; with XXX probability.

d. Logistics Attributes

(1) Generic Attributes: Accountability, Agility, Attainability, Capacity, Economy, Effectiveness, Enduring, Expeditionary, Flexibility, Integrated, Networked, Persistence, Precision, Reliability, Responsiveness, Scalability, Simplicity, Survivability, Sustainability, Tailorability, Visibility, Velocity.

(2) Tactical Cargo Transportation Example (JCA 4.1.2 – Logistics, Deployment and Distribution, Sustain the Force): Capability to transport cargo in units up to XXX weight and XXX/XXX/XXX length/width/height; over XXX distance in XXX timeframe; with XXX terrain, day/night, and weather conditions.

e. Command and Control Attributes

(1) Generic Attributes: Accessibility, Accuracy, Agility, Completeness, Interoperability, Latency, Operational Trust, Relevance, Robustness, Security, Simplicity, Timeliness, Understanding.

(2) Issue Emergency Action Message Example (JCA 5.5.2 – Command and Control, Direct, Task): Capability to compose messages in XXX format; transmit from authenticated originator(s) XXX to recipient(s) XXX; in time between transmission and receipt no greater than XXX; with no greater than XXX probability of interception; with at least XXX probability of correct message receipt.

f. Net-centric Attributes

(1) Generic Attributes: Accessibility, Accuracy, Agility, Availability, Capacity, Completeness, Controllability, Expeditionary, Flexibility, Integration, Interoperability, Latency, Maintainability, Reconfigurability, Relevance, Reliability, Responsiveness, Robustness, Scalability, Security, Survivability, Throughput, Timeliness, Visibility.

(2) Positioning, Navigation, and Timing (PNT) Example (JCA 6.2.4 – Net-Centric, Enterprise Services, PNT): Capability to provide globally available PNT services, with horizontal and vertical accuracy of XXX and XXX meters, under background noise/jamming conditions XXX, with operational availability of XXX.

g. Protection Attributes

(1) Generic Attributes: Capacity, Effectiveness, Integration, Networkability, Persistence, Responsiveness, Survivability.

(2) Tactical Missile Defense Example (JCA 7.1.1 – Protection, Prevent, Prevent Kinetic Attack): Capability to defend a land or water surface area of XXX within XXX distance of a point defense location; against adversary ballistic and cruise missile threats with detectability characteristics of XXX and operating up to speeds of XXX; with threats operating singly or in salvos of up to XXX, with a probability of successful defense of XXX.

h. Building Partnership Attributes

(1) Generic Attributes: Agility, Breadth, Depth, Effect, Flexibility, Persistence, Utility.

(2) Influence Foreign Audiences Example (JCA 8.1.2 – Building Partnerships, Communicate, Persuade Partner Audiences): Capability to deliver DOD information/message to XXX percentage of population of partner nation XXX within XXX time of specific event with XXX confidence.

i. Corporate Management and Support

(1) Generic Attributes: Accessibility, Accuracy, Auditability, Availability, Efficiency, Integration, Interoperability, Latency, Reliability, Responsiveness, Security, Throughput, Timeliness, Usability, Visibility.

(2) Financial Management Example (JCA 9.5.2 – Corporate Management and Support, Program Budget and Finance, Accounting and Finance): Capability to process XXX requests for payment within XXX timeframe, with payment error rate no greater than XXX, with real-time visibility to organizations XXX with latency no greater than XXX.

DRAFT

APPENDIX B TO ENCLOSURE C

CAPABILITIES BASED ASSESSMENT GUIDE

1. Overview

a. Purpose. A CBA provides a robust assessment of a specific mission area, or similar bounded set of activities, to assess the capability and capacity of the joint force to successfully complete the mission or activities.

(1) A CBA often leads to the identification of new or modified capability requirements and associated capability gaps. If the capability gaps represent significant operational risk to the joint force, then these capability requirements, along with recommendations for materiel and/or non-materiel approaches for closing or mitigating the capability gaps, may be submitted for staffing and validation by the appropriate validation authority.

(2) The intent of a CBA may also be satisfied through one or more other studies or analyses, as long as the analytical rigor and breadth of analysis is covered by the collective analytical efforts.

b. Traceability. The analytical work conducted as part of a CBA provides the traceability between strategic guidance, operational missions, Service and joint concepts, CONOPS, DIA- or Service-approved threat products, including but not limited to, capability requirements, and capability solutions.

(1) CBA activities support the development of content required in capability requirement documents and associated DODAF products, as well as development of materiel and non-materiel capability solutions. These results are not static, but are expected to be further refined throughout the follow-on processes.

(2) A number of DODAF views should be used to capture results of a CBA, facilitating reuse in capability requirement documents, acquisition activities, and capability requirement portfolio management. For more details on applicable DODAF views, see the DODAF Primer in Appendix C to this enclosure and reference ppp.

(3) When one or more studies or analyses are used in place of a CBA, the DODAF views for a CBA, or a tailored set thereof, should still be developed to capture the result of each study. Before proceeding from the collection of studies to authoring an ICD, the Sponsor may need to consolidate the DODAF products into a single set appropriate for the scope of the ICD.

c. Level of Rigor. The Sponsor must determine the level of analytic rigor needed in a CBA. The rigor which should be used in a CBA is a function of the complexity of the mission being assessed, the consequences of operational failure, and the uncertainties of the SSA products and other supporting data considered.

(1) When performing a CBA relative to a previously validated capability solution that may require replacement, recapitalization, or evolution to meet future capability requirements, the Sponsor is starting from a known baseline and making excursions to address potential future capability requirements. While the decision to consider recapitalization of an existing capability solution may be driven by a specific capability gap or set of gaps, a CBA must also consider the entire set of tasks, conditions, and standards fulfilled by the capability solution. Analyzing only a subset of tasks, conditions, and standards associated with the identified capability gap(s) may result in a future solution which closes one set of capability gaps only to create a different set of capability gaps. In this case a CBA should take no more than 60-90 calendar days to demonstrate that replacement, recapitalization, or evolution is required. The alternatives for the solution will be further considered in the AoA or similar study.

(2) When performing a CBA that addresses capability requirements most likely addressed through an IS solution, the CBA should take no more than 90 calendar days. The determination on whether a new IS is required or if a previously fielded system can be evolved to meet the need will be further considered in the AoA or similar study.

(3) When performing a CBA that is examining a new mission with a lot of uncertainty or complexity or is assessing the capability requirements for a new Service and joint concept, the risks and uncertainty drive the need for a more comprehensive CBA to determine if it is necessary to move to an evolution of a previously fielded capability solution or to pursue transformational capabilities to satisfy the capability requirements.

(4) One CBA may address any of these alternatives. In any case, the maximum time allotted for a CBA should be no more than 180 calendar days, and the assessment should be tailored to meet this objective. The time allotted does not include the time required for staffing and approval in the Sponsor organization.

d. Additional guidance. While this appendix provides an overview of the CBA process, references tt through vv offer more detailed guidance and best practices relating to these assessments. Organizing and executing a successful CBA and satisfying the demands of strategic guidance is a significant challenge. Consequently, a CBA, particularly one addressing a broad mission

area, should be conducted with a robust joint team that can bring the necessary breadth of expertise to bear on the problem.

2. CBA Process Steps

a. Study Initiation Notice. Each CBA begins with the Sponsor providing a study initiation notice to the Joint Staff Gatekeeper. This provides visibility, and facilitates participation by other stakeholders who may have valuable input to contribute to a CBA, or may be able to leverage the output of the CBA for other ongoing activities.

(1) The Sponsor must identify and build upon any previous CBAs, studies, lessons learned, and other analytical products applicable to the area of interest. The intent is to avoid any unnecessary repetition of prior efforts, and provide continuity between analyses for reviewers and decision makers.

(2) This does not preclude the CBA sponsoring organization from applying different context or different assumptions to previous analyses, as appropriate for the current CBA.

b. CBA Focus. The CBA's focus is derived from the strategic context, mission and scenarios to be examined, the timeframe under consideration, and the associated threats.

(1) Strategic context. The CBA must be relevant to the needs of the defense strategy and other strategic guidance contained in documents such as the NDS, QDR, NMS, DPG, and GEF. The products generated by the JSCP in reference u provide other data important for describing the breadth of the strategic environment and selecting an adequate scenario sample.

(2) Missions and scenarios. The CBA should use appropriate OPLANs or CONPLANs for near-term assessments or SSA products developed in accordance with references n and o for long-term assessments. Furthermore, the SSA products must be chosen in such a way that the full spectrum of operational situations relevant to the defense strategy will be examined, including other US government agency/department, allied/partner nation, and coalition activities. While it is important to scope the assessment to make it manageable, it is equally important to cover the spectrum of strategically relevant operational situations.

(3) Joint Lessons Learned. The CBA should use the Joint Lessons Learned Information System, in accordance with reference ss, to provide additional information relevant to the CBA area of interest.

(4) Use of DODAF views.

(a) DODAF views and associated data provide a structured means to document data associated with the CBA and more easily leverage and update data when developing capability requirement documents as shown in Figure C-B-1.

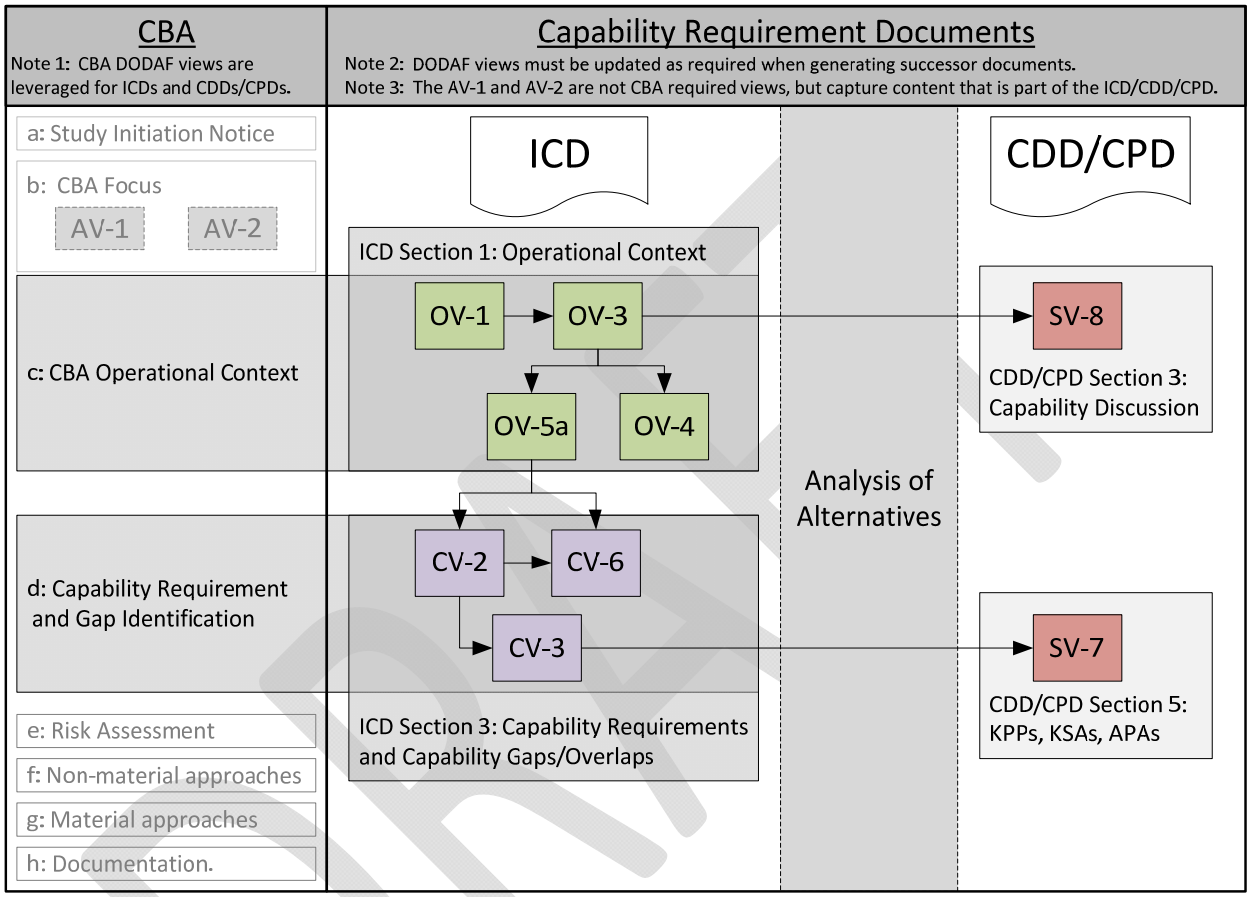

Figure C-B-1. DODAF Flow from CBA to Capability Requirement Documents

(b) DODAF views and associated data are intended to represent the context under which the CBA was conducted (i.e. – the existing enterprise) as modified, if applicable, by the recommendations of the CBA. (i.e. – the proposed future end state) Aspects of the existing EAs not impacted by the CBA recommendations must remain consistent with the existing EAs.

(c) The DODAF OVs and CVs illustrated in Figure C-B-1 should be generated during the CBA, as leveraging these DODAF views and associated data can significantly improve efficiency, saving time and resources later in the JCIDS and DAS processes.

1. Note that the level of detail in DODAF views generated during a CBA does not require the use of sophisticated architecture tools and

associated personnel unless desired by the Sponsor. The data required for most of the views can be structured as tables using Microsoft Excel or similar spreadsheet programs, and used in that form for the purposes of generating capability requirement documents and submitting associated DODAF views for review. The data must be submitted in such a form that it may be efficiently imported into architecture tools for follow-on efforts as desired by the Sponsor and other stakeholders. Providing only image files, Microsoft PowerPoint briefings, or other non-importable formats is not acceptable, as all data would need to be regenerated in an importable format prior to further use. Examples of DODAF views supporting JCIDS are available at the URL in reference c.

2. Data captured in the DODAF views during the CBA may be limited by knowledge at that stage of development, but should be updated throughout follow-on stages of JCIDS and DAS as more specific detail is developed through those efforts.

(d) The DODAF Systems Views (SVs) illustrated in Figure C-B-1 should NOT be generated during the CBA and are shown for context only. They require system level details that will not be available until an AoA is conducted, but are derived from the OVs and CVs generated during the CBA.

(e) In addition to specific views outlined in later sections of the CBA guidance, the Sponsor should be maintaining/updating the following views throughout the CBA activities for their own benefit, even though they are not mandatory submissions to go along with an ICD.

1. DODAF AV-1 – Overview and Summary Information. This overview/summary data from the CBA can be re-used when authoring the CBA results and the ICD executive summary

2. DODAF AV-2 – Integrated Dictionary. The definitions identified during the CBA can be re-used when authoring the CBA results and as a starting point for authoring the ICD Appendices B and C.

(d) For more details on DODAF views, see the DODAF Architecture Primer in Appendix C of Enclosure C of this manual and reference ppp.

c. Operational Context. The next step in the CBA is to consider the timeframe under consideration, applicable threats, and relevant Service and joint concepts, CONOPS, objectives, and related effects to be achieved.

(1) Timeframe. The timeframe considered in the CBA is important both to help establish the conditions and threats under which the mission is to be carried out, and as a key component in discussions between the requirement Sponsor and the acquisition community in determining the required IOC and

FOC dates. The IOC and FOC dates indicate when the joint warfighter needs initial and full capability provided by one or more capability solutions. The timing of IOC and FOC from this CBA step, together with the required capabilities identified in a later CBA step, supports development of the DODAF CV-3 later in the CBA when phasing of capability requirements is considered, and supports re-use when authoring the ICD operational context section. This view is particularly important when the operational context envisions the requirement for some of the identified capabilities to be available at earlier dates than other identified capabilities.

(2) Threats. Threats to the mission being analyzed should be derived from DIA- or Service-approved threat products, including but not limited to CTAs, the MSFD, and the Joint Country Forces Assessments. If additional assistance is required, contact DIA's Defense Technology and Long-Range Analysis (DIA/TLA) office, Acquisition Threat Support Division via the options shown in reference qqq. DIA/TLA support to JCIDS includes data provided by multiple types of DIA- and Service-validated threat products.

(a) Collaboration among the intelligence, counterintelligence (CI), requirements, and acquisition communities shall be maintained throughout the capability solution's life cycle to achieve the highest level of technological superiority possible over adversarial capabilities. This collaborative effort includes identification of adversary threat capabilities that represent the projected operational environment, and the anticipated capabilities and CONOPs that adversaries might employ against the capability being reviewed. These collaborative assessments are used as inputs to the Sponsor's studies, analyses, and other efforts in requirement development efforts.

(b) Operational tasks, conditions, and standards identified in studies or other analyses should be submitted to DIA/TLA to enable production of an initial threat environment assessment (ITEA). The ITEA identifies projected adversarial threat capabilities which are a factor in setting the capability requirements and initial objective values, including scientific and technological developments which could specifically affect the determination of capability requirements and development of capability solutions. DIA/TLA will continue to assist Sponsors, as needed, with updates to the threat assessments throughout the remainder of the capability solution's life cycle until superseded by a DIA- or Service-approved threat product, including but not limited to System Threat Assessment Report (STAR).

(c) Characteristics of adversary threat capabilities which are a factor in establishing capability requirements and associated initial objective values should be documented as CIPs. This enables the IC to provide more robust monitoring of threat changes throughout a capability solution's life cycle.

(3) Concepts and CONOPS. Concepts and CONOPS used as part of a CBA must be documented such that the reviewers and validation authorities can understand the context used to identify and evaluate the capabilities identified.

(a) Joint concepts, developed in accordance with reference m, are specifically designed to drive progress in the DOD and should be used as a starting point where applicable. The Capstone Concept for Joint Operations (CCJO) in reference rrr provides an overarching joint concept.

(b) Concepts and CONOPS must clearly identify whether operations are required in, or after exposure to, Chemical, Biological, Radiological, or Nuclear (CBRN) environments, through degraded GPS or cyber situations, or under the effect of other potential adversary stressors.

(c) There is no strict format for a concept or CONOPS used in a CBA, but it should describe the following areas at a minimum (See Appendix A to Enclosure D of this manual for additional CONOPS detail required to support CDDs and CPDs):

1. problem being addressed

2. mission expected to be performed

3. commander's intent

4. operational overview over the full range of military operations

5. objectives to be achieved

6. roles and responsibilities of tasked organizations

(d) The level of detail provided with the concept or CONOPS should provide the data required for the Sponsor to generate the following DODAF views, if DODAF views are not already provided as part of the concept or CONOPS. Each view should be considered as a starting point for further refinement and exploration of alternative concepts or CONOPS during the CBA.

1. DODAF Operational View (OV)-1 – High Level Operational Concept Graphic. The OV-1 provides stakeholders with a graphical view of the highest level of the concept or CONOPS to facilitate general understanding of the concept or CONOPS. The OV-1, as refined during the CBA, is reused in the capability requirement documents and other follow-on efforts.

2. DODAF OV-3 – Operational Resource Flow Matrix. The OV-3 translates the OV-1 picture into a complete set of nodes, activities, and interconnections upon which the rest of the architecture is based. This provides stakeholders with more detailed operational interactions which must take place between nodes/actors executing the concept or CONOPS, and any enabling/supporting capabilities which are involved, including identification of organizations that may be involved. This view must focus on the operational activities/effects necessary to execute the concept or CONOPS, and avoid the presumption of particular capability solutions which will be explored in a later step of the CBA. The OV-3, as refined during the CBA, provides the fundamental basis for traceability from other DODAF views and content in capability requirement documents back to the operational activities/effects applicable to the concepts and CONOPS. Note that generation of a DODAF OV-2 – Operational Resource Flow Description – may facilitate the generation of the OV-3.

3. DODAF OV-4 – Organizational Relationships Chart. The OV-4 provides stakeholders with an initial overview of the organizations intended to satisfy the concepts and CONOPS. This provides a baseline for excursions during and following the AoA (or similar study), as greater detail of potential capability solutions and associated organizations is developed.

(e) Any CONOPS used as the basis for a CBA must be approved by the CBA sponsoring Component at a minimum.

1. Approved Service and joint concepts or CONOPS, coupled with the SSA products, should be further refined to describe how the objectives are achieved with current or programmed forces, using doctrinal approaches. These refinements should include a logical projection of how current concepts and CONOPS might be expected to evolve for the timeframe under consideration.

2. Alternative Service and joint concepts, or alternative CONOPS, based on non-doctrinal approaches or changing the original approved concepts, may also be considered to mitigate the capability gap by using previously fielded capability solutions in a different manner.

(4) Identification of operational tasks.

(a) The military objectives outlined in the OPLANs, CONPLANs, and SSA products, including mission outcomes and associated desired effect, provide a source for developing the list of required tasks.

(b) The applicable concepts and CONOPS, and variations considered within the CBA provide the framework for developing lists of tasks

required to accomplish both the proposed and alternative CONOPS. The UJTL outlined in reference sss also provides a framework to aid in identifying and organizing the tasks, conditions and required capabilities. If the UJTL does not identify appropriate tasks for the Service and joint concepts or CONOPS under consideration, submit updates to the UJTL in accordance with reference sss.

(c) DODAF OV-5a – Operational Activity Decomposition Tree. The Sponsor should capture the output of this step in the OV-5a, which provides the relationship between the operational activities/effects from the OV-3 and the associated UJTs. The OV-5a, as refined during the CBA, provides traceability from other DODAF views and content in capability requirement documents back to the UJTs applicable to the concepts and CONOPS.

(5) Level of detail. The analysis of concepts and CONOPS required for this section of the CBA provides the Sponsor with a robust understanding of the operational context and tasks which must be performed, and supports further refinement and exploration of excursions during the CBA.

(a) At the early stage of a CBA, only the "as-is" architecture of previously developed capabilities will be available in great detail. The DODAF views related to the proposed capabilities will be captured in much less detail at this stage, but must be consistent with the concept(s) or CONOPS.

(b) System specific details should be avoided at this stage so that the later AoA or similar studies can be conducted with maximum flexibility, and allow DODAF views to mature as additional decisions are made and data is generated throughout the JCIDS and DAS processes.

d. Capability Requirement and Capability Gap Identification.

(1) The CBA Sponsor must identify the capability requirements which enable the activities/effects and UJTs identified in the DODAF OV-3 and OV-5a views, and through an assessment of current and programmed forces, identify any associated capability gaps and potential force redundancies for each scenario. Note that while some redundancies are intentional for the purpose of providing resiliency, unnecessary redundancies should be minimized.

(a) The operational conditions are derived from SSA products, and capability requirements are derived from tasks that must be accomplished to achieve the objectives under those operational conditions. The capability requirements and capability gaps must be described in terms of the SSA products assessed and the impact on achieving the relevant objectives. It is likely that the capability gaps will be inconsistent across different SSA products, so it is essential to associate identified capability gaps to their operational context.

(b) For capabilities provided by IS, the CBA must also use emerging guidance such as the DOD Information EA (DOD IEA) in reference p. To describe and characterize system contributions to military operations, use the DoD Data Framework and the Joint Command and Control (JC2) reference architecture for SECRET and below systems, and the Defense Intelligence Information Environment (DI2E) data construct for intelligence systems, in accordance with references ttt and uuu.

(2) The CBA must explain the methodology for determining the capability requirements and associated capability gaps, to ensure that the association between the capability requirements and strategic guidance is clear. A framing construct, such as the CML presented in Figure B-2, must be used to provide rigor to the traceability from strategic guidance, operational missions/scenarios, and threats, to the decomposition into specific capability requirements and conditions associated with UJTs. The framework used must also provide context for the comparison of capability requirements to the previously fielded and programmed capability solutions of the joint force as a means to identify operational risks associated with any capability gaps.

(a) The JCA framework outlined in reference vvv is a logical grouping of capabilities that provides the structure around which capability requirements and associated capability gaps can be aligned across the Department's capability requirement portfolios to correlate similar needs, leverage common capability solutions, and synchronize related activities. The sponsor is required to identify capability requirements to the Tier 3 JCAs at a minimum, but lower levels are recommended where it provides additional clarity to the capability requirements.

(b) DODAF Capability View (CV)-2 – Capability Taxonomy. As the sponsor identifies capability requirements and associated capability gaps, they can generate the CV-2 and specify the taxonomy associated with these capabilities. These capability requirements should be captured in a manner consistent with the operational attributes outlined in Appendix A to Enclosure C of this manual, and be expressed in terms of operational effectiveness rather than performance of a presumed capability solution. Quantitative criteria for mission success must be established for each capability requirement to support later assessment of how well potential materiel solutions satisfy the capability requirements. In most cases, these criteria will not be simple pass-fail standards, but instead will represent a continuum of values.

(c) DODAF CV-3 – Capability Phasing. The Sponsor builds upon the CV-2 with any applicable phasing of the identified capability requirements and captures that in the CV-3. For example, if only a subset are needed in a shorter timeframe than the timeframe required for the entire set of capabilities,

the CV-3 captures the information required to pursue an incremental development strategy while making sure that the correct capabilities are introduced at the correct times.

(d) DODAF CV-6 – Capability to Operational Activity Mapping. The Sponsor uses the CV-6 to ensure robust traceability between the capability requirements identified in the CV-2 and the operational activities identified in the OV-5a. This reduces the risk of disconnects between delivered capabilities and the operational activities they are intended to satisfy.

(3) Once the capability requirements are identified in the steps above, any shortcomings in the current or programmed force can be identified as capability gaps. The capability gaps can be characterized as to whether they are due to:

(a) lack of proficiency (inability to achieve the relevant effect in particular conditions);

(b) lack of sufficiency (inability to bring capable forces to bear due to force shortages or other commitments);

(c) lack of any fielded capability solution;

(d) need for replacement due to aging (fatigue life, technological obsolescence, etc.) of a fielded capability solution; or

(e) policy limitations (inability to use the force as needed due to policy constraints).

e. Risk Assessment.

(1) The capability gaps are then assessed against adversary threats in terms of the risk to mission (the ability to achieve the objectives of the scenario), the risk to force (the potential losses due to the capability gap), and other important considerations, such as resourcing risks and effects on allies, partner nations, and other US government agencies/departments. The conditions and standards developed for the associated tasks provide the basis for the assessments.

(2) Since a validation authority for capability requirement documents will ultimately decide which capability gaps are important enough to develop new capability solutions, the capability gaps must be directly associated to operational situations and consequences of failing to meet objectives. Table C-B-1 presents an example approach for assessing the risks and consequences associated with a particular capability gap. The capability gap is assessed

DRAFT

based on its impact in several areas: ability to achieve the objectives; operational timelines; resources; unanticipated requirements; force provider resourcing; and component functions, force management, institutional capacity.

Risk	Criteria	Low	Moderate	Significant	High
CCMD "Risk to Mission" Ability to execute assigned missions at acceptable human, materiel, financial, and strategic cost.	Achieve Objectives (Current Operations)	Very likely (80-100%)	Likely (50-80%)	Questionable (20-50%)	Unlikely (0-20%)
	Achieve Objectives (Contingencies)	Very Likely (Can Defeat)	Likely (Can Deny)	Questionable (Must Hold-Win)	Unlikely (Cannot Hold)
	Authorities	Full authority provided for all objectives	Authority provided to achieve most objectives	Insufficient authority to achieve key objectives	Lack of authority jeopardizes mission
	Planning	Level III or IV Plans	Level I or II Plans	CCDR CONOPS (Anticipated Event)	Initiate Planning (Complex Crisis)
	Resources Meet Required Timelines	As Planned	Limited Delays (Acceptable Costs)	Extended Delays (Substantial Costs)	Extreme Delays (Unacceptable Costs)
Service/JFP "Risk to Force" Ability to recruit, man, train, equip, and sustain the force to meet strategic objectives	Meet CCMD Requirements (Current Operations)	Full capacity to source all requirements	World-wide solutions for most requirements	Shortfalls in critical requirements	No solutions for critical requirements
	Meet CCMD Requirements (Contingencies)	Full capacity to source all requirements	Shortfalls cause minor plan deviations	Shortfalls cause major plan deviations	Shortfalls make plan execution impossible
	DOTMLPF-P Capability vs. Threat	Dominance	Superiority	Parity	Inferiority
	Readiness	Strategic depth for full spectrum missions	Strategic depth for current operations	Next-to-deploy forces ready "just-in-time"	Deployed forces not ready for mission
	Mobilization (Reserve Component Dwell Time (DT))	Presidential Recall (DT > 1:5)	Limited Partial Mobilization (1:5 > DT > 1:4)	Partial Mobilization (1:4 > DT > 1:3)	Full Mobilization (DT < 1:3)
	Stress on the Force (Active Component DT)	Limited Stress (DT > 1:2)	Increased Stress (1:2 > DT > 1:1.5)	Prolonged Stress (1:1.5 > DT > 1:1)	Extreme Stress (DT < 1:1)
	Institutional	Force Development and industrial base meet all mission requirements	Force Development and industrial base meet priority requirements	Force Development and industrial base meet some priority requirements	Force Development and industrial base fail to meet essential requirements

Table C-B-1. Example Approach for Assessing Risks

(3) While capturing risk levels is one aspect of the assessment, it is more critical to identify what tasks can't be completed or what operational impacts will be in effect if a specific capability gap goes unmitigated.

f. Non-materiel approaches. If the CBA identified capability gaps with an unacceptable level of operational risk, the Sponsor then determines if a non-materiel approach can wholly or partially mitigate any of the capability gaps by recommending changes to one or more of the DOTmLPF-P areas:

(1) Alternative Concepts and CONOPS using non-doctrinal approaches. The baseline assessment should only consider doctrinal CONOPS, but the non-

materiel approach assessment may consider non-doctrinal alternatives, particularly those documented in approved Service or joint concepts. Where applicable, alternatives must also consider CONOPS involving allied/partner nation or other US government agency/department participation.

(2) Organizational and personnel alternatives. A CBA cannot redesign the force, but it can suggest ways in which certain functions can be strengthened to eliminate gaps and point out mismatches between force availability and force needs. Finally, note that operating the programmed force under substantially different organizational or personnel assumptions will generally require the development of an alternative CONOPS to support those assumptions. The organizations identified during this activity should also be documented through updates to the DODAF OV-4 view.

(3) Training alternatives. The CBA should consider if changes to training could improve effectiveness of existing capabilities, or allow the introduction of new capabilities using existing materiel.

(4) Alternative uses of previously fielded materiel. The CBA should consider how existing materiel within an organization might be used in a new or unconventional manner to mitigate or close capability gaps, and reduce operational risk. The CBA should also consider the use of materiel fielded to other DOD Components, other US government agencies/departments, allied/partner nations, coalition partners, etc.

(5) Leadership and Education alternatives. The CBA should consider if changes to leadership and education could improve effectiveness of existing capabilities, or introduce new capabilities using existing materiel.

(6) Facility alternatives. The CBA should consider how existing facilities within an organization might be used in a new or unconventional manner to mitigate or close identified capability gaps, and reduce operational risk. The CBA should also consider the use of facilities not currently available within the organization, but fielded to other DOD Components, other US government agencies/departments, allied/partner nations, coalition partners, etc. The CBA may also consider how new facilities and/or locations may help to mitigate or close identified capability gaps, and reduce operational risk. If the facility alternatives identified here affect any of the operational nodes/activities, the facilities identified during this activity should also be documented through updates to the DODAF OV-3 and OV-4 views.

(7) Policy Alternatives. When considering policy alternatives, the CBA must document which policies are contributing to capability gaps and under which circumstances. A policy change that allows new applications of previously fielded capabilities or modifies force posture to increase deterrence

is always of interest and should be considered. Policy alternatives should identify changes to support engagements with non-DOD forces – other US government agency/department, allied/partner nation, coalition – required to address the related Service and joint concepts, CONOPS, and SSA products.

g. Materiel approaches. If unacceptable risk remains after considering the application of non-materiel approaches, the Sponsor then assesses general approaches for materiel capability solutions which can wholly or partially mitigate the capability gaps. Three categories of materiel approaches are:

(1) Evolution of previously fielded capability solution(s) with significant capability improvement, including development and fielding of improved IS, improved components or subsystems to address high obsolescence rates, or other upgrades and product improvements.

(2) Replacement or recapitalization of a previously fielded capability solution(s) with significant capability improvement. The CBA should also consider impact to retirement of previously fielded capability solution(s) as the new capability solution is brought into service, and whether quantities in the joint force should be reduced based on increases in capability.

(3) Introduction of a transformational capability solution(s) that differ significantly in form, function, operation, and capabilities from previously fielded capability solution(s). They may address capability gaps associated with a new mission, or describe breakout capabilities that offer significant improvement over current capability solutions or transform the ways of accomplishing a mission.

h. Documentation

(1) Upon completion, the Sponsor provides results of the CBA, or other studies intended to identify capability requirements and associated capability gaps, to the Joint Staff Gatekeeper for visibility and to support review of subsequent capability requirement documents. As CBAs serve as a means for Sponsors to identify their capability requirements and associated capability gaps as well as to identify other information required to be submitted in capability requirement documents, they are not validated through the JCIDS Process. Conduct of the CBA and approval of the results prior to submission to the Joint Staff Gatekeeper are at the discretion of the Sponsor.

(2) Following completion of the CBA, the Sponsor may offer recommendations for the most appropriate approach(es) to close or mitigate capability gaps and reduce operational risk by generating and submitting one or more capability requirement documents for review and validation by the appropriate validation authority.

APPENDIX C TO ENCLOSURE C

DOD ARCHITECTURE PRIMER

1. Introduction. This appendix provides:

a. DODAF Overview. A basic overview of the DODAF and viewpoints that are pertinent to the JCIDS process.

(1) DODAF is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate DOD managers at all levels to make key decisions more effectively through organized information sharing across Department, JCA, Component, and Program boundaries. DODAF supports the following core processes:

(a) Operations planning, including the operational contexts which serve as the basis for deriving capability requirements and identifying capability gaps.

(b) Review and validation of capability requirements and associated capability gaps via the JCIDS process, including management of the capability requirement portfolios.

(c) Approval of acquisition activities and milestones via the DAS process, including associated systems engineering and test/evaluation activities related to the capability solutions.

(d) Supporting resource decision making in the Planning, Programming, Budgeting, and Execution (PPBE) process, including more robust traceability between the missions, capability requirements, and capability solutions supported by the resources.

(2) For a more in depth discussion of DODAF, see reference ppp.

b. Guidance related to EAs and reference architectures.

c. Information about the federated architecture repository which enables access to architecture data and associated viewpoints from a wide variety of sources. See reference q for additional information on the federated repository.

2. Architecture Products. DODAF has several basic categories of viewpoints as illustrated in figure C-C-1, which are further supported by views which capture specific data related to the overall viewpoint.

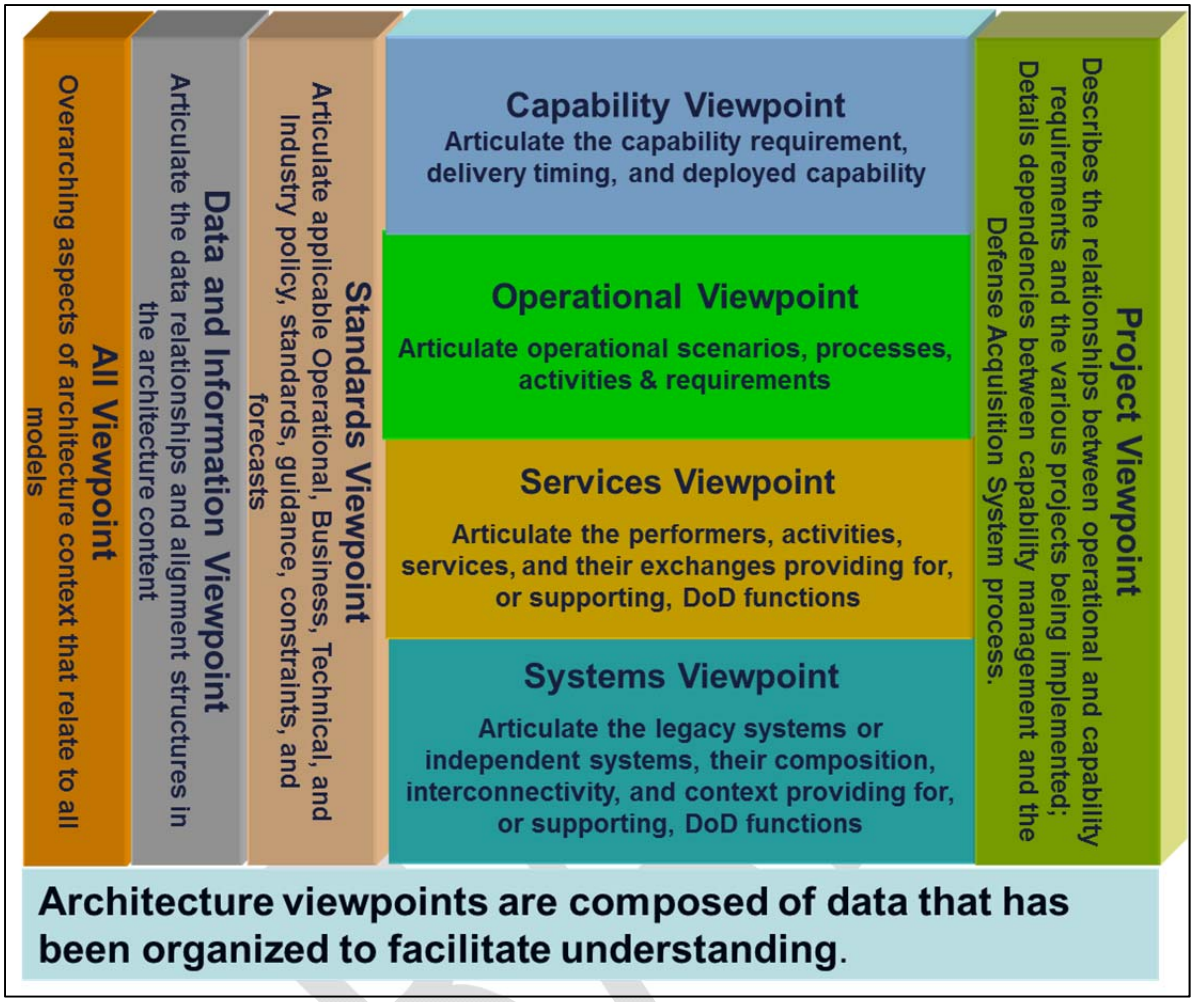

Figure C-C-1. DODAF Viewpoints

a. All Viewpoint

(1) AV-1: Overview and Summary Information. Describes a Project's Visions, Goals, Objectives, Plans, Activities, Events, Conditions, Measures, Effects (Outcomes), and produced objects.

(2) AV-2: Integrated Dictionary. An architectural data repository with definitions of all terms used throughout the architectural data and presentations.

b. Operational Viewpoint

(1) OV-1: High-Level Operational Concept Graphic. The high-level graphical/textual description of the operational concept.

(2) OV-2: Operational Resource Flow Description. A description of the Resource Flows exchanged between operational activities.

(3) OV-3: Operational Resource Flow Matrix. A description of the resources exchanged and the relevant attributes of the exchanges.

(4) OV-4: Organizational Relationships Chart. The organizational context, role or other relationships among organizations.

(5) OV-5:

(a) OV-5a: Operational Activity Decomposition Tree. The capabilities and activities (operational activities) organized in a hierarchal structure.

(b) OV-5b: Operational Activity Model. The context of capabilities and activities (operational activities) and their relationships among activities, inputs, and outputs; Additional data can show cost, performers or other pertinent information.

(6) OV-6:

(a) OV-6a: Operational Rules Model. One of three models used to describe activity (operational activity). It identifies business rules that constrain operations.

(b) OV-6b: State Transition Description. One of three models used to describe operational activity (activity). It identifies business process (activity) responses to events (usually, very short activities).

(c) OV-6c: Event-Trace Description. One of three models used to describe activity (operational activity). It traces actions in a scenario or sequence of events.

c. Capability Viewpoint

(1) CV-1: Vision. Addresses the enterprise concerns associated with the overall vision for transformational endeavors and thus defines the strategic context for a group of capabilities.

(2) CV-2: A hierarchy of capabilities which specifies all the capabilities that are referenced throughout one or more architectural descriptions.

(3) CV-3: Capability Phasing. The planned achievement of capability at different points in time or during specific periods of time. The CV-3 shows the capability phasing in terms of the activities, conditions, desired effects,

rules complied with, resource consumption and production, and measures, without regard to the performer and location solutions.

(4) CV-4: Capability Dependencies. The dependencies between planned capabilities and the definition of logical groupings of capabilities.

(5) CV-5: Capability to Organizational Development Mapping. The fulfillment of capability requirements shows the planned capability deployment and interconnection for a particular capability phase. The CV-5 shows the planned solution for the phase in terms of performers and locations and their associated concepts.

(6) CV-6: Capability to Operational Activities Mapping. A mapping between the capabilities required and the operational activities that those capabilities support.

(7) CV-7: Capability to Services Mapping. A mapping between the capabilities and the services that these capabilities enable.

d. Project Viewpoint

(1) PV-1: Project Portfolio Relationships. It describes the dependency relationships between the organizations and projects and the organizational structures needed to manage a portfolio of projects.

(2) PV-2: Project Timelines. A timeline perspective on programs or projects, with the key milestones and interdependencies.

(3) PV-3: Project to Capability Mapping. A mapping of programs and projects to capabilities to show how the specific projects and program elements help to achieve a capability.

e. Systems Viewpoint

(1) SV-1: Systems Interface Description. The identification of systems, system items, and their interconnections.

(2) SV-2: Systems Resource Flow Description. A description of Resource Flows exchanged between systems.

(3) SV-3: Systems-Systems Matrix. The relationships among systems in a given Architectural Description. It can be designed to show relationships of interest, (e.g., system-type interfaces, planned vs. existing interfaces).

(4) SV-4: Systems Functionality Description. The functions (activities) performed by systems and the system data flows among system functions (activities).

(5) SV-5:

(a) SV-5a: Operational Activity to Systems Function Traceability Matrix. A mapping of system functions (activities) back to operational activities (activities).

(b) SV-5b: Operational Activity to Systems Traceability Matrix. A mapping of systems back to capabilities or operational activities (activities).

(6) SV-6: Systems Resource Flow Matrix. Provides details of system resource flow elements being exchanged between systems and the attributes of that exchange.

(7) SV-7: Systems Measures Matrix. The measures (metrics) of Systems Model elements for the appropriate timeframe(s).

(8) SV-8: Systems Evolution Description. The planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation.

(9) SV-9: Systems Technology & Skills Forecast. The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future system development.

(10) SV-10:

(a) SV-10a: Systems Rules Model. One of three models used to describe system functionality. It identifies constraints that are imposed on systems functionality due to system design or implementation.

(b) SV-10b: Systems State Transition Description. One of three models used to describe system functionality. It identifies responses of systems to events.

(c) SV-10c: Systems Event-Trace Description. One of three models used to describe system functionality. It identifies system-specific refinements of critical sequences of events described in the Operational Viewpoint.

f. Data and Information Viewpoint

(1) DIV-1: Conceptual Data Model. The required high-level data concepts and their relationships.

(2) DIV-2: Logical Data Model. The documentation of the data requirements and structural business process (activity) rules.

(3) DIV-3: Physical Data Model. The physical implementation format of the Logical Data Model entities, e.g., message formats, file structures, physical schema.

g. Services Viewpoint

(1) SvcV-1: Services Context Description. The identification of services, service items, and their interconnections.

(2) SvcV-2: Services Resource Flow Description. A description of Resource Flows exchanged between services.

(3) SvcV-3:

(a) SvcV-3a: Systems-Services Matrix. The relationships among or between systems and services in a given Architectural Description.

(b) SvcV-3b: Services-Services Matrix. The relationships among services in a given Architectural Description. It can be designed to show relationships of interest, (e.g., service-type interfaces, planned vs. existing interfaces).

(4) SvcV-4: Services Functionality Description. The functions performed by services and the service data flows among service functions (activities).

(5) SvcV-5: Operational Activity to Services Traceability Matrix. A mapping of services (activities) back to operational activities (activities).

(6) SvcV-6: Services Resource Flow Matrix. It provides details of service Resource Flow elements being exchanged between services and the attributes of that exchange.

(7) SvcV-7: Services Measures Matrix. The measures (metrics) of Services Model elements for the appropriate timeframe(s).

(8) SvcV-8: Services Evolution Description. The planned incremental steps toward migrating a suite of services to a more efficient suite or toward evolving current services to a future implementation.

DRAFT

(9) SvcV-9: Services Technology & Skills Forecast. The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future service development.

(10) SvcV-10:

(a) SvcV-10a: Services Rules Model. One of three models used to describe service functionality. It identifies constraints that are imposed on systems functionality due to some aspect of system design or implementation.

(b) SvcV-10b: Services State Transition Description. One of three models used to describe service functionality. It identifies responses of services to events.

(c) SvcV-10c: Services Event-Trace Description. One of three models used to describe service functionality. It identifies service-specific refinements of critical sequences of events described in the Operational Viewpoint.

h. Standards Viewpoint

(1) StdV-1: Standards Profile. The listing of standards that apply to solution elements.

(2) StdV-2: Standards Forecast. The description of emerging standards and potential impact on current solution elements, within a set of time frames.

i. Architecture products developed under earlier versions of DODAF are related to current DODAF standards as shown in Figure C-C-2. In support of subsequent JCIDS documents or acquisition milestones, architectures built under earlier DODAF standards will be updated to the most current DODAF standard.

DRAFT

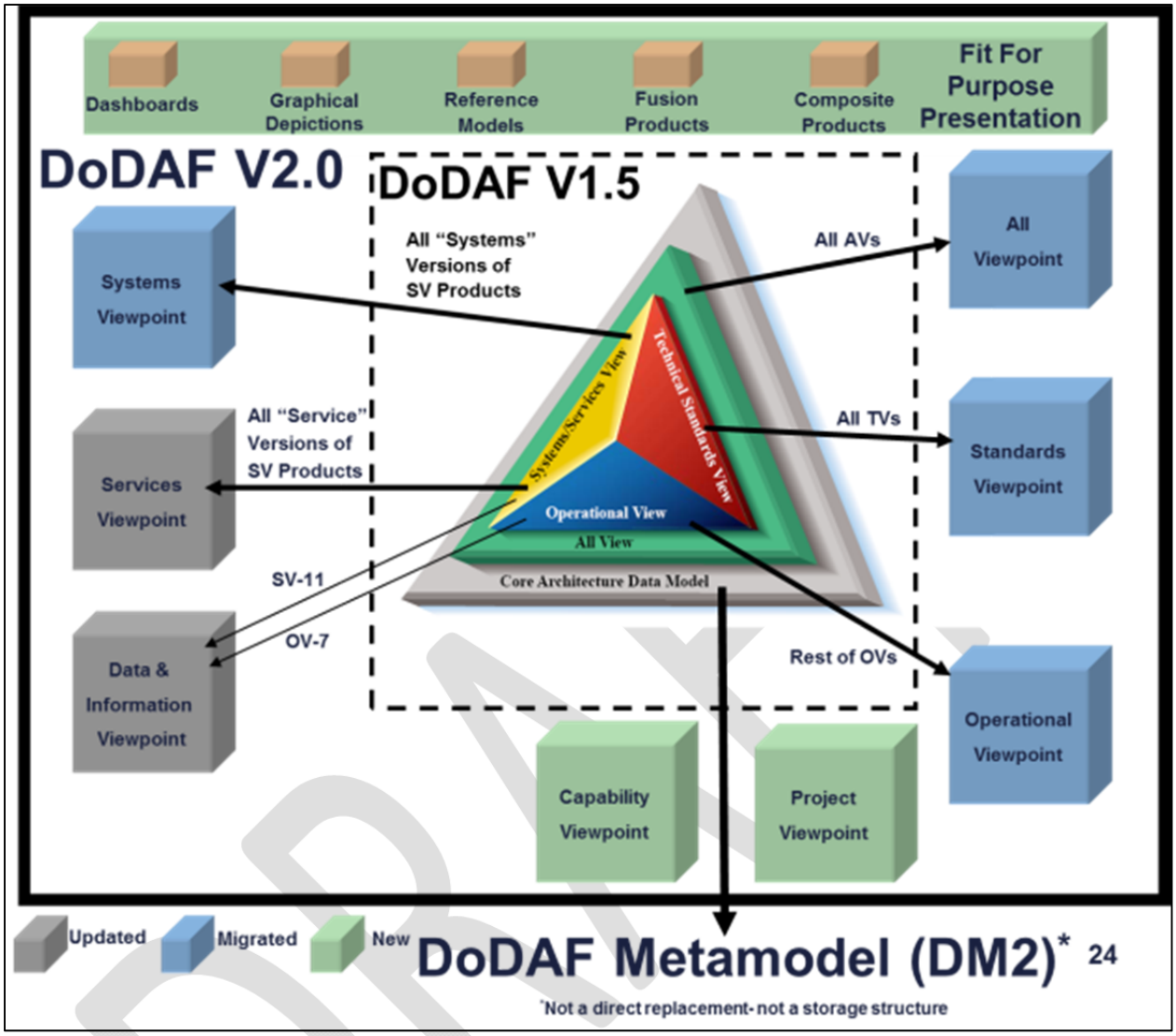

Figure C-C-2. Comparison of DODAF Standards

3. Architecture Discovery and Accessibility

a. Architecture Discovery. Architecture discovery is the first step in implementation of architecture information sharing and integration. Knowing where architecture products and data reside and having access to that information is critical to support architecture based analysis processes. At a minimum, DOD Component architecture repositories will make each architecture project with its associated products (viewpoints) and architecture data sets discoverable to enterprise content search and discovery services.

b. Use of Enterprise Services. The Defense Information Systems Agency provides enterprise services for Enterprise Content Search and Discovery (ECS&D), as well as cataloging information for discovery by DOD users. The key service that is used by the Warfighter Mission Area (WMA) architecture

federation effort is the Enterprise Catalog Service available on the Non-classified Internet Protocol Routing Network (NIPRNET) and Secure Internet Protocol Routing Network (SIPRNET). Detailed instructions for how to use the ECS&D service is located at the URLs in reference www.

(1) Architectures registered in the WMA Architecture Federation and Integration Portal (WMA-AFIP) repository are automatically made discoverable to the ECS&D service.

(2) Content registered with the catalog service is immediately discoverable to ECS&D services. When the URL points to document root, full text search functionality is enabled. Data can be loaded by:

(a) Using DOD Discovery Metadata Specification (DDMS) compliant web services by either Simple Object Access Protocol or Representational State Transfer services.

(b) Uploading a DDMS-compliant extensible markup language document to the Enterprise Catalog team

(c) Manual entry using a web based form

(3) The process consists of the following steps:

(a) Create a test collection

(b) Upload a data set ("documents") or enter data in the test collection

(c) Validate the test data

(d) Create a production collection

(e) Upload data sets/enter data in the production collection

c. Architecture Repository Types. For discovery of architecture content, the following three types of DOD Component architecture repositories have been identified:

(1) An authoritative, database driven repository that is web-accessible. (e.g. Army Capability Architecture Development and Integration Environment).

(2) An authoritative, non-database driven repository that is web-accessible (e.g. a SharePoint Portal).

(3) An authoritative repository that is not web-accessible (e.g. Shared drive, Commercial-Off-The-Shelf (COTS) tool environment, etc.).

(4) Independent of repository type, the DOD Component is responsible for:

(a) Ensuring all architectures and architecture related data developed by the Component are posted to the repository and made discoverable via enterprise services, and made accessible to external stakeholders.

(b) Working with DOD CIO and appropriate mission area leads for delivery of structured data to support architecture based analysis requirements.

(c) If existing repositories are not web-accessible, establishing processes and guidelines to make content of off-line repository web-enabled. Use of free enterprise tools such as Intelink/Inteldocs are a recommended option.

(5) DOD Components with no authoritative repository. Organizations that fall under another DOD Component that has an established architecture repository will leverage that repository if feasible.

d. Accessibility of Architectures. Discovery of architectures does not ensure that the products and related data sets are accessible by users. Accessibility must be granted in a timely fashion to authorized users in order to support architecture-based analysis and decision making processes.

(1) NIPRNET Accessibility. In most NIPRNET environments basic Common Access Card (CAC) authentication is sufficient to protect unclassified artifacts. If special protection above basic CAC authentication is required, procedures for requesting access must be posted in a visible location and access must be granted to authorized users within two business days of request.

(2) SIPRNET Accessibility. Public Key Infrastructure (PKI) Token authentication is in the process of widespread implementation on SIPRNET. If special protection above basic SIPRNET access or SIPRNET PKI Token authentication is required, procedures for requesting access must be posted in a visible location and access must be granted to authorized users within 2 business days of request.

4. <u>WMA-AFIP</u>

a. The purpose of the WMA-AFIP, located at the URL shown in reference q, is to provide a common context, federated environment for sharing of WMA architecture, mission thread, and other related WMA capability integration information and data between various authoritative repositories in order to increase effectiveness and efficiency of decision-making in a dynamic environment by our customers.

b. The WMA-AFIP supports four lines of effort:

(1) Architecture Federation Methodology Development. The Joint Staff J6, Deputy Director for Command, Control, Communications, Computers, and Cyber Integration (J-6/DDC5I) and architecture federation partners will mature the methodologies and processes to support requirements for technical solution development (web services) of a federated architecture information sharing environment. This environment allows discoverability, accessibility, visualization, reuse and traceability among various DOD-wide architecture repositories to support the following architecture information sharing needs:

(a) Architecture products (DODAF and Fit for Purpose views)

(b) Systems/services

(c) Joint activities

(d) Information/data exchanges

(e) Joint nodes/performers (i.e. organizations/facilities/ platforms)

(f) UJTL/JCA repositories (Joint Doctrine, Education, & Training Electronic Information System (JDEIS))

(g) System/service functions

(h) IT standards

(i) IT technical views

(j) JCIDS architecture documentation (i.e. KM/DS), DOD Information Network (DODIN) Technical Guidance – Federation and support for JCIDS architecture based analysis processes

(k) Process documentation/project architecture development

(l) Interoperability and capability requirement portfolio analysis of architecture data and associated artifacts/views

(m) Use case identification, support, and storyboard for web service development

(n) Feedback and process improvement

(2) Technology Development. J6/DDC5I and architecture federation partners will lead development of web-service enabled technical solutions to consume and expose baseline architectures and data from a federated set of architecture repositories. This includes:

(a) Technology support for consumption of DODAF Physical Exchange Specifications (PES) compliant web services and data.

(b) Leverage DODIN Enterprise Services.

(c) Development of the service oriented environment to support exposure of federated WMA architecture data and associated artifacts/views, products, analyses, and reports.

(d) User interface design and development (standardized portal interface).

(e) Support for architecture federation and information sharing with the Information Enterprise, Business, and Intelligence mission area Enterprise and Reference Architectures.

(f) Support for WMA Mission Thread (MT) exposure and development to provide operational context.

(g) Create reusable repository of WMA MTs.

(h) Develop web services to expose WMA MT products and data.

(i) Expose WMA MT Data through standardized portal interface.

(j) Federate Tier 2/3 WMA MTs from other repositories to Tier 1 WMA MTs.

(k) Normalize data and federate between WMA MTs.

(l) Extract and convert architectures and associated data from various tools and converting to a reusable DODAF format.

(m) Provide technical support to standardize and expose architectures from stakeholders reliant on WMA Architecture Federation (support for legacy architectures that are not located in web-enabled environments).

(3) Core Capability Support: Deployment and Maintenance of Production Environment. Support for the core capability and related services are essential to success. J6/DDC5I is responsible for development and maintenance of processes and solutions to support:

(a) Standardized portal interface maintenance and improvements

(b) Web service maintenance and improvements

(c) NIPRNET production environment

(d) SIPRNET production environment

(e) Cross-domain synchronization

(f) Configuration control/change management

(g) Federated architecture data management

(4) WMA Architecture Lexicon Development and Standardization. WMA architectures must achieve semantic understanding with DoD-level architectures and with adjacent architectures. The architecture data and associated artifacts/views must align within a common framework of semantic understanding based on the use of component and mission area taxonomies or other mechanisms aligned at the department level (e.g., Community of Interest (COI)/Community of Practice (CoP) common vocabularies or DOD-level taxonomies from capability or reference architectures). This type of alignment will support the detail required for technical analysis of capability gaps, overlaps, redundancies, interdependencies, and interoperability. This line of effort includes:

(a) Synchronization and development of WMA architecture lexicons to support the WMA EA, architecture development and federation points, aligned to the DOD IEA and Business and Intelligence mission areas.

(b) WMA architecture lexicon maintenance.

(INTENTIONALLY BLANK)

DRAFT

ENCLOSURE D

CAPABILITY REQUIREMENT DOCUMENT GENERATION

1. General Document Guidance

a. Purpose. Capability requirement documents serve as a means for Sponsors to document new or modified capability requirements and associated capability gaps, along with other relevant information, for review and validation.

(1) Capability requirement documents are generally submitted only in cases where the Sponsor deems the operational risk of unmitigated capability gaps to be unacceptable.

(2) All capability requirement documents are drafted in accordance with the formats in this enclosure and, other than for JUONs, JEONs, and DOD Component UONs, are submitted to the Joint Staff Gatekeeper for approval of Sponsor proposed JSD assignment prior to staffing via the processes outlined in Enclosure E of this manual.

(3) Capability requirement documents are then staffed for review and validation by the appropriate requirement validation authority, determined by the assigned JSD, via the processes outlined in Enclosures F and G of this manual. Capability requirement documents may not be used to support validation efforts of other capability requirements until they have been validated by the appropriate validation authority.

(4) Validated capability requirement documents, including those validated by independent validation authorities and updates to previously validated capability requirement documents, are archived in the KM/DS system at the URL in reference h to provide visibility to all stakeholders. This includes cases where the validation authority has delegated change authority to make subsequent non-KPP changes. The validated capability requirement documents in the KM/DS system serve as the basis for development of individual materiel and non-materiel capability solutions, a primary source of information for assessments within and across capability requirement portfolios, and support for acquisition, resourcing, and other decisions across DOD.

b. Coordination of Intelligence Community (IC) capability requirement documents. In accordance with reference xxx, capability requirement documents related to Major System Acquisitions (MSAs), Major Defense Acquisition Programs (MDAPs), and MAIS, or related to programs designated by the Secretary of Defense or the Director of National Intelligence (DNI) to be of special interest:

(1) Capability requirement documents that are funded primarily or wholly with National Intelligence Program (NIP) funding, will be developed, reviewed, and validated in accordance with the IC Capability Requirements (ICCR) process outlined in reference yyy.

(2) Capability requirement documents that are funded primarily or wholly with Military Intelligence Program (MIP) funding, will be developed, reviewed, and validated under the JCIDS process outlined in this manual and in reference b.

(3) Enclosure E outlines the common Gatekeeper function for both ICCR and JCIDS processes, ensuring visibility of all capability requirement documents across both processes.

c. Coordination of DBS Problem Statement and Business Case Documents

(1) DBS requirements are generally reviewed and validated by the Deputy Chief Management Officer (DCMO) in accordance with references bb and lll, unless otherwise required to obtain JCB or JROC validation.

(2) In support of reference zzz, the DCMO maintains a common Gatekeeper function with the Joint Staff Gatekeeper for the JCIDS process and the acquisition of DBS. DBS documents are submitted to the Joint Staff Gatekeeper to initiate staffing and ensure appropriate visibility and participation across processes.

d. Types of capability requirement documents. The five categories of capability requirement documents are:

(1) ICD (includes the IS-ICD variant). An ICD specifies one or more capability requirements and associated capability gaps which represent unacceptable operational risk if left unmitigated. The ICD also recommends partially or wholly mitigating identified capability gap(s) with a non-materiel capability solution, materiel capability solution, or some combination of the two. A validated ICD is an entrance criterion necessary for each MDD.

(2) DCR. A DCR recommends partially or wholly mitigating one or more identified capability requirements and associated capability gaps with non-materiel capability solutions, through changes to one or more of the eight DOTmLPF-P areas. In cases where a DCR is not generated as a successor document to a previously validated ICD, it also specifies the capability requirements and associated capability gaps for review and validation.

(3) CDD (includes the IS-CDD variant). A CDD specifies capability requirements, in terms of developmental KPPs, KSAs, and APAs, and other

related information necessary to support development of one or more increments of a materiel capability solution. A sponsor approved draft CDD is an entrance criterion necessary for each RFP release in support of the TMRR phase of acquisition and MS A acquisition decision. A validated CDD is an entrance criterion necessary for each development RFP release decision point and MS B acquisition decision.

(4) CPD. A CPD specifies capability requirements, in terms of production KPPs, KSAs, and APAs, and other related information necessary to support production of a single increment of a materiel capability solution. A validated CPD is an entrance criterion necessary for each MS C acquisition decision. To ensure that the production activities meet validated requirements in cases where the MDA waives MS C, a CPD must be validated, or CDD revalidated, prior to either the low-rate initial production (LRIP) decision or the full rate production decision in cases where LRIP is not applicable.

(5) JUON, JEON, and DOD Component UON. A JUON, JEON, or DOD Component UON specifies capability requirements driven by ongoing or anticipated contingency operations, which if left unfulfilled, would result in capability gaps leading to unacceptable loss of life or critical mission failure. Expedited staffing and validation procedures for JUONs and JEONs are outlined in Enclosure G. Expedited staffing and validation procedures for DOD Component UONs are outlined in references hh through oo. A validated JUON, JEON, or DOD Component UON, or other validated capability requirement, is a necessary precursor to initiation of rapid acquisition efforts. Warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed in accordance with reference gg. While fielding a capability solution in less than two years is a typical goal, JUONs and JEONs may also be validated to support near-term resourcing and initiation of efforts to field capability solutions in greater than two years.

(6) Limitation on IS-ICD and IS-CDD Variants. The IS variants allowed by the IS-ICD and IS-CDD are narrowly focused on facilitating more efficient and timely software development efforts, and are not appropriate for hardware development efforts or capturing capability requirements which span a broad scope of combined hardware, software, and/or DOTmLPF-P efforts. See IS-ICD and IS-CDD sections later in this enclosure for more details.

e. Support to the acquisition process. While the review and validation of capability requirement documents serve purposes broader than materiel acquisition, several of the capability requirement documents support specific points in the acquisition process as shown in figure D-1.

(1) Deliberate acquisition. Validation of three of the capability requirement documents – ICDs, CDDs, and CPDs – correspond to and inform the MDD, development RFP release/MS B, and MS C acquisition decision

points, respectively. The post-AoA (or similar study) review corresponds to the MS A acquisition decision.

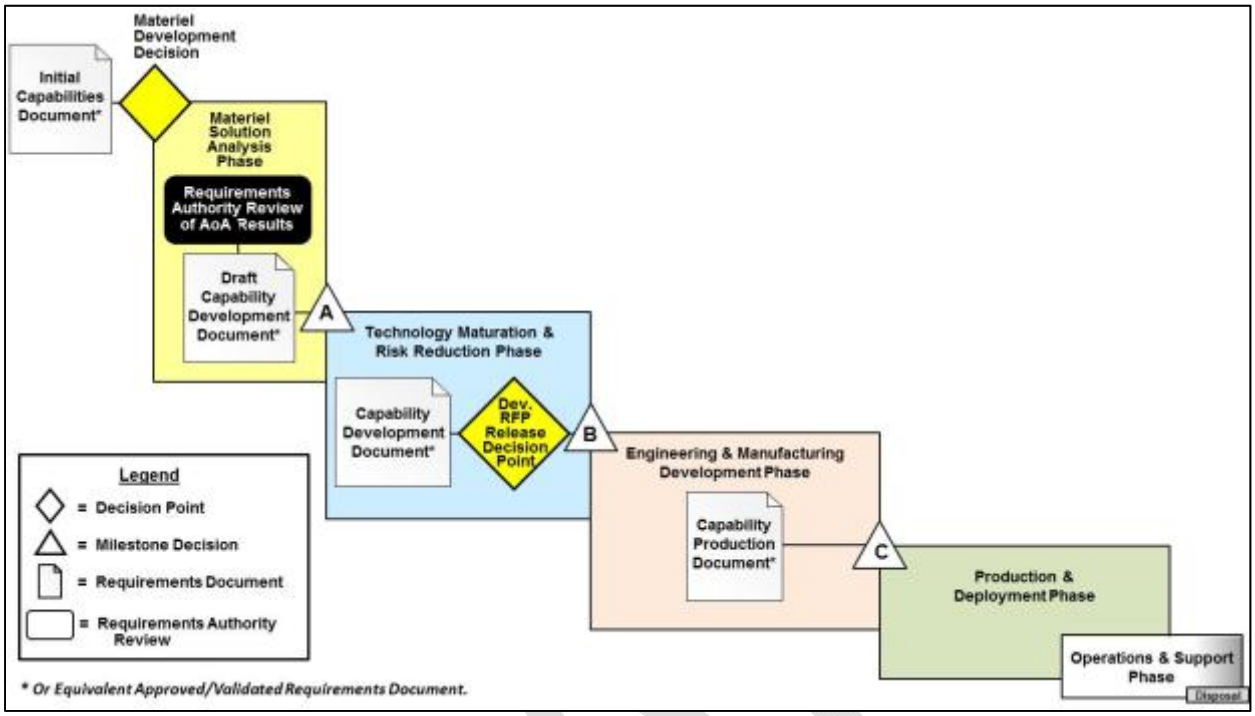

Figure D-1: JCIDS and DAS Process Interactions (Deliberate Process)

(a) ICD Validation. As part of ICD validation, the validation authority may also provide recommendations for the development of AoA guidance in support of reference bb. The data in a validated ICD, and its associated DODAF OVs and CVs, supports the acquisition process at several points, including the MDD; the AoA or similar study completed during the MSA phase of acquisition, as required; update of the EA, development of the solution architecture; the Acquisition Strategy; and the MS A acquisition decision.

(b) Post-AoA (or similar study) review. This review conducted by the validation authority as outlined in Enclosure F of this manual, together with the draft CDD generated by the Sponsor, not submitted to the Joint Staff Gatekeeper for staffing and validation at that time, supports the MS A decision point and the release of the RFP for the TMRR phase of acquisition. It does not utilize a separate capability requirement document but rather reviews the results and recommendations of the study, the KPPs, KSAs, and APAs in the draft CDD, updates to CONOPS and/or OMS/MP, and other activities conducted during the MSA phase of acquisition.

(c) CDD Validation

1. A validated CDD is a prerequisite to program initiation.

a. For most programs, program initiation occurs at MS B and the validated CDD is required prior to the development RFP release decision point leading up to the MS B acquisition decision.

b. For shipbuilding programs, program initiation occurs at MS A and the validated CDD is required prior to the earlier of MS A or the RFP release for activities to be executed during the TMRR phase of acquisition.

2. Development of a CDD is guided by the ICD, the DOD IEA in reference p or other Component EA, the AoA, the Acquisition Strategy, and the results of competitive prototyping and the preliminary design review. Incorporating knowledge gained from activities completed during the TMRR phase of acquisition into the development KPPs, KSAs, and APAs of the CDD, and proposing refinements to previously validated capability requirements if needed, is essential to having stable requirements and a technically feasible program delivering an effective capability solution to the warfighter.

3. Close collaboration between the MDA and the requirements validation authority, and their subordinate personnel, is essential during the development and review of the CDD, as the content of the CDD is critical to development of the:

a. Systems Engineering Plan (SEP), which documents technical performance measures necessary to achieve the KPPs, KSAs, and APAs.

b. Test and Evaluation Master Plan (TEMP), which establishes parameters, criteria, and desired test and evaluation (T&E) strategy, and will be further refined during the EMD phase of acquisition and updated as necessary to support developmental and operational T&E.

4. Reference bb requires Sponsors to develop and approve a draft CDD prior to MS A, not submitted to the Joint Staff Gatekeeper for staffing and validation at that time, to inform the development of the RFP in support of the TMRR phase of acquisition. The draft CDD may be refined throughout the TMRR phase of acquisition, but must be validated in time to support the development RFP release decision point. The draft CDD should contain at least the following CDD sections:

a. Operational Context (CDD Section 1), with focus on the summary of the Service and joint concepts and/or CONOPS. Ensure content is consistent with applicable DODAF OVs previously submitted, with any refinements generated from efforts to this point.

b. Capability Discussion (CDD Section 3), with focus on the summary of the previously validated capability requirements being addressed

in the draft CDD. Ensure content is consistent with applicable DODAF CVs previously submitted, with any refinements generated from efforts to this point.

c. Program Summary (CDD Section 4), with focus on the synchronization of SoS efforts across other CDDs, CPDs, and DCRs, and identification of dependencies on any legacy or future enabling capabilities.

d. Development KPPs, KSAs, and APAs (CDD Section 5), with focus on the initial/draft performance attributes resulting from the AoA or similar studies. Initial/draft attributes for the six mandatory KPPs, or justification for why they are not applicable, must also be provided. Ensure content is consistent with the DODAF SV-7, drafted to provide traceability between previously validated capability requirements and the proposed KPPs, KSAs, and APAs of the recommended capability solution.

e. Other System Attributes (CDD Section 6), with focus on attributes which require significant efforts during the TMRR phase of acquisition.

f. Technology Readiness Assessment (CDD Section 10), with focus on identifying the critical technologies which need to be matured during the TMRR phase of acquisition.

5. An AoA or similar studies must be completed, provided to the studies repository, and reviewed by the validation authority before:

a. A draft CDD is generated and approved before and in support of the RFP release for the TMRR phase of acquisition and the MS-A decision.

b. The CDD is submitted for staffing and validation ahead of and in support of MS-B, if MS-A was not required.

c. If an AoA has not been conducted, the sponsor will explain, in Section (3) of the CDD, why an AoA was not justified.

(d) CPD Validation

1. Development of a CPD is guided by applicable ICDs and CDD; the DOD IEA in reference p or other Component EA, AoA and/or supporting analytical results; the acquisition strategy, developmental and operational test results; and the CDR. The CPD Sponsor will apply lessons learned during the EMD phase of acquisition, lessons learned from previous increments, risk reduction activities, assessments (for JCTDs, qualified prototype projects, and quick-reaction technology projects), experimentation, T&E, modeling and simulation, performance and schedule tradeoffs and

affordability analysis in the delivery of the capability solution. The KPPs previously defined in a CDD may be refined (with a rationale provided) and should be tailored to the proposed system to be procured.

a. A CPD typically applies to a single increment of a single system or SoS. When the CPD is part of a FoS approach, the CPD will identify the traceability to the validated ICD or other source document, AoA or similar studies, and any related CDDs and/or CPDs that are necessary to deliver the required capability solution and to allow the required program synchronization. There may be cases where the validation authority decides it is appropriate to use a combined CPD to describe closely interdependent systems that provide the required capability solution.

b. The CPD Sponsor, in coordination and collaboration with the appropriate DOD components, agencies, and FCB, will prepare the CPD. Continuous collaboration between the Sponsor writing the CPD and the systems acquisition PM who will have to deliver a capability solution in compliance with the CPD is essential. The CPD Sponsor also will collaborate with Sponsors of related CDDs and/or CPDs that are required in FoS and SoS solutions, particularly those generated from a common ICD.

2. A validated CPD is an entrance criterion for acquisition MS C, and must be validated before the production RFP is released. To ensure that the production activities meet validated requirements in cases where the MDA waives MS C, a CPD must be validated, or CDD revalidated, prior to release of the RFP for either the low-rate initial production (LRIP) decision or the full rate production decision in cases where LRIP is not applicable.

(2) Rapid acquisition

(a) Validation of JUONs, JEONs, or DOD Component UONs support rapid acquisition in accordance with reference bb, which is conducted through a variant of the process shown in figure D-1.

(b) Rapid acquisition activities do not require typical successor documents of CDDs or CPDs unless being proposed for validation as enduring capability requirements to support transition of capability solutions to enduring PORs.

f. Document sequences and variations. Capability requirement document sequences do not have to follow a purely linear progression as shown in Figure D-1, and may follow variations as outlined in Figure D-2.

(1) The ICD is the most common starting point to document capability requirements when a materiel approach is deemed to be most appropriate.

(a) The ICD typically leads to an AoA or similar study and then the CDD and CPD for development of a materiel capability solution. In many cases, a combination of materiel and non-materiel approaches may result from an ICD.

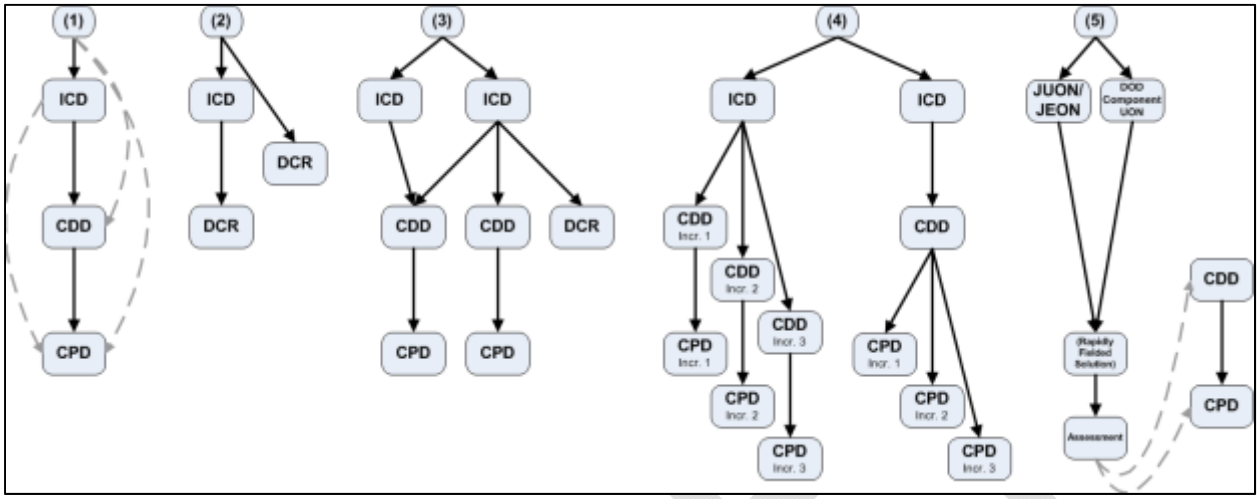

Figure D-2. Typical Capability Requirement Document Sequences

(b) In certain cases, a CDD or CPD may be generated without an associated ICD, when an ICD waiver is approved by the Joint Staff Gatekeeper, in coordination with the validation authority and MDA.

1. This approach may be appropriate when there has already been demonstration of the capability solution in an operational environment. For example, ICDs may not me required when successful JUONs, JEONs, or DOD Component UONs are proposed as enduring capability requirements, or when successful JCTDs or experiments with a positive assessment of operational utility are recommended to transition to PORs.

2. An ICD may lead directly to a CPD if capability requirements and associated capability gaps can be satisfied through US and/or foreign COTS, GOTS, or other NDI, with no significant development or integration efforts.

3. In cases where the Sponsor proposes to proceed directly to a CDD or CPD, the Sponsor will request an ICD waiver through the Joint Staff Gatekeeper in accordance with Enclosure E of this manual. The Joint Staff Gatekeeper, in coordination with the MDA and validation authority, may approve an ICD waiver, and the MDA may direct in the MDD that the MSA phase of acquisition be abbreviated or eliminated, and further development of a capability solution start directly at MS A, MS B, or MS C. If the MDA directed at MDD that a program start at MS C, a CDD is not required and a CPD is used to support MS C.

a. The Sponsor will provide ICD content, including capability requirement and capability gap table, in the appropriate successor document as outlined in DCR, CDD, and CPD document formats.

b. The Sponsor will also provide DODAF OVs and CVs applicable to the ICD in accordance with Table D-1.

(2) DCRs may be generated to document capability requirements when a non-materiel approach is deemed to be most appropriate.

(a) A DCR may be generated from one or more validated ICDs as a non-materiel solution to a previously validated capability requirement and associated capability gap, or as a complement to a materiel capability solution which will be developed through the acquisition process. The DCR will provide traceability to the applicable ICD(s). Additional DOTmLPF-P analysis may be completed as required to fully define the DCR.

(b) A DCR may be generated without an associated ICD if non-materiel approaches appear to be the most viable solution for identified capability requirements. The Sponsor will provide ICD content, including capability requirement and capability gap table, in the appropriate successor document as outlined in DCR, CDD, and CPD document formats. A Joint Staff Gatekeeper approved ICD waiver is not required for DCRs without associated ICDs.

(c) ICDs which require significant DOTmLPF-P changes as enablers to a recommended materiel approach may be staffed in parallel with the complementary DCR.

(3) Combining and splitting sequences of capability requirement document.

(a) One ICD may lead to the creation of multiple CDDs and/or DCRs, each of which contribute to satisfying the capability requirements and closing or mitigating capability gaps identified in the ICD.

(b) Two or more ICDs may lead to the creation of a single CDD, where the capability solution to be developed satisfies more than one capability requirement and closes or mitigates more than one associated capability gap.

(4) Related increments of capability requirement documents

(a) An ICD may lead to the creation of multiple CDDs for a SoS or Family of Systems (FoS) approach.

1. A single CDD may address a SoS, where a set of systems are integrated to deliver a unique capability solution.

2. Separate CDDs are required for each system in a FoS, where similar capabilities are provided through different approaches to achieve similar or complementary effects.

(b) Depending upon the nature and urgency of the capability requirements, and the current state of technology, the Sponsor may document multiple increments of capability requirements in a single CDD, and use the CDD to support multiple MS B decisions. Multiple CPDs from a single CDD are typical for incremental development efforts, such as when the DODAF CV-3 indicates different timeframes for different capability requirements or the performance levels thereof. This can facilitate the development of more mature long-term capability solutions while also providing interim capability solutions in a timely manner, while minimizing the staffing of multiple CDDs. Each increment described in the CDD may spawn a separate CPD, if needed, in support of MS C decisions for each increment. In cases of incremental development, the CDD will either:

1. Outline the general incremental strategy, with later update(s) to the CDD providing the specific KPPs, KSAs, APAs, and other requirements for future increments to be validated prior to development of those increments.

2. If sufficient information from an AoA or similar study is available, identify the specific KPPs, KSAs, APAs, and other requirements for each increment, allowing for development of future increments without needing to update and revalidate the CDD prior to starting development efforts on the identified increments. If needed, a CDD describing more than one capability increment may still be updated and revalidated before the MS B decision for each increment to incorporate the results of the activities during the EMD phase of acquisition for previous increments (i.e., updated life cycle cost, schedule, performance, and quantity tradeoffs, testing, and lessons learned).

(5) Urgent/Emergent Capability Requirement Documents

(a) JUONs, JEONs, and DOD Component UONs are validated through streamlined staffing processes to allow rapid acquisition efforts to field a capability solution in an expedited timeframe. CDDs and CPDs are not required for initial development and fielding, and various considerations of the deliberate acquisition process are streamlined or bypassed in the interest of timeliness.

(b) Following the fielding of capability solutions to JUONs and JEONs, the requirement Sponsor completes an assessment of operational utility to provide essential feedback for continuing rapid acquisition efforts

and/or to identify the need for long term sustainment of the capability solution through the deliberate acquisition process. Post-fielding assessments of DOD Component UONs are at the discretion of the DOD Component validation authority.

(c) For capability solutions proposed for transition to the deliberate acquisition process, the JUON, JEON, or DOD Component UON, along with the associated assessment, serves as partial source data for the capability solutions Sponsor to generate the CDD or CPD supporting validation of enduring capability requirements. The validation authority determines the proper document to be used based upon the MDA's identification of a point of entry into the acquisition process

(d) In cases of transitioning JUONs, JEONs, or DOD Component UONs where no further development or production is planned, the Sponsor will coordinate with the validation authority and the MDA to identify potential tailoring of the CPD. This ensures that essential aspects of the validated enduring capability requirements are captured to enable robust management of capability requirement portfolios.

(e) Sponsors of rapidly fielded capability solutions proposing transition from the urgent/emergent to the deliberate requirements and acquisition processes will submit the supporting assessment of operational utility for the rapidly fielded capability solution to the studies repository prior to submitting the associated CDD or CPD for staffing and validation.

g. Capability Requirement Document Updates/Revisions

(1) Updates to a capability requirement document are required if the Sponsor proposes changes to the capability requirements, including KPPs, KSAs, and APAs, after validation, or if changes are made in the approved Service and joint concepts, CONOPS, or EA and solution architecture, which affect the capability requirements and/or capability solution. Updates to capability requirement documents may also be required as a result of JROC/JCB Tripwire, CIP breach reviews, Nunn-McCurdy Unit Cost Breach, or MAIS Critical Change Report reviews.

(a) The validation authority generally retains change authority for KPPs and other aspects of documents which impact certifications or endorsements, unless otherwise delegated in the validation memorandum. The validation authority will issue a new or updated validation memorandum to indicate approval of the updated document.

(b) The validation authority generally delegates change authority for KSAs, APAs, and other aspects of documents, unless otherwise retained in the validation memorandum. The Sponsor organization with delegated change

authority will issue a change memorandum to indicate approval of the updated document.

(c) Certifications and endorsements will be reviewed to ensure that those impacted by the proposed changes, or are otherwise out of date, receive updated certification and endorsement prior to validation of the updated document.

(d) Updated documents are not authoritative until the updated document and the associated signed approval memorandum are provided to the Joint Staff Gatekeeper for archiving.

(2) A CDD may be updated in lieu of a CPD to support MS C acquisition decisions for each successive capability increment in cases where EMD activities have not driven substantive changes to the developmental KPPs, KSAs, and APAs, and other supporting data throughout the validated CDD, and the amendments do not adversely affect the acquisition of the previously validated capability increments. To use a CDD update in lieu of CPD, the Sponsor will resubmit the updated CDD in accordance with the normal staffing processes for review, update of certifications/endorsements, and validation.

(3) In accordance with reference bb, the Sponsor will review the AoA or similar study for continuing relevance prior to each MS decision. Any applicable updates to capability requirement document, and the impact upon previous AoA recommendations, should be included in that review.

(4) No additional changes or amendments will be made to previously validated ORDs or other legacy capability requirement documents, unless minor changes only are approved by the Joint Staff Gatekeeper and Lead FCB.

(a) To facilitate significant amendments or changes, Sponsors shall transcribe legacy content, and any previously validated changes or amendments, into the appropriate current document format for staffing and validation. Updates will incorporate, or justify the absence of, the mandatory KPPs identified in Appendix A to this enclosure.

(b) The legacy document will be submitted as an attachment to the updated capability requirement document in the KM/DS system, unless it is already resident in the KM/DS system.

(5) Updates to capability requirement documents will be submitted to the Joint Staff Gatekeeper in accordance with Enclosure E to either initiate staffing for review and potential re-validation for changes requiring JCB or JROC validation, or for visibility and archiving purposes for changes under the authority of the DOD Component validation authority.

h. Situations not requiring new capability requirement documents. Capability requirement documents are not written to take the place of an RFF or RFC where materiel capabilities already exist in the joint force and the GFM processes should be used to make the forces/capabilities available to the Combatant Commanders (CCDRs). In cases where previously fielded capability solutions do not exist in sufficient quantities to be satisfied by GFM:

(1) If the Sponsor has a validated CDD or CPD for a capability solution, including rapidly fielded capability solutions already transitioned to a POR, the Sponsor may submit the document with updated quantities for revalidation by the appropriate validation authority.

(2) If a different Sponsor has a validated CDD or CPD for a capability solution, including rapidly fielded capability solutions already transitioned to a POR, a Sponsor may submit a new Joint DCR with the requirement for increased quantities of previously fielded capability solution for validation by the appropriate validation authority. The recommended solution may be an increase in quantities in the other Sponsor's CDD or CPD, along with appropriate transfer of funding between Sponsors to provide for the increased quantities.

(3) If a Sponsor has a validated JUON, JEON, or DOD Component UON for a rapidly fielded capability solution, and that capability solution has not been validated, via a CDD or CPD, as an enduring capability requirement in support of transition to a POR, the Sponsor may submit an update to the originally validated document with updated quantities for revalidation by the appropriate validation authority.

(4) If a different Sponsor has a validated JUON, JEON, or DOD Component UON for a rapidly fielded capability solution, and that capability solution has not been validated through a CDD or CPD as an enduring capability requirement in support of transition to a POR, the Sponsor may submit a new JUON, JEON, or DOD Component UON with the urgent requirement for additional quantities of a previously fielded capability solution.

(a) The recommended solution may be an increase in quantities of the other Sponsor's rapidly fielded capability solution, along with agreement between Sponsors to provide funding for procurement, operations, and support of the increased quantities. Such an agreement will be provided to the Joint Staff Gatekeeper and forwarded to the JRAC.

(b) In cases where the original capability requirements were validated as a DOD Component UON, the VCJCS shall designate the shared capability requirements as a JUON or JEON, and the rapidly fielded capability solution will be managed in accordance with reference gg.

(5) For urgent quantity increases in support of ongoing or anticipated contingency operations, when timely changes cannot otherwise be accomplished, a JUON, JEON, or DOD Component UON may be used in place of a DCR or an update to a validated CDD or CPD in the cases outlined above.

i. Precedence of recommended approaches. When conducting analyses and drafting capability requirement documents, Sponsors will consider both non-materiel and materiel solutions, and to the maximum extent possible, recommend approaches in the preferred order listed below, starting with non-materiel approaches and then in accordance with reference aa. If applicable, Sponsors will explain in the document summary why less preferred approaches were recommended.

(1) Implementation of DOTmLPF-P changes which do not require development and procurement of a new materiel capability solution.

(2) Procurement or modification of commercially available products, services, and technologies, from domestic or international sources, or the development of dual-use technologies.

(3) The additional production or modification of previously developed U.S. and/or allied / partner-nation / other US government agency/department systems or equipment.

(4) A cooperative development program with one or more allied nations.

(5) A new, joint, DOD Component or other US government agency/department development program.

(6) A new DOD Component-unique development program.

j. Required DODAF Views. DODAF views applicable to supporting all capability requirement documents are shown in Table D-1. These views are used to facilitate validation decision making and capability requirement portfolio management. Additional DODAF views applicable to the NR KPP are outlined in Appendix E to this enclosure. More detail on each DODAF view is available in Appendix C to Enclosure C of this manual and in reference ppp. Examples of DODAF views supporting capability requirement documents are available at the URL in reference c.

(1) DODAF views and associated data supporting the capability requirement document shall be made accessible by Sponsors through a URL to the architecture data repository. Sponsors without architecture data repositories connected to the WMA-AFIP accessible through the URL in reference q should refer to Appendix C to Enclosure C of this manual for more information. Only the DODAF views specified by the document formats, or

additional views deemed appropriate by the Sponsor, should be included in the actual capability requirement document.

(2) DODAF views and associated data submitted in support of narrowly scoped ICDs, and CDDs/CPDs supporting development of particular materiel capability solutions, are expected to align the new or updated DODAF views with previously generated EAs, with updates to the EAs made as necessary.

(3) DODAF views and associated data submitted in support of broadly scoped ICDs are expected to represent the initial or updated EA associated with the scope of the ICD.

(4) Data for DODAF views should be captured to the greatest extent possible during CBAs to reduce workload when generating capability requirement documents and performing follow-on efforts. As Sponsors define new or updated capability requirements, and develop associated materiel and non-materiel capability solutions, they should update previously submitted architecture data and associated artifacts/views rather than re-creating the architecture data and associated artifacts/views. In addition to saving time and effort, re-use of architecture data and associated artifacts/views reduces the likelihood of unexpected disconnects between current and previous architectures.

Document	**OV-1**	**OV-3**	**OV-4**	**OV-5a**	**CV-2**	**CV-3**	**CV-6**	**SV-7**	**SV-8**
ICD/DCR	S	S	S	S	S	S	S		
CDD/CPD	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	S/P	S/P
Note 1	All capability requirement documents should leverage and update DODAF views generated during the CBA or other prior analysis, to facilitate more efficient reuse and leverage in follow-on activities throughout the requirements and acquisition processes.								
Note 2	S: The Sponsor, or operational user/representative, is responsible for development of the architecture data S/P: The Sponsor, or operational user/representative, works jointly with the program office (depending upon program stage), to develop the architecture data. DOD Components may have additional architectural/regulatory requirements for CDDs/CPDs. (e.g. – HQDA requires the SV-10c, USMC requires the SV-3, etc.)								
Note 3	The OV-5a must use UJTs (and Service task list extensions, if applicable) for alignment of activities. Programs must align or extend to the leaf-level activities. In cases where the program supports an activity not represented in the UJTL, the shortcomings are to be identified in the activity taxonomy and considered for incorporation upon the next update of the UJTL.								

Table D-1. DODAF views supporting capability requirement documents.

k. Formatting Standards

(1) Software compatibility. Microsoft Office 7.0 or greater.

(2) Paper size and margins. Use 8.5-inch by 11-inch pages with 1-inch margins on all sides.

(3) Font. For document content, use Times New Roman or Bookman Old Style 12-point for document content. For classification markings, use Arial 24-point bold.

(4) Style. Underline paragraph headings. Use bold only for emphasis within text. Use sentence case throughout text and uppercase for titles.

(5) Spacing/alignment. Single-space draft and final versions. Double-space between paragraphs, bullets, and between titles and text. Left align text. Center titles.

(6) Indentation. Indent paragraphs 0.5 inch from the left margin. Indent subparagraphs an additional 0.5 inch from left margin.

1. Classification and Releasability

(1) All documents containing classified information will display appropriate classification and releasability markings (overall and portion) in accordance with reference aaaa. See Enclosure E of this manual for impacts of classification on procedures for document submission to the Joint Staff Gatekeeper.

(2) For capability requirement documents advocating creation of international acquisition programs with allies/partner nations, Sponsors will consider, to the greatest extent possible, foreign disclosure review and document structuring to facilitate releasability, in whole or in part, to the nation(s) concerned.

(3) Capability requirement documents and supporting data are joint information, the release of which is governed by reference bbbb. See reference a for additional responsibilities related to release of capability requirement documents and other JROC information.

DRAFT

2. ICD

a. Background

(1) The purpose of an ICD is to document capability requirements and associated capability gaps in cases where the Sponsor deems the operational risk of unmitigated capability gaps to be unacceptable.

(a) The ICD, and its associated DODAF OVs and CVs, provides traceability to the operational context and other relevant factors for the capability requirements, quantifies any associated capability gaps and operational risks across the joint force based upon the identified capability requirements, and proposes materiel and/or non-materiel approaches to closing or mitigating some or all of the identified capability gaps.

(b) The ICD serves as the basis for validation by the appropriate validation authority identified in Enclosure F of this manual.

(2) For capability requirements likely to be addressed by IS solutions – software development, and off-the-shelf hardware if required – Sponsors should consider the IS-ICD variant detailed in the next section of this enclosure. For capability requirements likely to be addressed by a mix of IS and non-IS solutions, Sponsors must use the regular ICD format and consider an IS-CDD after ICD validation to streamline the IS portion of solution development.

b. Format

(1) Cover Page. The cover page of an ICD shall include the following information.

(a) Classification.

(b) Title, starting with the phrase "Initial Capabilities Document for…"

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New ICDs, and modifications to previously validated ICDs, must be endorsed by the Sponsor J8-equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of Requirements

Management Certification Training (RMCT) in accordance with Enclosure A of this manual.

(f) Proposed validation authority.

(g) Proposed MDA.

(h) Proposed JSD. See Enclosure E of this manual for more detail of JSDs.

(2) Validation Page

(a) While a document is in draft, a placeholder page will be included, with a statement of: "This document (include revision numbering as appropriate) has not yet been validated, and shall not be considered to be an authoritative source for the content herein. This document may be considered authoritative only when this page has been replaced by a signed validation memorandum from the appropriate validation authority."

(b) Once validated by the requirement validation authority, the placeholder page will be replaced by the signed memorandum indicating validation of the document.

1. For documents with JSD of JROC Interest or JCB Interest, the placeholder page will be retained until the signed JROCM is inserted. Any Sponsor approvals are not authoritative with respect to the document validation prior to JROC or JCB validation, and then only to the degree the JROCM delegates follow on authority to the Sponsor. The placeholder validation page will be retained until replaced by the validation JROCM.

2. For documents with JSD of Joint Integration or Joint Information, the Sponsor signed memorandum (or equivalent document/form) is authoritative with respect to the document validation.

(c) If revisions to a document are proposed after validation, the placeholder page will be reinserted ahead of the original validation memorandum, until the updated validation memorandum is inserted. The original validation memorandum and memoranda validating subsequent changes, if applicable, are retained as part of the authoritative document.

(3) Executive Summary. An executive summary, not to exceed one page, shall follow the validation page and precede the body of the ICD. As the sponsor develops the executive summary, they should leverage applicable content from the DODAF AV-1 generated during the CBA to the greatest extent possible.

c. Document body. The body of the ICD shall have the following five sections, and shall be no more than 10 pages long. In cases where a limited amount of content is classified at a higher level than the bulk of the document, a classified annex may be used to facilitate greater access to the document at lower classification levels. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail.

(1) Operational Context

(a) The purpose of this section is to provide context for the capability requirements identified in the ICD. This information facilitates review and validation of the ICD from the standpoint of how the capability requirements contribute to the missions and activities of the joint force.

1. Narrative in the operational context section should be derived from and consistent with DODAF OVs generated during prior analysis, as modified for the scope and purpose of the ICD, including the DODAF OV-1, OV-3, OV-4, and OV-5a.

2. Other than the DODAF OV-1 which is required in this section, do not include other architecture data and associated artifacts/views in the document unless specifically needed for illustration purposes in the body of the ICD. Provide data for the remainder of the required DODAF OVs in the repository located at the URL specified in the reference section of the document.

(b) Describe the range of military operations being addressed and the traceability to relevant parts of Unified Command Plan (UCP)-assigned missions, OPLANs/CONPLANs, SSA Products, Service and joint concepts, CONOPS, and/or other relevant factors to which the capability requirements identified in the ICD contribute. If operations are required in, or after exposure to, CBRN environments, discuss how and where this fits in the operational context.

(c) Identify the timeframe under consideration for IOC and FOC based on input from supported/supporting CCMDs and the acquisition community. Note that the timeframes presented in this section must be consistent with the DODAF CV-3 and any phasing of capability requirements proposed in section (3) of the ICD.

(d) Identify what measurable operational outcomes are required; what effects must be produced to achieve those outcomes; how they

complement the integrated joint/multinational warfighting force; and what enabling capabilities are required to achieve the desired operational outcomes.

(e) Ensure any key intelligence support capabilities required to enable the capability solution's operational activities are addressed and documented within the operational context.

(f) Include the DODAF OV-1 in this section, and where applicable, ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the DODAF OV-1.

(2) Threat Summary

(a) The purpose of this section is to provide context for the capability requirements identified in the ICD, and to provide appropriate traceability to the DIA- or Service-approved threat products used during the development of the capability requirements and identification of associated capability gaps. This information also enables threat assessment as part of the intelligence certification provided during ICD review and validation, and facilitates more rapid review and updating of successor documents when/if applicable threat products are updated.

1. ICDs address capability requirements and associated capability gaps related to the conduct of operational tasks and missions, rather than defining specific capability solutions and their performance parameters. ICDs should therefore provide sufficient information and analysis to allow general identification of intelligence support requirements associated with closing or mitigating the identified capability gaps.

2. Although ICDs do not contain a paragraph dedicated to intelligence supportability, Sponsors should ensure that intelligence support requirements necessary to enable the concepts and CONOPS in the scope of the ICD are identified in terms of the broad intelligence supportability categories described in Appendix I of this enclosure, and included in ICD Operational Context, Capability Requirements and Gaps/Overlaps, and Assessment of Non-Materiel Approaches sections, as appropriate.

(b) Cite the threat products used during the development of the capability requirements identified in the ICD.

1. For ICDs likely to result in ACAT ID or ACAT IAM programs, ensure the most current DIA-approved threat products are used to develop the ICD and any associated studies or analysis.

2. For all other ICDs, ensure the most current DIA- or Service-approved threat products are used to develop the ICD and any associated studies or analysis.

(c) Provide a general description of all threat capabilities in the expected operational environment, the nature of current and anticipated threats (both lethal and non-lethal) which are a factor in setting the capability requirements and initial objective values, and threat tactics, if available. Include CBRN threats if the operational context includes the ability to operate in CBRN environments.

1. Ensure judgments or extrapolations regarding adversarial capabilities are appropriate, logical, complete, and consistent with DIA- and Service-approved threat products. Also consider threats to follow-on research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts. Note that threats are factors that an adversary can control and direct, or will be able to direct, and do not include environmental or natural factors such as weather or terrain.

2. Ensure characteristics of adversary threat capabilities which are a factor in establishing capability requirements and associated initial objective values are documented as CIPs, which enables the IC to provide more robust monitoring of threat changes throughout a capability solution's life cycle.

(3) Capability Requirements and Gaps/Overlaps

(a) The purpose of this section is to both identify the specific capability requirements, with associated JCAs and operational attributes, and to assess associated capability gaps and/or redundancies in terms of a comparison between capability requirements and capability solutions currently available to the joint force or in development.

1. Narrative in the capability requirement and capability gap section should be derived from and consistent with DODAF CVs generated during prior analysis, as modified for the scope and purpose of the ICD, including the DODAF CV-2, CV-3, and CV-6.

2. Data for the required DODAF CVs is to be provided in the repository located at the URL specified in the reference section of the document.

(b) In separate paragraphs, describe the capability requirements as identified during the CBA or other study in terms of the required operational attributes with appropriate quantitative parameters and metrics, e.g.,

outcomes, time, distance, effect (including scale), obstacles to be overcome, supportability, etc. See Appendix A to Enclosure C of this manual for examples of appropriate operational attributes which should be used where applicable, although other operational attributes may be identified and used when those in Appendix A to Enclosure C of this manual are not appropriate.

1. Indicate the initial objective value for each operational attribute, together with specific operational implications which drive the value to be proposed at the specified level. The intent is to provide a point value which satisfies the operational need(s) for the capability, while serving as the starting point for analysis supporting capability requirement trade-offs above and below the initial objective value.

a. Values listed as "TBD", those specified only as a ratio relative to the value of a legacy capability solution, or operational attributes without quantifiable measures, are not allowed. In such cases, the Sponsor is not ready to document capability requirements in an ICD and must perform additional analysis based upon the applicable Service and joint concepts or CONOPS before finalizing the ICD.

b. Initial objective values should be the value necessary to achieve mission objectives with moderate operational risk. Explain why the capability requirements are essential to the Sponsor in order to achieve assigned goals and objectives. This discussion should leverage the DODAF CV-6 which provides traceability between the operational tasks in the DODAF OV-5a with the capability requirements in the DODAF CV-2. Include assessment of operational implications – increased or decreased operational risks – which may be a factor as capability requirements are traded up or down during follow-on analysis and development efforts.

2. Define capability requirements in the lexicon established for the JCAs, the tasks, standards, and conditions from the applicable Universal Joint Tasks or DOD Component equivalents, the relevant range of military operations, and the timeframe under consideration.

3. Capability requirements should be general enough so as not to prejudice decisions in favor of a particular capability solution but specific enough to evaluate alternative approaches to achieve the capability.

4. Capability requirements shown in this section need only be those requirements which have associated gaps or overlaps/redundancies. This does not preclude the inclusion of capability requirements which are currently satisfied by capability solutions and do not have associated capability gaps, if inclusion of such capability requirements provides necessary context or serves other purposes. (i.e. – a capability requirement might be satisfied by a fielded capability solution, but the Sponsor proposes a much more cost

effective capability solution or a consolidation of multiple independent solutions into a single common capability solution.)

5. Ensure that all intelligence support requirements, resources, or other programs/capabilities necessary to enable each capability are identified in terms of the broad descriptions of categories discussed in this enclosure. Ensure that any current or projected gaps or shortfalls in intelligence support capabilities are identified and documented.

(c) For each capability requirement identified, describe the capability gaps or overlaps in terms of the difference between the initial objective values enumerated above and the performance levels of capability solutions currently available to the joint force or in development. Identify those capability requirements for which there exist overlaps or redundancies, including considerations of existing or planned capabilities in other DOD Components, other US government agencies/departments, and allied/partner nations. Assess whether the overlap is advisable for operational redundancy, or if the overlap should be evaluated as potential tradeoffs to satisfy identified capability gaps.

1. When describing "current capabilities" in the narrative paragraphs, in order to assess the gap between the proposed capability requirements and current state of the art, one must consider all PORs and rapidly fielded capability solutions in the joint force.

a. Sponsors may not exclude viable capability solutions from the comparison because they are not the Sponsor's preferred solution, or because they are developed and operated by another DOD Component.

b. Prior to authoring this section, Sponsors must ensure review of identified capability gaps by someone with visibility into capability solutions protected by higher classification levels.

c. If identified capability gaps would be different in light of capability solutions protected by higher classification levels, Sponsors may provide supplemental data in the form of a classified appendix as described at the end of the ICD format guidance.

2. When describing a recapitalization (or "next generation") situation, the "current capabilities" must consider the capability solution being replaced, as well as other viable solutions as noted above, even though the plan may be to retire the older solution as the new solution becomes available. Life extension or continuing/restarting production of the previously fielded capability solution, or possibly leveraging portions of previously fielded capability solutions, may be part of tradeoff discussions and/or follow-on AoA activities.

(d) Clearly identify how each capability gap identified impacts the operational context in section (1) of the ICD, in terms of inability to execute part or all of an operational plan and/or unacceptable levels of operational risk. This discussion should leverage the DODAF CV-6 which provides traceability between the operational tasks in the DODAF OV-5a with the capability requirements in the DODAF CV-2. Where workarounds are feasible until the requirements proposed in the ICD are satisfied by capability solutions, identify the workarounds and operational risk(s) associated with them.

(e) Summary table. Provide a summary table for the relationship between capability requirements in each JCA and relevant operational attributes, and associated gaps/overlaps with respect to current or programmed force capabilities in a table as shown in Table D-2.

Capability Requirements			**Current Capabilities** (basis for gap/overlap)	
Capability Requirement Name/Number	**Operational Attribute/ Metric**	**Initial Objective**	**Source/ System**	**Current Performance**
(for example) JCA 2.2: BA / Collection				
Capability Requirement 1			Description	
	Attribute 1.1	Value (no TBDs)		Value (no TBDs)
	Attribute 1.n	Value (no TBDs)		Value (no TBDs)
(for example) JCA 3.1: FA / Maneuver				
Capability Requirement 2			Description	
	Attribute 2.1	Value (no TBDs)		Value (no TBDs)
	Attribute 2.n	Value (no TBDs)		Value (no TBDs)
(for example) JCA 3.2: FA / Engagement				
Capability Requirement 3			Description	
	Attribute 3.1	Value (no TBDs)		Value (no TBDs)
	Attribute 3.n	Value (no TBDs)		Value (no TBDs)
JCA X.x: TBD / tbd				
Capability Requirement n			Description	
	Attribute n.n	Value (no TBDs)		Value (no TBDs)

Table D-2. Example Capability Requirement and Gap/Overlap Table

1. In cases where phased introduction of capabilities is appropriate to the concepts or CONOPS, different levels of capability requirements can be listed for different timeframes, and must be consistent with the DODAF CV-3.

2. The example table shown is intended to be illustrative, and may be tailored as long as it still clearly articulates both the capability requirements and the difference between those capability requirements and the current/programmed joint force.

(4) Assessment of Non-Materiel Approaches

(a) The purpose of this section is to identify what non-materiel approaches can close or mitigate capability gaps identified in Section (3) of the ICD, and what remaining capability gaps may require a materiel solution. This information also informs the DOTmLPF-P review and endorsement conducted during staffing of the document. All DOTmLPF-P considerations must be addressed in an ICD unless they are not applicable in a particular case. In cases where one or more of the DOTmLPF-P factors may not applicable, the Sponsor shall coordinate with the applicable organization identified in Appendix H to Enclosure F of this manual to ensure that the DOTmLPF-P endorsement is not withheld due to missing information.

(b) Summarize the changes to DOTmLPF-P that can satisfy the capability gaps in part or in whole. Include consideration of capabilities in allied/partner nations, other US government agencies/departments, and other DOD Components. Ensure that organizational implications of DOTmLPF-P recommendations are captured in updates to the DODAF OV-4.

(c) If there is an issue of sufficiency in capability solutions currently available to the joint force or in development (not enough units of capability to be effective) without requiring increased proficiency in capability solutions currently available to the joint force or in development (not enough performance in each unit of capability), capture the assessment of "little-m" quantity changes in this section.

(d) Ensure intelligence-related aspects of DOTmLPF-P approaches are adequately identified and discussed in this paragraph. Ensure the documentation reflects that the IC's expertise has been adequately leveraged. If a capability solution to the requirements in this ICD is expected to require new, unique, and unplanned intelligence support, or will require additional support (as projected by the intelligence architecture), then consider and document whether the current IC architecture can support the new or additional support requirements identified and, if necessary, what DOTmLPF-P changes are required.

(e) See Appendix H to this enclosure for more guidance on DOTmLPF-P content.

(5) Final Recommendations

(a) The purpose of this section is to identify one or more paths forward to satisfy the capability requirements and close or mitigate associated capability gaps identified in the document. Ensure materiel and non-materiel recommendations reflect a thorough understanding of the threat considerations and intelligence support requirements and capabilities for the functional and operational areas.

(b) Identify DOTmLPF-P recommendations to be considered as part of a materiel solution.

(c) Identify DOTmLPF-P recommendations to be considered independent of a materiel solution.

(d) For all capability requirements that cannot be met using non-materiel approaches, include specific recommendations on the type of materiel approach preferred to close or mitigate each capability gap, which may be used by the MDA to inform the scope of the AoA or similar study:

1. Evolution of a previously fielded capability solution(s) with significant capability improvement, including development and fielding of improved IS, improved components or subsystems to address high obsolescence rates, or other upgrades and product improvements.

2. Replacement or recapitalization of a previously fielded capability solution(s) with significant capability improvement. The ICD will describe plans to retire previously fielded capability solution(s) as the new capability solution(s) is brought into service, and whether quantities in the joint force should be reduced based on increases in capability.

3. Introduction of a transformational capability solution(s) that differ significantly in form, function, and operation from previously fielded capability solution(s). They may address gaps associated with a new mission, or describe breakout capability solution(s) that offer significant improvement over current capability solution(s), or transform the ways of accomplishing a mission.

4. In developing the recommended approach, the sponsor should update the appropriate DODAF OVs and CVs generated in prior analysis to reflect the implications of the recommended approach. If DODAF OVs and CVs were not generated during prior analysis, they must be generated to support submission of the ICD.

(e) Leverage of S&T to reduce operational risk, ensuring technologies are sufficiently mature prior to initiation of a new or enhanced capability solution. Identify ongoing or new developmental technologies that have the potential to mitigate capability gaps. Emphasize technologies that

enhance joint warfighting capability against emerging threats and/or increase affordability within the capability requirement portfolio.

(f) Acceptance of operational risk. Not every identified capability gap needs to be immediately addressed by a capability solution or S&T effort. A relatively low priority of the capability requirement to the overall joint force may not justify the life cycle costs of taking further action at the present time.

(g) Affordability

1. While the ICD should not have a specific capability solution in mind, nor the level of detail required to produce associated cost estimates, a constrained fiscal environment with competing demands for resources requires that opportunity cost inform life cycle cost, performance, schedule, and quantity tradeoff discussions.

2. Identify the notional resources available to pursue a capability solution, including materiel and non-materiel costs over its anticipated life cycle. This data is not intended to reflect resource costs of a specific capability solution which will be determined later in the process, but rather identify what resources are proposed to be available, and if necessary highlight resource shortfalls which may require taking more operational risk by reducing resources in other areas.

d. Appendices. Only the following four appendices are allowed in the document. Additional reference documents or data may be submitted in accordance with procedures outlined in Enclosure E of this manual.

(1) Appendix A: References. Ahead of other references provided in this appendix, provide a URL for required architecture data and associated artifacts/views identified in Table D-1 and, if applicable, Table D-E-3.

(2) Appendix B: Acronym List.

(3) Appendix C: Glossary. As the sponsor develops the document glossary, they should leverage applicable terms from the DODAF AV-2 generated during the CBA to the greatest extent possible. The document glossary and the DODAF AV-2 do not have to be identical, as some terms will only apply to the document or the DODAF architecture. Terms that apply to both must be consistent between the document and the architecture products.

(4) Appendix D: (Optional) Classified Annex. A classified annex may be used in cases where only a small subset of the document needs to be protected at a higher classification level. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified

content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail. If used, classified annexes shall be provided to the Joint Staff Gatekeeper or Joint Staff J-8, Special Access Program Coordinator (J-8/SAPCOORD) in accordance with the classification of the annex.

DRAFT

3. IS-ICD

a. Background

(1) The purpose of an IS-ICD is focused on facilitating more efficient and timely software development efforts, and is not appropriate for hardware development efforts or capturing capability requirements which span a broad scope of combined hardware, software, and/or DOTmLPF-P efforts.

(a) The IS-ICD is a variant of the regular ICD, implementing the "IT Box" model outlined in this section. IS-ICDs streamline the requirements process relative to IS efforts by delegating requirements oversight and document formats for subsequent documents as identified in the IS-ICD. This provides IS programs greater flexibility to incorporate evolving technologies and achieve faster responses from requirement validation processes than is typical for other kinds of materiel or non-materiel solutions.

(b) The document serves as the basis for validation by the appropriate validation authority identified in Enclosure F of this manual. Applicability of any potential streamlining of acquisition processes is at the discretion of the MDA in accordance with references aa and bb.

(2) IS-ICDs are appropriate for:

(a) The procurement or modification of GOTS/COTS IS products from domestic or international sources, or the development of dual-use technologies.

(b) The additional production or modification of previously-developed U.S. and/or allied /partner-nation / other US government agency/department IS products.

(c) Development, integration, and acquisition of customized application software, including commercial IS capability solutions with integrated, DOD-specific performance characteristics/standards.

(d) All hardware associated with an IS-ICD must be COTS/GOTS. Hardware modifications are restricted to those necessary for system integration and enhancements to meet capability requirements specified in the IS-ICD, and hardware refresh due to obsolescence.

(e) Approaches where the capability solution involves research, development, and/or acquisition of applications systems software, and the projected life cycle costs exceed $15 million. IS-ICDs with life cycle costs less than $15 million may be submitted for review and validation if validated requirements are needed to support budgetary requests or other purposes.

(3) IS-ICDs are NOT appropriate for:

(a) Software embedded as a subset of a capability solution developed under other validated capability requirement documents. In this case, the software requirements are validated as part of the capability requirements for the overall capability solution.

(b) Software requiring a host platform, such as a manned or unmanned vehicle, which does not yet have validated capability requirement documents. In this case, the software requirements can be included in the capability requirements of the host platform, or as a separate IS-ICD submitted after validation of the host platform capability requirement documents.

(c) Increases in quantities of previously fielded IS without modification, which are not addressed by an IT Box. These increased quantities may be addressed by a DCR. Increases in quantity which remain within the scope of a previously validated IT Box, may be accomplished without revalidation.

(d) Requirements for DBS capabilities defined and acquired in accordance with references bb and lll.

(4) In cases where the potential for use of the IT-Box construct is unclear or in dispute, the Joint Staff Gatekeeper, in consultation with the validation authority as needed, will determine whether an ICD or IS-ICD will be used.

(5) Sponsors shall use the IS-ICD format when applicable for capability requirement documents with JSDs of JROC Interest and JCB Interest. Sponsors are encouraged to use and validate IS-ICDs for capability requirement documents with JSDs of Joint Integration or Joint Information. In cases where previously validated ICDs are proposed to transition to the IT Box model, the previously validated ICD is amended with IS-ICD content and revalidated to delegate oversight authority.

(6) The "IT Box" model. The IT Box model calls for fewer iterations of validating capability requirement documents through the JCIDS process by describing the overall IS program, and delegating validation of detailed follow-on requirement and solution oversight to a flag-level organization other than the JROC or JCB. CDDs and CPDs are generally not required as successor documents to an IS-ICD, and the delegated oversight authority may prescribe alternative document formats most appropriate to the follow-on efforts.

(a) The IT Box model uses initial minimum values in place of initial objective values so that the baseline capability is clearly specified, and the

delegated oversight body has flexibility to further develop capabilities without revalidation of the capability requirement document.

(b) Successor documents used, whether in regular JCIDS or alternate formats, must be provided to the KM/DS system for information purposes and visibility in the capability requirement portfolios.

(c) An example of Sponsor documents used for managing follow-on efforts is provided later in this section, but is not intended to limit potential flexibilities provided by the IS-ICD.

(7) Revalidation. IS-ICDs require revalidation if the Sponsor proposes:

(a) Adding new capability requirements beyond the scope of the validated IS-ICD.

(b) Increasing programmed development and integration funding beyond the level of funding identified in the IS-ICD.

(c) Disestablishment of the delegated requirements oversight body approved in the validated IS-ICD, or designation of an alternate oversight body.

(d) Changes to MAIS programs proposed in conjunction with the validation of a CDD or IS-CDD do not require revalidation of the IS-ICD.

(8) Biennial FCB Review. For all IS programs with a valid IS-ICD, the lead FCB shall receive an update every second year following the validation. The lead FCB will determine if the JROC or JCB should review the following items, and will make appropriate recommendations for action.

(a) Progress in delivering capability solutions within the required timeframe and available funding.

(b) Compliance with applicable EA and data standards.

(c) Other items identified by the IS-ICD validation.

b. Format Changes

(1) Cover Page. The cover page for an IS-ICD shall be the same as for a regular ICD except that the title will begin with the phrase "Information Systems Initial Capabilities Document for…"

(2) Validation Page. The validation page for an IS-ICD is the same as for a regular ICD.

(3) Executive Summary. The executive summary for an IS-ICD is the same as for a regular ICD.

c. Differences from ICD in document body. The body of an IS-ICD differs from a regular ICD in two sections, and shall be no more than 10 pages long including any content modified or augmented by a classified annex, if used. See the regular ICD section for content of the unchanged sections.

(1) Capability Requirements and Gaps/Overlaps – ICD Section (3). In addition to ICD content for this section, include an NR KPP table with initial minimum value in accordance with Appendix E to this enclosure.

(2) Final Recommendations – ICD Section (5). In addition to ICD content for this section, with the capability requirements making up one side of the IT Box, briefly discuss the remaining sides of the IT Box, illustrated in Figure D-3.

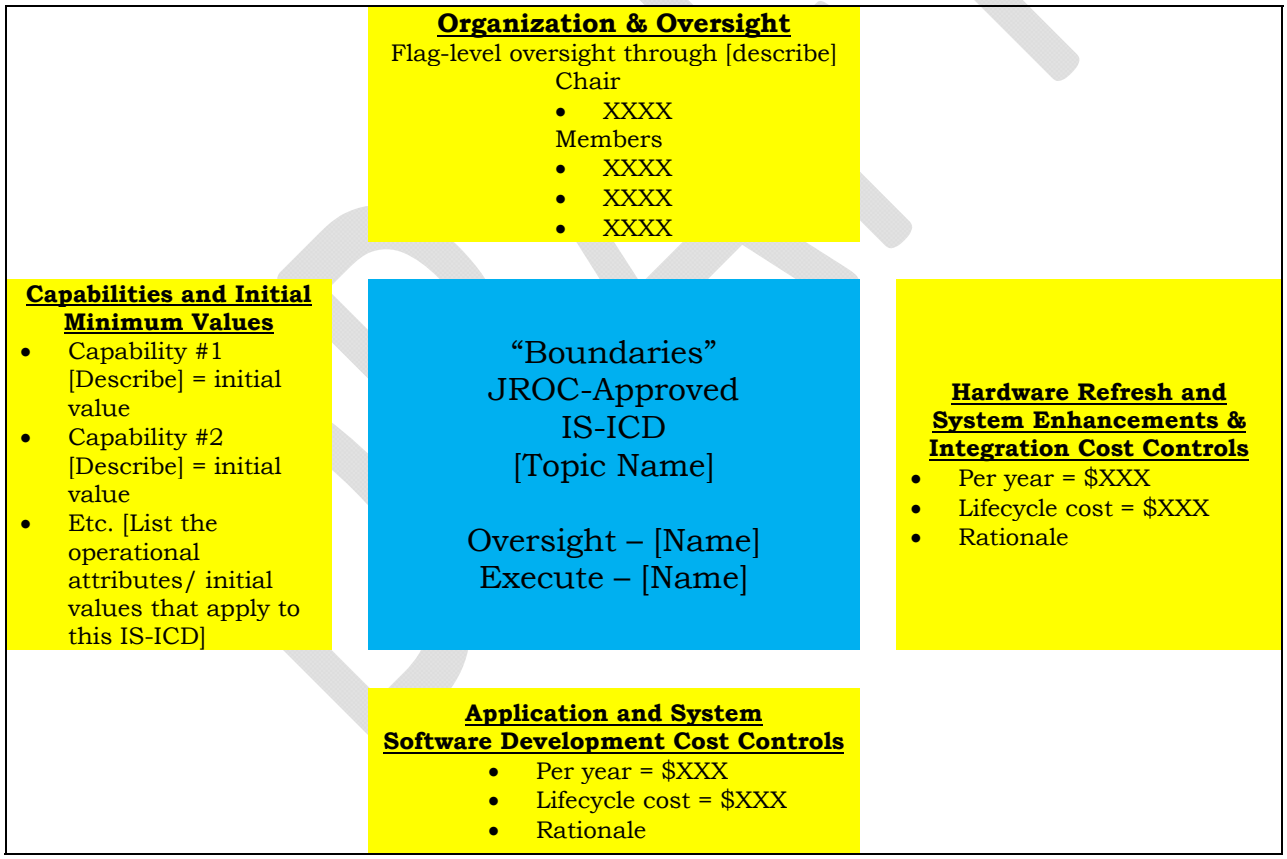

Figure D-3. Components of the "IT Box" model in IS-ICDs

(a) Identify the proposed flag-level oversight body, the chair of that body, and the organizations represented on the body to receive delegated requirements oversight duties, including approval of increases to capabilities above initial minimum values within the bounds of the IT Box.

(b) Show projected life cycle costs for the program. Break out costs into annual estimates of development and integration as well as sustainment costs as shown in Table D-4.

Resources Required (Note 2)									
BY$$ (Note 1)	**FYxx**	**FYxx+1**	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**	**Post-FYDP (FYyy-FYzz)**	**Life Cycle Cost (FYxx-FYzz)**
Application and System Software Development Costs									
Hardware Refresh, System Integration Costs									
Total									
Note 1: All resources normalized to a standard budget year reference – BY$$. **Note 2: Current year is FYxx. First post-FYDP year is FYyy. End of planned capability life, or end of 30-year TOA projection if no planned service life, is FYzz.**									

Table D-4. Example Life Cycle Cost Summary Table for IS-ICDs

d. Appendices. The appendices for an IS-ICD are the same as for a regular ICD.

e. Example of managing an IS requirements using the IT Box construct from an IS-ICD or IS-CDD:

(1) As the IS-ICD and IS-CDD only streamline the applicable requirements processes, the Sponsor must still ensure compliance with acquisition policy and processes in references aa and bb, and Information Support Plan (ISP) policy and processes in accordance with reference cccc.

(2) Since the standard CDD and CPD are not typically required, an IS-ICD or IS-CDD provides Sponsors the flexibility to manage IS requirements with alternate documents and validation processes as necessary, as long as development efforts remain within the boundaries of the validated IT-Box and any additional guidance provided by the validation authority.

(3) The following example of documents used for managing follow-on efforts is intended to be illustrative, and is not intended to limit potential flexibilities provided by the IS-ICD or IS-CDD. Regardless of successor documents used, the Sponsor must satisfy the NR-KPP, when applicable, and any acquisition activities dependent upon content from capability requirement documents.

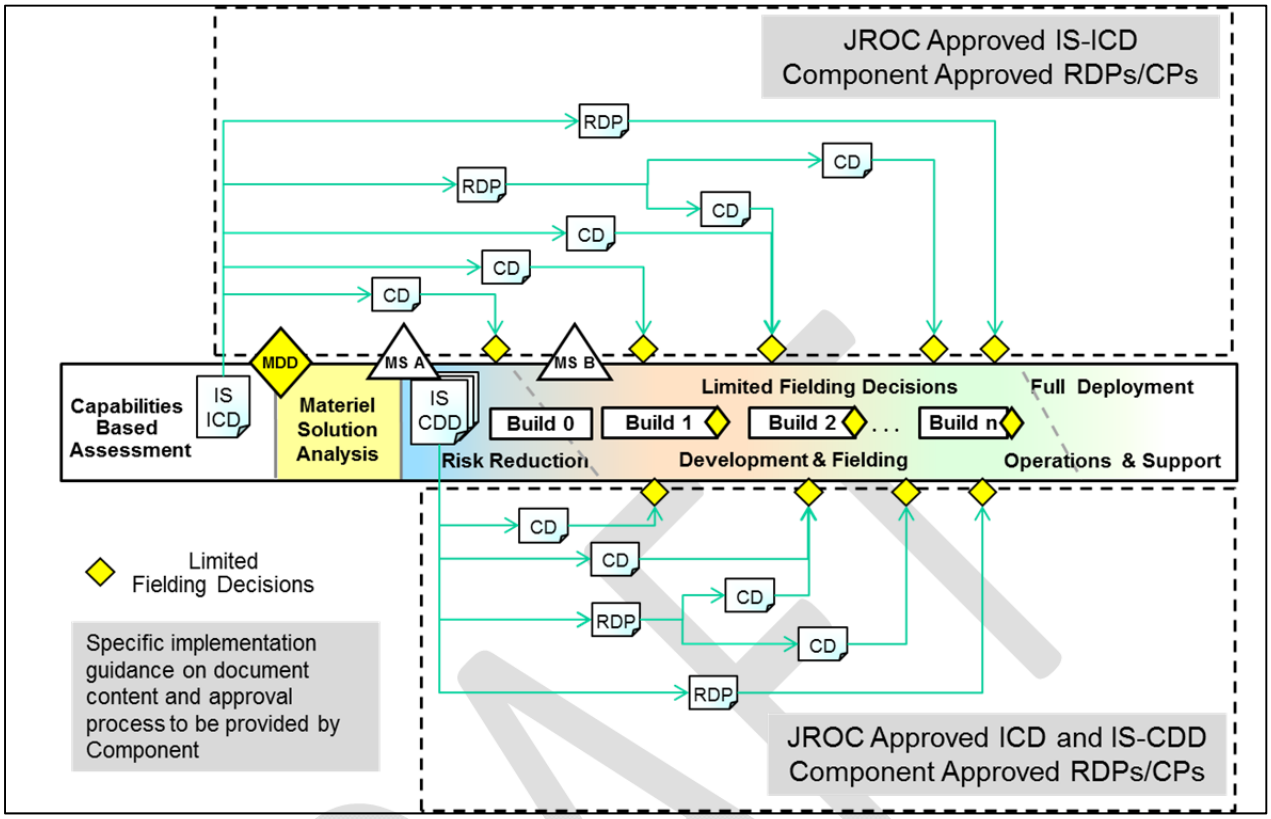

Figure D-4. Example of IS-ICD or IS-CDD Successor Documents

(4) For the purpose of this example, two document types have been created and illustrated in Figure D-4. The Requirements Definition Package (RDP) and the Capability Drop (CD). Actual names, content, and approval process are at the discretion of the delegated oversight authority.

(5) The RDP (or equivalent) is a first level refinement of one or more capability requirements identified in an IS-ICD or IS-CDD, and is co-developed by the operational user (or representative) and the program office. The RDP (or equivalent) identifies the KPPs (including the NR KPP), KSAs, and APAs necessary to scope and cost a specific solution implementation. The RDP (or equivalent) may also identify non-materiel changes that need to be implemented to fully realize the IS capability. The RDP (or equivalent) is approved by the delegated oversight authority identified in the IS-ICD or IS-CDD.

(a) In the case of an IS-ICD, one or more RDPs (or equivalents) could be the equivalent of a CDD in terms of providing greater specificity of a capability solution intended to address part or all of the capability requirements identified in the IS-ICD.

(b) In the case of an IS-CDD, an RDP (or equivalent) may not be necessary if the required level of specificity for the capability solution is already contained in the IS-CDD. However, RDPs (or equivalents) may still be used if needed to decompose the overall capability requirements of the IS-CDD into more manageable parts to facilitate the development efforts.

(c) One or more RDPs (or equivalents) together could represent the total set of capability solutions developed to satisfy the capability requirements in the IS-ICD or IS-CDD.

(d) In support of reference bb, a draft RDP (or equivalent) shall be used before validation to support MS A decisions for IS technology/prototyping efforts. The RDP (or equivalent) shall be submitted to the delegated oversight authority for validation ahead of a MS B decision.

(e) Following validation by the delegated oversight authority, the RDP (or equivalent) would be posted to the KM/DS system for information purposes and for visibility into capability requirement portfolios managed in accordance with Enclosure B of this manual.

(f) The RDP (or equivalent) could then be used in multiple ways. It could be used to initiate an IS program to develop, test, and deliver the full capability defined in the RDP (or equivalent). It could also be used as a basis for defining multiple software builds of incremental capabilities, documented in something like a CD (or equivalent).

(g) If an IS program has a projected life cycle cost such that it is designated an MDAP or MAIS, the capability requirement document must be written as a regular or IS CDD and approved by the JROC to comply with statute.

(6) The CD (or equivalent) could describe the performance characteristics of a relatively small increment of capability included in a software build necessary for partial deployment of the capability solution, typically developed and fielded within a short period of time. It could be developed through a rapid prototyping effort with the user to ensure it meets their needs. A CD (or equivalent) could be developed directly from the definitions in the IS-ICD in the event of a more timely need for the capability. More commonly, multiple CDs (or equivalents) would be derived from an RDP (or equivalent) or IS-CDD to deliver all of the capabilities defined in the RDP (or equivalent) or IS-CDD.

(a) If not already covered by the ISP associated with the RDP (or equivalent) or IS-CDD, the Sponsor must submit an ISP in support of the CD (or equivalent) separately to DOD CIO for certification purposes in accordance with reference cccc.

(b) The approval of CDs (or equivalents) may be delegated to a lower level requirements authority as determined by the delegated oversight authority to ensure timely decision making.

(7) Deployment decisions are made by the MDA whenever the product - whether from an RDP, a CD, or equivalents - is ready for deployment to the user.

DRAFT

4. DCR

a. Background

(1) The purpose of a DCR is to propose non-materiel capability solutions as an alternative to, or complement of, materiel capability solutions. DCRs may also be used to validate capability requirements where service contracting in accordance with reference nnn provides the most appropriate capability solution.

(a) For non-materiel solutions which impact only the Sponsor organization, DCRs are not required by the JCIDS process, as DOD Components manage Component specific DOTmLPF-P at their discretion. Sponsors may use (or not) a DCR in support of non-materiel capability solutions or as enablers of materiel capability solutions in accordance with policies and processes of that organization.

(b) For non-materiel solutions which impact more than just the Sponsor organization, a Joint DCR is used to ensure equities of all effected organizations are addressed during review and validation. By definition, Joint DCRs have impact to the joint force and are assigned a JSD of JROC Interest or JCB Interest in accordance with Enclosure E of this manual.

(c) The DCR serves as the basis for validation by the appropriate validation authority identified in Enclosure F of this manual.

(2) Joint DOTmLPF-P FPOs. FPOs are designated for each of the DOTmLPF-P areas, and provide advice related to their specific functional area to Sponsors of Joint DCRs and affected FCBs during the drafting and review of Joint DCRs. The FPOs are listed in Table D-5.

DOTmLPF-P Area	Functional Process Owner	Associated Guidance/Processes
Joint Doctrine	Joint Staff/J-7	Reference ww
Joint Organizations	Joint Staff/J-8 (with J-1 & J-5 support)	Reference xx
Joint Training	Joint Staff/J-7	Reference yy
Joint Materiel	Joint Staff/J-8	N/A (Coordinate quantity changes with affected Sponsors)
Joint Leadership and Education	Joint Staff/J-7	References zz and aaa
Joint Personnel	Joint Staff/J-1	Reference bbb
Joint Facilities	Joint Staff/J-4	References ccc and ddd
Joint Policy	Joint Staff/J-5	Reference eee

Table D-5. Joint DOTmLPF-P FPOs

b. Format

(1) Cover Page. The cover page of a Joint DCR shall include the following information.

(a) Classification.

(b) Title, starting with the phrase "Joint DOTmLPF-P Change Recommendation for…".

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New Joint DCRs, and modifications to previously validated Joint DCRs, must be endorsed by the Sponsor J8-equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure A of this manual.

(f) Proposed lead organization. Defines a single organization, which may be different from the document Sponsor, which will have responsibility for coordinating the proposed changes, and if applicable, the activities of other Office(s) of Primary Responsibility (OPR) assigned to specific recommendations within the Joint DCR.

(2) Validation Page

(a) While a document is in draft, a placeholder page will be included, with a statement of: "This document (include revision numbering as appropriate) has not yet been validated, and shall not be considered to be an authoritative source for the content herein. This document may be considered authoritative only when this page has been replaced by a signed validation memorandum from the appropriate validation authority."

(b) Once validated by the requirement validation authority, the placeholder page will be replaced by the signed JROCM indicating validation of the document. Any Sponsor approvals prior to JROC validation are not authoritative with respect to the document validation and should not replace the placeholder validation page.

(c) If revisions to a document are proposed after validation, the placeholder page will be reinserted ahead of the original validation memorandum, until the updated validation memorandum is inserted. The

original validation JROCM and JROCMs validating subsequent changes, if applicable, are retained as part of the authoritative document.

(3) Executive Summary. An executive summary, not to exceed one page, shall follow the validation page and precede the body of the Joint DCR. As the sponsor develops the executive summary, they should leverage applicable content from the DODAF AV-1 generated during the CBA to the greatest extent possible.

c. Document body. The body of the Joint DCR shall have the following five sections, and shall be no more than 30 pages long. In cases where a limited amount of content is classified at a higher level than the bulk of the document, a classified annex may be used to facilitate greater access to the document at lower classification levels. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail.

(1) Operational Context

(a) The purpose of this section is to provide context for the recommendations addressed by the Joint DCR. This information facilitates the review and validation of the Joint DCR from the standpoint of how the recommendations address or enable solutions to validated capability requirements and contribute to the missions and activities of the joint force.

1. Narrative in the operational context section should be derived from and consistent with DODAF OVs generated during prior analysis, as modified for the scope and purpose of the Joint DCR, including the DODAF OV-1, OV-3, OV-4, and OV-5a.

2. Other than the DODAF OV-1 which is required in this section, do not include other architecture data and associated artifacts/views in the document unless specifically needed for illustration purposes in the body of the Joint DCR. Provide data for the remainder of the required DODAF OVs in the repository located at the URL specified in the reference section of the document.

(b) If the Joint DCR is a successor document to one or more previously validated capability requirement documents:

1. Cite the validated source documents which identified the capability requirements addressed or enabled by the Joint DCR, and ensure

that any source documents not already present in the KM/DS system are provided to the Joint Staff Gatekeeper for reference purposes.

2. From the source document(s), summarize the operational context(s) associated with the validated capability requirements addressed or enabled by the Joint DCR. Ensure that any changes to operational context(s) which have occurred since validation of the capability requirements are addressed in this section. If any changes to the operational context have been made, ensure the DODAF OVs previously submitted with the ICD are updated and resubmitted to reflect the applicable changes.

3. For Joint DCRs with impact to intelligence equities, ensure any key intelligence support capabilities affected by the changes to DOTmLPF-P are addressed within the operational context.

4. Include the DODAF OV-1 in this section, and where applicable, ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the DODAF OV-1.

(c) If the Joint DCR is not based upon a previously validated capability requirement document, provide the operational context as outlined for Section (1) of an ICD. If applicable, ensure this section includes reference to relevant JROCMs, CCMD IPLs, joint monthly readiness reviews, quarterly reports to the Secretary of Defense, etc., that relate to the change recommendations.

(2) Threat Summary

(a) A threat summary is not applicable to all Joint DCRs, depending upon the nature of the change recommendations. When applicable, the purpose of this section is to provide context for the capability requirements addressed or enabled by the Joint DCR, to provide appropriate traceability to the DIA- or Service-approved threat products used during refinement of the capability requirements, and to describe updates to the threat products since validation of the capability requirements. When applicable, this information also enables threat assessment as part of the intelligence certification provided during Joint DCR review and validation, and facilitates rapid review and update of successor documents when/if applicable threat products are updated.

1. While many Joint DCRs do not require threat assessment or intelligence certification, some may be driven by changes to threat environment, or propose DOTmLPF-P changes which affect intelligence supportability of previously fielded capability solutions. In addition, some Joint DCRs may be specifically focused on intelligence activities or previously

fielded capability solutions. In these cases, an intelligence certification will generally be required.

2. Sponsors should ensure that all intelligence support requirements are identified in terms of the broad descriptions of categories described in Appendix I of this enclosure, and included in the Joint DCR Operational Context, Capability Discussion, and Implementation Plans sections, as appropriate.

(b) If the Joint DCR is a successor document to one or more previously validated capability requirement documents:

1. Cite the latest the DIA- or Service-approved threat products applicable to the capability requirements addressed or enabled by the Joint DCR. Ensure the applicable threat products reflect the most current analysis and findings related to evolving threats.

a. For Joint DCRs enabling or associated with ACAT ID or ACAT IAM programs, ensure the most current DIA-approved threat products are used to develop the Joint DCR and any associated studies or analysis.

b. For all other Joint DCRs where threat products are applicable, ensure the most current DIA- or Service-approved threat products are used to develop the Joint DCR and any associated studies or analysis.

2. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed or enabled by the Joint DCR.

(c) If the Joint DCR is not based upon a previously validated capability requirement document, provide the threat summary as outlined for Section (2) of an ICD.

(3) Capability Discussion

(a) The purpose of this section is to identify the validated capability requirements addressed or enabled by the Joint DCR, and to outline the results of related studies or analysis performed to define the change recommendations.

1. Narrative in the capability requirement and capability gap section should be derived from and consistent with DODAF CVs generated during prior analysis, as modified for the scope and purpose of the ICD, including the DODAF CV-2, CV-3, and CV-6.

2. Data for the required DODAF CVs is to be provided in the repository located at the URL specified in the reference section of the document.

3. If the Joint DCR is a successor document to one or more previously validated capability requirement documents, provide an overview of the validated capability requirements addressed or enabled by the Joint DCR.

4. If the Joint DCR is not based upon a previously validated capability requirement document, provide the capability requirement and associated capability gap information outlined for Section (3) of an ICD.

(b) Summarize all related analyses and/or studies (i.e., AoA or similar studies) conducted to develop the change recommendations. Include the alternatives, objective, criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in the KM/DS system are uploaded for reference purposes.

(c) Ensure any key intelligence support capabilities affected by the changes to DOTmLPF-P are addressed. Ensure the summary of analysis highlights any intelligence-related analyses considered.

(4) Change Recommendations

(a) The purpose of this section is to outline recommendations in one or more DOTmLPF-P areas that provide or enable capability solutions to satisfy validated capability requirements and associated capability gaps. This section also identifies related interdependencies which must be satisfied to provide a successful capability solution.

(b) Use this section to describe change recommendations in terms of each applicable joint DOTmLPF-P area. See Appendix H to this enclosure for more guidance on DOTmLPF-P content.

(c) For each change recommendation to a DOTmLPF-P area, provide the following:

1. Description of the recommended change.

2. Changes to tactics, techniques, and procedures and/or implications on the safe use of the proposed non-materiel solution in the proposed operating environment.

3. Forces and systems affected and impact on interoperability. As appropriate for each recommendation, provide to the repository located at

the URL specified in the reference section of the document, architecture data and associated artifacts/views identified in Table D-1 and, if applicable, Table D-E-3.

4. If a recommendation includes incorporating future technology (materiel component), include a brief discussion of the maturity of critical technology or future systems involved and a risk assessment of the approach.

5. Related support required to implement recommendations, including but not limited to additional research, hardware, DOD manpower, test range time, contractor support, etc.

6. Cite any DOD policies or other issues (treaties, protocols, agreements, legal issues, DOD roles, missions and functions, other US government agency/department, multinational, etc.) that would prevent the effective implementation of the recommended changes and the reason the proposed changes cannot comply with it. Provide proposed changes to the policy or other issue, and identify other potential implications from the proposed mitigation.

7. If impacted by the recommendations in the Joint DCR, update applicable DODAF OVs and CVs to reflect how the capability solutions outlined in the Joint DCR address validated capability requirements and close associated capability gaps in the capability requirement portfolios without introducing unnecessary redundancy in capability or capacity. Data for the required DODAF CVs is to be provided in the repository located at the URL specified in the reference section of the document.

(5) Implementation Plans

(a) The purpose of this section is to outline notional implementation plans for the recommended DOTmLPF-P changes, which will be further refined after validation by the Sponsor or lead organization, task OPR(s), and affected Joint DOTmLPF-P FPO(s).

(b) For each change recommendation to a DOTmLPF-P area, provide the following:

1. Proposed implementation plan, including major milestones and completion dates.

2. Discussion of relationships between recommendations and associated implementation timing (i.e., a joint organizational change has implications for a personnel change, which influences training plans).

3. Ensure that previously fielded or newly introduced key intelligence support capabilities affected by the changes to DOTmLPF-P are identified and adequately addressed in the implementation plan

4. Proposed OPR and rationale. Identify the proposed OPR for each action and provide rationale. Sponsors should attempt to socialize OPR nomination with the affected organizations, but may submit a DCR without formal acceptance of the OPR nomination. The validation memorandum will formalize the assignment of the OPR(s) based upon discussions during the staffing process.

a. If known at the time of staffing, provide specific organizational POC information for each OPR, to include name, organization, office code (if applicable), phone number, and NIPRNET/SIPRNET e-mail addresses. This POC should be the person responsible for implementing the recommended changes within the OPR. For change recommendations with multiple OPRs (e.g., Services, CCMDs), provide organizational POC information for each applicable OPR.

b. If specific POC information for one or more OPRs is not known at the time of staffing, POC information will be determined within 60 days of staffing and provided to the Sponsor of the Joint DCR, the lead FCB, and affected Joint DOTmLPF-P FPOs. If changes to POC information occur, updated information will be provided to the same recipients.

(c) Provide rough-order-of-magnitude total resources required to implement the proposed change as shown in Table D-6, including cost by FY and type of funding required. In cases with funds controlled by different organizations, multiple tables may be used to show changes to funding in each organization.

1. Note that Joint DCRs involve "change recommendations," so cost data should represent only new costs or changes to previously funded efforts. For example, if a recommendation is to change an aspect of joint training, and the change does not require increased resources over that already programmed to cover the total cost of implementing the proposal, including course development, instructor staffing and/or billets, instructor education, training facilities, training materials, hardware, and mock-ups, etc., then do not include those resources in this table.

2. While cost estimation for non-materiel capability solutions are not bound by the same statutes and policy as materiel capability solutions, Sponsors are encouraged to leverage cost estimation approaches outlined in reference bb.

Resource Changes Required to Implement DOTmLPF-P (Note 2)									
BY$$ (Note 1)	**FYxx**	**FYxx+1**	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**	**Post-FYDP (FYyy-FYzz)**	**Life Cycle Cost (FYxx-FYzz)**
RDT&E									
Procurement									
MILCON									
O&M									
MILPERS									
Total									

Note 1: All resources normalized to a standard budget year reference – BY$$.

Note 2: Current year is FYxx. First post-FYDP year is FYyy. End of planned capability life, or end of 30-year TOA projection if no planned service life, is FYzz.

Table D-6. Summary of Resources Required

d. Appendices. Only the following four appendices are allowed in the document. Additional reference documents or data may be submitted in accordance with procedures outlined in Enclosure E of this manual.

(1) Appendix A: References. Ahead of other references provided in this appendix, provide a URL for required architecture data and associated artifacts/views identified in Table D-1 and, if applicable, Table D-E-3.

(2) Appendix B: Acronym List.

(3) Appendix C: Glossary. As the Sponsor develops the document glossary, they should leverage applicable terms from the DODAF AV-2 generated during the CBA to the greatest extent possible. The document glossary and the DODAF AV-2 do not have to be identical, as some terms will only apply to the document or the DODAF architecture. Terms that apply to both must be consistent between the document and the architecture products.

(4) Appendix D: (Optional) Classified Annex. A classified annex may be used in cases where only a small subset of the document needs to be protected at a higher classification level. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail. If used, classified

annexes shall be provided to the Joint Staff Gatekeeper or Joint Staff J-8, Special Access Program Coordinator (J-8/SAPCOORD) in accordance with the classification of the annex.

DRAFT

5. CDD

a. Background

(1) Purpose. The purpose of a CDD is to propose development of a specific materiel capability solution intended to wholly or partially satisfy validated capability requirements and close or mitigate associated capability gaps.

(a) The CDD, and its associated DODAF SVs, provides traceability to predecessor documents and previously validated capability requirements, provides supporting data for certifications and endorsements, identifies related DOTmLPF-P impacts of the proposed capability solution, and outlines projected life cycle costs which will result from pursuing the capability solution.

(b) The CDD provides development KPPs, KSAs, and APAs, to guide the development of one or more increments of a specific system. Each increment described by a CDD must provide a safe, operationally effective, suitable, and useful capability solution in the intended environment, commensurate with the investment.

(c) The document serves as the basis for validation by the appropriate validation authority identified in Enclosure F of this manual.

(2) IS-CDD variant. If a CDD describes a capability solution with a significant IS component, the validation of an IS-CDD may permit alternate document formats and delegated approval authority for flexibility in managing IS capability development under the CDD, without having to revalidate an IS-ICD. To use the IT Box construct in a CDD, see the IS-CDD section of this enclosure. IS programs that are designated as MDAPs must have a validated CDD even if authority to use alternate document formats has been delegated by a preceding IS-ICD.

b. Format

(1) Cover Page. The cover page of a CDD shall include the following information.

(a) Classification.

(b) Title, starting with the phrase “Capability Development Document for…”.

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New CDDs, and

modifications to previously validated CDDs, must be endorsed by the Sponsor J8-equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure A of this manual.

(f) Proposed validation authority.

(g) Proposed MDA.

(h) Proposed JSD. See Enclosure E of this manual for more detail of JSDs.

(i) Proposed ACAT.

(2) Validation Page

(a) While a document is in draft, a placeholder page will be included, with a statement of: "This document (include revision numbering as appropriate) has not yet been validated, and shall not be considered to be an authoritative source for the content herein. This document may be considered authoritative only when this page has been replaced by a signed validation memorandum from the appropriate validation authority."

(b) Once validated by the requirement validation authority, the placeholder page will be replaced by the signed memorandum indicating validation of the document.

1. For documents with JSD of JROC Interest or JCB Interest, the placeholder page will be retained until the signed JROCM is inserted. Any Sponsor approvals prior to JROC or JCB validation are not authoritative with respect to the document validation and should not replace the placeholder validation page.

2. For documents with JSD of Joint Integration or Joint Information, the Sponsor signed memorandum (or equivalent document/form) is authoritative with respect to the document validation.

(c) If revisions to a document are proposed after validation, the placeholder page will be reinserted ahead of the original validation memorandum, until the updated validation memorandum is inserted. The

original validation memorandum and memoranda validating subsequent changes, if applicable, are retained as part of the authoritative document.

(3) Executive Summary. An executive summary, not to exceed one page, shall follow the validation page and precede the body of the CDD. As the sponsor develops the executive summary, they should leverage applicable content from the DODAF AV-1 to the greatest extent possible.

c. Document body. The body of the CDD shall have the following 12 sections, and shall be no more than 45 pages long. In cases where a limited amount of content is classified at a higher level than the bulk of the document, a classified annex may be used to facilitate greater access to the document at lower classification levels. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail.

(1) Operational Context

(a) The purpose of this section is to provide context for the capability requirements addressed by the CDD. This information facilitates review and validation of the CDD from the standpoint of how the capability solutions contribute to the missions and activities of the joint force.

1. Narrative in the operational context section should be derived from and consistent with DODAF OVs generated during prior analysis, as modified for the scope and purpose of the CDD, including the DODAF OV-1, OV-3, OV-4, and OV-5a.

2. Other than the DODAF OV-1 which is required in this section, do not include other architecture data and associated artifacts/views in the document unless specifically referenced for illustration purposes elsewhere in the body of the CDD. Provide data for the remainder of the required DODAF OVs in the repository located at the URL specified in the reference section of the document.

(b) If the CDD is a successor document to one or more previously validated capability requirement documents:

1. Cite the validated source documents which identified the capability requirements addressed by the CDD, and ensure that any source documents not already present in the KM/DS system are provided to the Joint Staff Gatekeeper for reference purposes.

2. From the source document(s), summarize the operational context(s) associated with the validated capability requirements addressed by the CDD. Ensure that any changes to operational context(s) which have occurred since validation of the capability requirements are addressed in this section. If any changes to the operational context have been made, ensure the DODAF OVs previously submitted with the ICD are updated and resubmitted to reflect the applicable changes.

3. Ensure any key intelligence support capabilities required to enable the capability solution's operational activities are addressed and documented within the operational context.

4. Include the DODAF OV-1 in this section, and where applicable, ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the DODAF OV-1.

(c) If the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, approves an ICD waiver and the CDD is not based upon a previously validated capability requirement document, provide the operational context and initial DODAF OVs as outlined for Section (1) of an ICD.

(2) Threat Summary

(a) The purpose of this section is to provide context for the capability requirements addressed by the CDD, to provide appropriate traceability to the DIA- or Service-approved threat products used during refinement of the capability requirements during development, and to describe any updates to the threat products which have occurred since validation of the capability requirements. This information also enables threat assessment as part of the intelligence certification provided during CDD review and validation, and facilitates more rapid review and updating of successor documents when/if threat products are updated.

(b) If the CDD is a successor document to one or more previously validated capability requirement documents:

1. Cite the latest DIA- or Service-approved threat products applicable to the capability requirements addressed by the CDD. Ensure the applicable threat information has been updated since validation of the ICD, considering evolving threats identified in the most current DIA- or Service-approved threat products. Clearly identify threats which were factors in setting the ICD capability requirements and initial objective values.

a. For CDDs associated with ACAT ID programs, ensure the most current DIA-approved threat products are used to develop the CDD and any associated studies or analysis.

b. For all other CDDs, ensure the most current DIA- or Service-approved threat products are used to develop the CDD and any associated studies or analysis.

2. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed by the CDD. Also consider evolving threats to on-going and follow-on research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts.

3. Summarize CIPs identified in the ICD which are applicable to the KPPs, KSAs, or APAs identified in the CDD.

(c) If the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, approves an ICD waiver and the CDD is not based upon a previously validated capability requirement document, provide the threat summary as outlined for Section (2) of an ICD.

(3) Capability Discussion

(a) The purpose of this section is to identify the validated capability requirements and associated capability gaps addressed by the CDD, and to outline the results of related studies or analysis performed since validation of the capability requirements.

1. Narrative in the capability discussion section, especially the discussion of dependencies, should be derived from and consistent with DODAF SV-8 generated during prior analysis, as modified for the scope and purpose of the CDD.

2. If any refinements to capability requirements have been made in the analysis leading up to the CDD, the Sponsor will update previously submitted DODAF CVs to be consistent with the CDD and the DODAF SV-8.

3. Data for the required DODAF SV-8, and modifications to any previously submitted DODAF CVs, is to be provided in the repository located at the URL specified in the reference section of the document.

(b) If the CDD is a successor document to one or more previously validated capability requirement documents:

1. Summarize all related analyses and/or studies conducted to derive the KPPs, KSAs, and APAs presented later in the CDD. Ensure the summary includes any intelligence-related analyses considered. Include the

alternatives, objective, criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in the KM/DS system are uploaded for reference purposes.

2. Provide a table that briefly describes the contribution this CDD makes to the fulfillment of capability requirements and closing of capability gaps described in the applicable ICDs, and the relationships to other CDDs, CPDs, or DCRs that also support these capability requirements, as illustrated in Table D-7. Discuss the relationship of the capability solution described in the CDD to other materiel and non-materiel capability solutions contributing to satisfying the capability requirements. Discuss dependencies on separate DCRs in this section, and discuss any new/additional DOTmLPF-P changes or required synchronization in Section (11).

Capability Requirement	**CDD Contribution**	**Related CDDs**	**Related CPDs**
Capability 1 from ICD 1	Brief Description of the Contribution	CDD Title	CPD Title
Capability 2 from ICD 2	Brief Description of the Contribution	CDD Title	CPD Title
Other validated source document	Brief Description of the Contribution	CDD Title	CPD Title

Table D-7. Supported ICDs and Related CDD/CPDs/DCRs

3. The DODAF SV-8 captures, as a function of time, all external dependencies between the capability solution articulated in the CDD and previously fielded and planned capability solutions, including interactions with intelligence capabilities where appropriate. This provides insight into the evolution of dependencies and enablers over the planned life-cycle of the capability solution.

a. Use the narrative in this section to discuss particularly critical dependencies, and those with known risks or other issues.

b. In SoS capability solutions, the Sponsor is responsible for ensuring that related capability solutions, identified in other CDDs, CPDs, and DCRs, remain compatible and that the development is synchronized. These related capability solutions should tie to a common ICD or set of ICDs. In cases where development of SoS capability solutions involves multiple solution Sponsors, a lead Sponsor should be identified to coordinate efforts across organizations.

c. Address whether the capability solution will be subject to, or affected by, any undeveloped (or underdeveloped) intelligence technologies, or will be affected by the deactivation of previously fielded intelligence programs. Consider whether this will affect the effectiveness and timely

delivery of the capability solution or increment. Ensure all timeframes for any enabling or program-required/dependent intelligence capabilities (previously fielded and future) are consistent with the capability solution's development schedule and planned IOC and FOC.

(c) If the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, approves an ICD waiver and the CDD is not based upon a previously validated capability requirement document, provide the capability requirement and associated capability gap information outlined for Section (3) of an ICD.

(4) Program Summary

(a) The purpose of this section is to outline the overall approach for developing one or more capability solutions to satisfy the validated capability requirements and associated capability gaps, and to identify related interdependencies which must be satisfied to provide a successful capability solution.

(b) Provide a summary of the overall program strategy for reaching full capability and, if applicable, the relationship between increments defined in the CDD. Carefully address the considerations (e.g., technologies to be developed, other systems in the FoS or SoS, inactivation of legacy systems) that are relevant to the incremental delivery plan. For follow-on increments, provide an update on the acquisition status of previous increments, and discuss any updates to the program strategy to reflect lessons learned from previous increments, changes in approved Service and joint concepts, CONOPS, or the DOD IEA and the solution architecture or other pertinent information.

(c) Define what actions, when complete, will constitute attainment of IOC and FOC of the current increment. Specify the target date for IOC and FOC attainment based on discussions and coordination between the requirement Sponsor and the acquisition community. Describe the types and quantities of assets required to attain IOC and FOC.

1. Identify the operational units, including other DOD Components, government agencies, or allied/partner nations if applicable, that will employ the capability solution, and define the quantities required for each organization. This information should leverage and be consistent with the DODAF OV-4 generated during prior analysis, as updated for the scope and purpose of the CDD.

2. Total quantities must include the required operational inventory, as well as quantities required for training, spares, scheduled repair/overhaul pipeline, and anticipated attrition over the life cycle, to maintain the required operational and training inventory. Initial production

planning should be based upon these quantities, and changes to these quantities may trigger a JROC/JCB Tripwire review in accordance with Enclosure B of this manual.

(5) Development KPPs, KSAs, and APAs

(a) The purpose of this section is to outline the development KPPs, KSAs, and APAs intended to satisfy the validated capability requirements and associated capability gaps. Sponsors should avoid over specification of KPPs, KSAs, and APAs, or inclusion of technical specifications as KPPs, KSAs, and APAs, unless essential to addressing a specific capability requirement. In accordance with reference bb, CDD KPPs are inserted verbatim into the performance section of the APB.

(b) Provide tables summarizing development KPPs, KSAs, and APAs in threshold/objective format, as illustrated in Tables D-8 through D-10. If detail associated with each KPP, KSA, and APA cannot be adequately captured within the tables, additional detail may be provided in separate numbered subparagraphs. Note that the tables shown here are examples, and Sponsors may adapt the table formats as needed, provided the required information is clearly understandable to stakeholders.

Tier 1 to 3 JCAs	**Key Performance Parameter**	**Development Threshold**	**Development Objective**
	KPP 1	Value	Value
	KPP 2	Value	Value
	KPP 3	Value	Value

Table D-8. Example KPP Table

Tier 1 to 3 JCAs	**Key System Attribute**	**Development Threshold**	**Development Objective**
	KSA 1	Value	Value
	KSA 2	Value	Value
	KSA 3	Value	Value

Table D-9. Example KSA Table

Tier 1 to 3 JCAs	**Additional Performance Attribute**	**Development Threshold**	**Development Objective**
	APA 1	Value	Value
	APA 2	Value	Value
	APA 3	Value	Value

Table D-10. Example APA Table

1. Correlate each KPP, KSA, and APA to the operational attributes of the capability requirements defined in the ICD, and the Tier 1 through 3 JCAs to which they contribute directly. In accordance with Appendix A of this enclosure, ensure the parameters most critical to mission

effectiveness are captured as KPPs. The narrative in this section should be derived from and consistent with DODAF CV-3, SV-7, and SV-8 generated during prior analysis, as modified for the scope and purpose of the CDD.

a. If the CDD is describing multiple increments, clearly identify which KPPs, KSAs, or APAs apply to each increment, and the development threshold/objective values for each.

b. If degraded levels of performance are acceptable under certain mission environments or conditions, articulate separate development threshold/objective values for the affected KPPs, KSAs, and APAs.

c. If the CDD is describing a SoS solution, it must describe the KPPs, KSAs, and APAs for the SoS level of performance as well as any unique KPPs, KSAs, or APAs for each of the constituent systems.

d. Ensure identification of KPPs, KSAs, and APAs that are dependent upon or enabled by intelligence resources or support, including CIPs which must be tracked by the IC to ensure continuing relevance of the development threshold and development objective values associated with KPPs, KSAs, and APAs. Ensure that intelligence-related KPPs, KSAs, and APAs are supported by adequate information and analysis, and rationale for each is consistent with the analysis and findings of the applicable intelligence ICDs.

2. Present each KPP, KSA, and APA in terms of parameters needed to address the validated capability requirements, consistent with the DODAF CV-3.

a. These parameters should reflect MOP for the system rather than MOE in conducting the mission, as the latter should instead be evaluated against the capability requirements identified in the DODAF CV-3. Ensure parameters chosen are measurable, testable, and support efficient and effective T&E.

b. Provide development threshold values for each which represent the value below which performance would require re-evaluation of military utility in the applicable CONOPS. Provide development objective values in cases where the increased performance level of a parameter provides significant increases in operational utility. If the development objective/threshold values are the same, indicate this by including the statement "threshold = objective."

c. Differences between development threshold/objective values also provide trade space for the Sponsor to explore during the EMD phase of acquisition without having to revalidate the CDD to pursue different levels of performance. The PM may use this information to provide incentives

for the development contractor or to weigh capability tradeoffs between development threshold/objective values.

(c) In addition to KPPs, KSAs, and APAs essential to the capability requirements being addressed by the CDD, Sponsors must address the six mandatory KPPs detailed in Appendix A to this enclosure.

1. For each mandatory KPP, provide specific attributes related to the KPP which must be met rather than a generic statement that the certifications or endorsements for the KPPs will be obtained.

2. Not all mandatory KPPs will be applicable to every capability requirement, so Sponsors may either implement the KPPs or articulate why a particular KPP is not applicable to their operational context.

3. Exclusion of a mandatory KPP is subject to the approval of the certifying or endorsing organization as identified in Enclosure E of this manual. Early coordination with the appropriate certifying or endorsing organization of proposals to exclude a mandatory KPP is essential to avoiding delays during staffing.

(6) Other System Attributes

(a) The purpose of this section is to identify any other system attributes not identified elsewhere in the document, especially those that tend to be design, life cycle cost, or risk drivers. Attributes which are critical to mission success should be identified as KPPs rather than as attributes in this section.

(b) Other system attributes may include, but are not limited to, the following:

1. Embedded instrumentation, electronic attack (EA), and wartime reserve mode (WARM) requirements.

2. Human Systems Integration (HSI) considerations that have a major impact on system effectiveness and suitability.

3. Natural environmental factors, including climatic design type, terrain, meteorological and oceanographic (METOC) factors, impacts and effects.

4. Physical and operational security needs, including technology security, foreign disclosure, defense exportability features, and anti-tamper.

5. Weather, oceanographic and astro-geophysical support needs throughout the program's projected life cycle, including data accuracy and forecast needs.

6. For systems that may be used in allied, partner-nation, coalition, or multinational operations, issues relating to applicable US-ratified international standardization agreements which will be incorporated in the derived system requirements, in accordance with references dddd through gggg.

7. Transportability and deployability considerations, in accordance with reference hhhh, will include how the capability solution and related materiel will be moved either to or within the theater, and identify any lift constraints.

8. Space, Weight, Power, and Cooling (SWaP-C) margin requirements and open system attributes, to ensure future flexibility and upgradability of systems and sub-systems to changing technologies and threats.

(7) Spectrum Requirements

(a) The purpose of this section is to identify electromagnetic (EM) spectrum requirements and to ensure compliance with appropriate policy and guidance. This information also informs the NR KPP review and certification conducted during staffing of the CDD.

(b) All IS must comply with the spectrum management and EM environment effects (E3) direction. The spectrum supportability process includes joint, DOD, national and international policies and procedures for the management and use of the EM spectrum. The spectrum supportability process is detailed in Appendix E to this enclosure, with details on compliance available at reference iiii.

(c) If the capability will interface with, or use, the Joint Worldwide Intelligence Communications System (JWICS) or other intelligence-managed dissemination systems to receive or transmit information, ensure bandwidth requirements and quality of service requirements are addressed. If there are potential issues regarding E3 interference from threat emitters, ensure these issues are identified in this section. Ensure this section is consistent with the threat discussion in paragraph 2 and in the DIA- or Service-approved threat products, including but not limited to the related STAR/System Threat Assessment (STA).

(8) Intelligence Supportability

(a) The purpose of this section is to identify intelligence support requirements and to ensure compliance with appropriate IC policy and guidance. This information also informs the Intelligence review and certification conducted during staffing of the CDD.

(b) Identify, as specifically as possible, all intelligence support requirements throughout the projected life cycle in accordance with Appendix I of this enclosure.

(9) Weapon Safety Assurance

(a) The purpose of this section is to ensure compliance with appropriate weapon safety policy and guidance, and when appropriate, to document specific tailoring of weapon safety requirements driven by unique aspects of the operational context. This information also informs the weapon safety review and endorsement conducted during staffing of the CDD.

(b) In accordance with reference jjjj, all munitions capable of being used, packaged, handled, stored, or transported by any Service in joint warfighting environments are considered to be joint weapons and require a joint weapons safety review and WSE in accordance with Appendix A to Enclosure F of this manual and references jjjj and kkkk. See Appendix J of this enclosure for baseline weapon safety requirements and additional guidance on setting tailored weapon safety requirements if required.

(10) Technology Readiness

(a) The purpose of this section is to highlight known technological challenges which may impact the ability to reach the level of performance identified in the KPPs, KSAs, or APAs, or represent risk to delivering capabilities on schedule and within budget. This information may be used to inform life cycle cost, performance, schedule, and quantity tradeoff discussions during review and validation of the CDD.

1. For the draft CDD generated prior to the MS A acquisition decision, this section identifies specific technological risk areas which should be the focus of risk reduction efforts pursued during the TMRR phase of acquisition.

2. For the CDD generated and validated prior to the MS B acquisition decision, this section identifies any remaining technological risk areas which require particular attention during the EMD phase of acquisition.

(b) This section should be consistent with the Technology Readiness Assessment (TRA), performed in accordance with reference llll prior to Milestone B, if the TRA has been completed in time to inform the CDD. In

cases where a TRA has not been completed in time to inform the CDD, the Sponsor shall ensure that TRA-like analyses are used to develop this section of the CDD.

(c) For each critical technology, discuss potential workaround(s) to achieve partial or complete program success in the event that the technology does not mature as anticipated. In particular, highlight how incremental acquisition strategies and/or modular open architecture approaches are being used to enable flexibility in critical technology areas. Where known, include decision points and criteria for implementing the potential workaround(s).

(11) DOTmLPF-P Considerations

(a) The purpose of this section is to outline DOTmLPF-P changes which are required to successfully implement the materiel capability solution. This information also informs the DOTmLPF-P review and endorsement conducted during staffing of the CDD. See Appendix H to this enclosure for more guidance on DOTmLPF-P content.

(b) Sponsors must address all DOTmLPF-P considerations in a CDD unless not applicable in a particular case. In cases where one or more of the DOTmLPF-P factors may not applicable, the Sponsor shall coordinate with the applicable organization identified in Appendix H to Enclosure F of this manual to ensure that the DOTmLPF-P endorsement is not withheld due to missing information.

(c) Discuss any DOTmLPF-P changes associated with fielding the system, to include those approaches that would impact Service and joint concepts, CONOPS, or plans within a CCMD Area of Responsibility (AOR). Describe the implications for all recommended changes. DOTmLPF-P changes should be considered from two perspectives:

1. Enabling – changes that enable the implementation, operations, and support of the specific system;

2. Integrating – changes that must be made to support integration of this system with previously fielded capability solutions.

(d) Include each of the DOTmLPF-P areas impacted by the capability solution addressed in the CDD. For DOTmLPF-P changes already addressed in separate DCRs, cite the DCR which applies and provide status. For DOTmLPF-P changes not already addressed in separate DCRs, provide details of the recommended changes and implementation plans in the following areas:

1. Doctrine. Identify changes to doctrine which may be required to fully implement the capability solution.

2. Organization. Identify changes to organizational structures which may be required to fully implement the capability solution.

3. Training

a. Specify non-materiel considerations related to training required to fully realize the operational utility of the system. Outline changes or updates to current training practices which enable a new system to replace a legacy system. Training implications must be addressed from the beginning of the acquisition process, integrated with the planning, materiel development, and production, and updated throughout the capability solution's life cycle.

b. In cases where the mission of the system is training, or operational context requires the warfighter to dictate specific materiel training requirements or approaches, the Sponsor should include training KPPs, KSAs, and/or APAs in Section (5) of the CDD.

4. Previously fielded materiel. Include "little-m" changes in quantities to, or new applications of, other materiel capability solutions.

5. Leadership and Education. Identify changes to leadership and education programs which may be required to ensure personnel are capable of fully implementing the capability solution.

6. Personnel. Identify changes to personnel quantities, types (officer, enlisted, civilian, and/or contractor), and skill sets required to fully implement the capability solution.

7. Facilities. Specify facility, shelter, supporting infrastructure, and ESOH asset requirements, and the associated life cycle costs, availability, and acquisition MS schedule(s) related to supporting the system. Detail any basing needs (forward and main operating bases, institutional training base, and depot requirements).

8. Policy. Identify changes to policy which may be required to fully implement the capability solution.

(e) Ensure any intelligence-related DOTmLPF-P considerations, identified through related ISP processes or during analysis done for section 8 of the CDD, are addressed.

(12) Program Affordability

(a) The purpose of this section is to identify the overall resources associated with pursuing the capability solution, including materiel and non-materiel costs over its projected life cycle, and to ensure those resources are planned to be available for successful execution of the program. This information informs life cycle cost, performance, schedule, and quantity tradeoff discussions. Cost estimation used in CDDs shall be consistent with methods outlined in reference bb.

(b) Cite applicable life cycle cost analyses conducted to date, to include other cost models that may include other US government agency/department or exportable-based business cases to reduce DOD life cycle costs. Ensure that resource estimates have been reviewed by the Sponsor's cost analysis organization to ensure best practices are being followed. Also ensure that any final reports or other results documentation, not already present in the KM/DS system, are uploaded for reference purposes.

Acquisition Resources Required (Note 2)									
BY$$ (Note 1)	**FYxx**	**FYxx+1**	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**	**Post-FYDP (FYyy-FYzz)**	**To Complete (FYxx-FYzz)**
RDT&E									
Procurement									
MILCON									
O&M (Acq)									
MILPERS (Acq)									
Total (Acq)									
Acq. Quantity									

Warfighter Resources Required for System Operations and Support (Note 3)					
BY$$ (Note 1)	**Pre-IOC Ops (FYxx-FYaa)**	**IOC to FOC Ops (FYaa-FYbb)**	**Post-FOC Ops (FYbb-FYcc)**	**Operational Life (FYxx-FYcc)**	**Note 1: All resources normalized to a standard budget year reference – BY$$.** **Note 2: Current year is FYxx. First post-FYDP year is FYyy. End of planned production run is FYzz.** **Note 3: Planned IOC is FYaa. Planned FOC is FYbb. Planned end-of-life is FYcc.**
O&M (Ops)					
MILPERS (Ops)					
Total (Ops)					

Table D-11. Summary of Resources Required

(c) Show projected life cycle costs as shown in Table D-11, including cost by FY and type of funding based upon threshold levels of performance. Show cost factors used to determine ACAT level, per reference bb. Present key results from sensitivity and uncertainty analyses, including

the confidence levels associated with resource estimates, based on the program's current level of knowledge. The affordability determination is made as part of the life cycle cost assessment in the analysis supporting the CDD development, which may include updates to earlier cost analyses. Ensure that life cycle cost in the CDD includes all associated DOTmLPF-P and intelligence support considerations.

(d) In a similar manner to what is required by references bb, mmmm, and nnnn, describe how the resources outlined in Table D-11 are affordable under the constraints of the Component's expected TOA over a 30-year timeframe, including identification of legacy capabilities which will be reduced in scope or eliminated to allow funding of the proposed new capability. The 30-year "sand chart" data will be generated using the same OSD inflator values used to comply with affordability in reference bb, and will be provided either within the CDD or as supplemental data uploaded to the KM/DS system.

d. Appendices. Only the following four appendices are allowed in the document. Additional reference documents or data may be submitted in accordance with procedures outlined in Enclosure E of this manual.

(1) Appendix A: References. Ahead of other references provided in this appendix, provide a URL for required architecture data and associated artifacts/views identified in Table D-1 and, if applicable, Table D-E-3.

(2) Appendix B: Acronym List.

(3) Appendix C: Glossary. As the sponsor develops the document glossary, they should leverage applicable terms from the DODAF AV-2 to the greatest extent possible. The document glossary and the DODAF AV-2 do not have to be identical, as some terms will only apply to the document or the DODAF architecture. Terms that apply to both must be consistent between the document and the architecture products.

(4) Appendix D: (Optional) Classified Annex. A classified annex may be used in cases where only a small subset of the document needs to be protected at a higher classification level. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail. If used, classified annexes shall be provided to the Joint Staff Gatekeeper or Joint Staff J-8, Special Access Program Coordinator (J-8/SAPCOORD) in accordance with the classification of the annex.

6. IS-CDD

a. Background

(1) The purpose of an IS-CDD is focused on facilitating more efficient and timely software development efforts, and are not appropriate for hardware development efforts or capturing capability requirements which span a broad scope of combined hardware, software, and/or DOTmLPF-P efforts.

(a) The IS-CDD is a variant of the regular CDD, implementing the "IT Box" model outlined in the IS-ICD section of this enclosure. IS-CDDs streamline the requirements process relative to IS efforts by delegating requirements oversight for subsequent documents as identified in the IS-CDD. This provides IS programs greater flexibility to incorporate evolving technologies and achieve faster responses from requirement validation processes than is typical for other kinds of materiel or non-materiel solutions. In general, the IS-ICD is the preferred method for implementing the "IT Box" model, but:

1. IS-CDDs may be used in cases where a validated ICD contains capability requirements which can be addressed by a combination of IS and non-IS capability solutions and the IT Box construct is applicable to the IS portion of the capability solution(s).

2. IS-CDDs may be used for MDAP and MAIS programs to comply with statutory requirements for a CDD while allowing for other flexibilities of the IT Box model. IS-CDD are also appropriate for use in cases where a validated CDD was generated before the IT-Box construct was introduced, and the Sponsor wants to revalidate under the IT-Box construct.

3. Use of the IT Box model in a CDD does not require that predecessor capability requirement document (ICD, ORD, etc.) also use the IT Box model. I.e. – conversion of a CDD to IS-CDD does not also require conversion of the related ICD to an IS-ICD.

(b) The document serves as the basis for validation by the appropriate validation authority identified in Enclosure F of this manual. Applicability of any potential streamlining of acquisition processes is at the discretion of the MDA in accordance with references aa and bb.

(2) IS-CDDs are appropriate in the same situations where the IS-ICD is appropriate. IS-CDDs are NOT appropriate in the same situations where the IS-ICD is not appropriate. See the IS-ICD format section earlier in this enclosure.

(3) In cases where the potential for use of the IT-Box construct is unclear or in dispute, the Joint Staff Gatekeeper, in consultation with the validation authority as needed, will determine whether a CDD or IS-CDD will be used.

(4) Sponsors shall use the IS-CDD format when applicable for capability requirement documents with JSDs of JROC Interest and JCB Interest. Sponsors are encouraged to use and validate IS-CDDs for capability requirement documents with JSDs of Joint Integration or Joint Information. In cases where previously validated CDDs are proposed to transition to the IT Box model, the previously validated CDD is amended with IS-CDD content and revalidated to delegate oversight authority.

(5) The "IT Box" model. The IT Box model calls for fewer iterations of validating capability requirement documents through the JCIDS process by describing the overall IS program, and delegating validation of detailed follow-on requirement and solution oversight to a flag-level organization other than the JROC or JCB. CPDs are not required as successor documents to an IS-CDD, and the delegated authority may prescribe alternative document formats most appropriate to the follow-on efforts.

(a) For an IS-CDD, KPPs, KSAs, and APAs are used to articulate performance rather than the initial minimum values used in an IS-ICD.

(b) Successor documents used, whether in regular JCIDS or alternate formats, must be provided to the KM/DS system for information purposes and visibility in the capability requirement portfolios.

(c) An example of Sponsor documents used for managing follow-on efforts is provided in the IS-ICD section, but is not intended to limit potential flexibilities provided by the IS-CDD.

(6) Revalidation requirements for IS-CDDs are the same as for the IS-ICD. See the IS-ICD format section earlier in this enclosure.

(7) Biennial FCB review requirements for IS-CDDs are the same as for the IS-ICD. See the IS-ICD format section earlier in this enclosure.

b. Format Changes

(1) Cover Page. The cover page for an IS-CDD shall be the same as for a regular CDD except that the title will begin with the phrase "Information Systems Capability Development Document for…"

(2) Validation Page. The validation page for an IS-CDD is the same as for a regular CDD.

(3) Executive Summary. The executive summary for an IS-CDD is the same as for a regular CDD.

c. Differences from CDD in document body. The body of an IS CDD differs from a regular CDD in three sections, and shall be no more than 45 pages long including any content modified or augmented by a classified annex, if used. See the regular CDD section for content of the unchanged sections.

(1) Program Summary – CDD Section (4). In addition to CDD content for this section, briefly discuss the remaining sides of the IT Box, using KPPs on the left side as illustrated in Figure D-5. Identify the proposed flag-level oversight body, the chair of that body, and the organizations represented on the body being proposed to receive delegated requirements oversight duties.

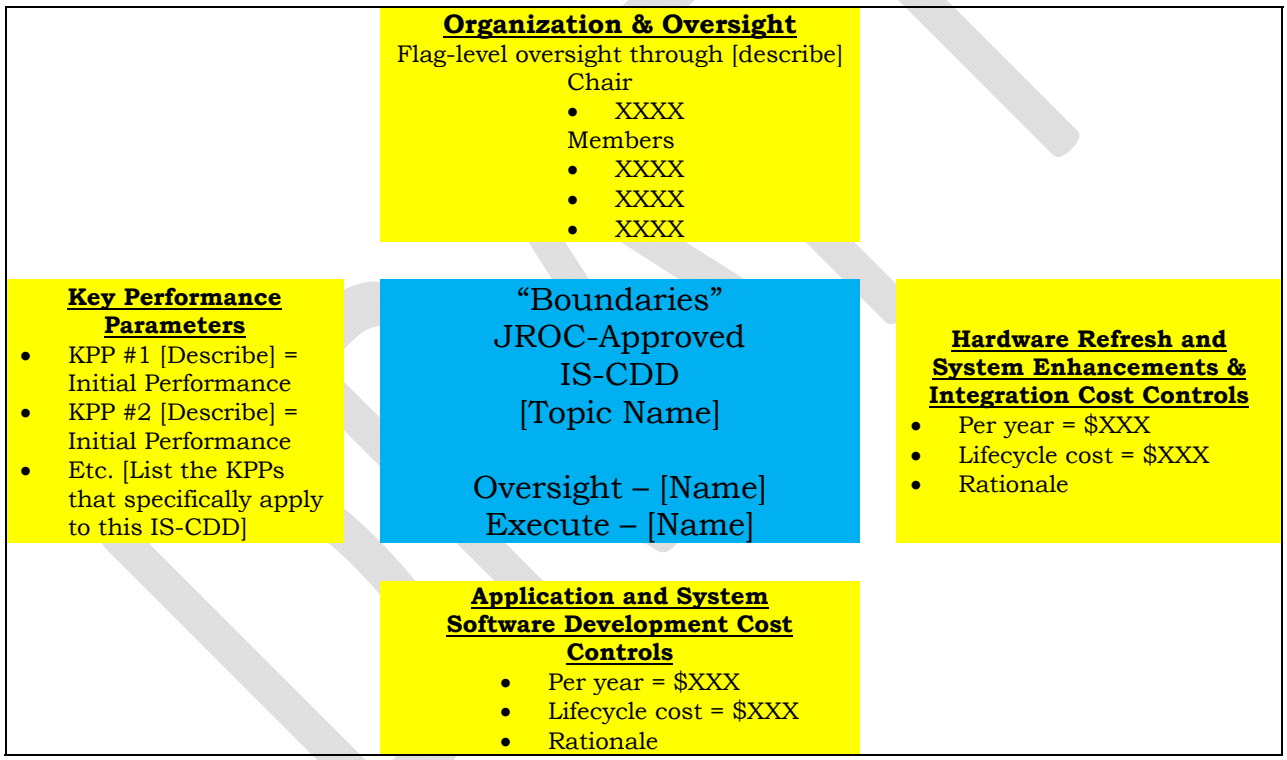

Figure D-5. Components of the "IT Box" model in IS-CDDs

(2) Development KPPs, KSAs, and APAs – CDD Section (5). In addition to CDD content for this section, the KPPs, KSAs, and APAs may be quantified in terms of initial performance values rather than threshold/objective values.

(3) Program Affordability – CDD Section (12). In place of the resources required table used in a CDD, identify the programmed funding by year for the software development and sustainment and for hardware refresh and integration, as shown in Table D-12. Provide rationale for the level of funding required in the same manner as for a CDD.

Resources Required (Note 2)									
BY$$ (Note 1)	**FYxx**	**FYxx+1**	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**	**Post-FYDP (FYyy-FYzz)**	**Life Cycle Cost (FYxx-FYzz)**
Application and System Software Development Costs									
Hardware Refresh, System Integration Costs									
Total									

Note 1: All resources normalized to a standard budget year reference – BY$$.

Note 2: Current year is FYxx. First post-FYDP year is FYyy. End of planned capability life, or end of 30-year TOA projection if no planned service life, is FYzz.

Table D-12. Example Life Cycle Cost Summary Table for IS-CDDs

d. Appendices. The appendices for an IS-CDD are the same as for a regular CDD.

DRAFT

7. CPD

a. Background

(1) The purpose of a CPD is to propose production of an increment of a specific materiel capability solution intended to wholly or partially satisfy validated capability requirements and close or mitigate associated capability gaps.

(a) The CPD, and its associated DODAF SVs, provides traceability to predecessor documents and previously validated capability requirements, provides supporting data for certifications and endorsements, identifies related DOTmLPF-P impacts of the proposed capability solution, and outlines projected life cycle costs which will result from pursuing the capability solution.

(b) The CPD provides production KPPs, KSAs, and APAs, to guide the production and deployment of a single increment of a specific system. Each increment described by a CPD must provide a safe, operationally effective, suitable, and useful capability solution in the intended environment, commensurate with the investment.

(c) The document serves as the basis for validation by the appropriate validation authority identified in Enclosure F of this manual.

(2) Because a CPD is finalized after the CDR and after the majority of capability development, it is normally not appropriate to introduce new capability requirements in a CPD. New capability requirements should be included in the next increment in an evolutionary program or in a CDD for future modification or upgrade if no additional increments are planned.

(3) The most significant difference between the CDD and the CPD is the refinement of production threshold and production objective values for KPPs, KSAs, and APAs previously identified in the CDD or other capability requirement document. Refinements to the KPPs, KSAs, and APAs may drive updates to the SEP and TEMP. Each production threshold listed in the CPD depicts the minimum performance that the system is expected to deliver for an increment's IOC or FOC based on the system design subsequent to the critical design review (CDR).

b. Format

(1) Cover Page. The cover page of a CPD shall include the following information.

(a) Classification.

(b) Title, starting with the phrase "Capability Production Document for…".

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New CPDs, and modifications to previously validated CPDs, must be endorsed by the Sponsor J8-equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure A of this manual.

(f) Proposed validation authority.

(g) Proposed MDA.

(h) Proposed JSD. See Enclosure E of this manual for more detail of JSDs.

(i) Proposed ACAT.

(2) Validation Page

(a) While a document is in draft, a placeholder page will be included, with a statement of: "This document (include revision numbering as appropriate) has not yet been validated, and shall not be considered to be an authoritative source for the content herein. This document may be considered authoritative only when this page has been replaced by a signed validation memorandum from the appropriate validation authority."

(b) Once validated by the requirement validation authority, the placeholder page will be replaced by the signed memorandum indicating validation of the document.

1. For documents with JSD of JROC Interest or JCB Interest, the placeholder page will be retained until the signed JROCM is inserted. Any Sponsor approvals prior to JROC or JCB validation are not authoritative with respect to the document validation and should not replace the placeholder validation page.

2. For documents with JSD of Joint Integration or Joint Information, the Sponsor signed memorandum (or equivalent document/form) is authoritative with respect to the document validation.

(c) If revisions to a document are proposed after validation, the placeholder page will be reinserted ahead of the original validation memorandum, until the updated validation memorandum is inserted. The original validation memorandum and memoranda validating subsequent changes, if applicable, are retained as part of the authoritative document.

(3) Executive Summary. An executive summary, not to exceed one page, shall follow the validation page and precede the body of the CPD. As the sponsor develops the executive summary, they should leverage applicable content from the DODAF AV-1 to the greatest extent possible.

c. Document body. The body of the CPD shall have the following 12 sections, and shall be no more than 40 pages long. In cases where a limited amount of content is classified at a higher level than the bulk of the document, a classified annex may be used to facilitate greater access to the document at lower classification levels. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail.

(1) Operational Context

(a) The purpose of this section is to provide context for the capability requirements addressed by the CPD. This information facilitates review and validation of the CPD from the standpoint of how the capability solutions contribute to the overarching missions and activities of the joint force.

1. Narrative in the operational context section should be derived from and consistent with DODAF OVs generated during prior analysis, as modified for the scope and purpose of the CPD, including the DODAF OV-1, OV-3, OV-4, and OV-5a.

2. Other than the DODAF OV-1 which is required in this section, do not include other architecture data and associated artifacts/views in the document unless specifically referenced for illustration purposes elsewhere in the body of the CPD. Provide data for the remainder of the required DODAF OVs in the repository located at the URL specified in the reference section of the document.

(b) If the CPD is a successor document to one or more previously validated capability requirement documents:

1. Cite the validated source documents which identified the capability requirements addressed by the CPD, and ensure that any source documents not already present in the KM/DS system are provided to the Joint Staff Gatekeeper for reference purposes.

2. From the source document(s), summarize the operational context(s) associated with the validated capability requirements addressed by the CPD. Ensure that any changes to operational context(s) which have occurred since validation of the capability requirements are addressed in this section. If any changes to the operational context have been made, ensure the DODAF OVs previously submitted with the ICD and/or CDD are updated and resubmitted to reflect the applicable changes.

3. Ensure any key intelligence support capabilities required to enable the capability solution's operational activities are addressed and documented within the operational context.

4. Include the DODAF OV-1 in this section, and where applicable, ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the DODAF OV-1.

(c) If the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, approves an ICD and CDD waiver and the CPD is not based upon a previously validated capability requirement document, provide the operational context and initial DODAF OVs as outlined for Section (1) of an ICD.

(2) Threat Summary

(a) The purpose of this section is to provide context for the capability requirements addressed by the CPD, to provide appropriate traceability to the DIA- or Service-approved threat products used during refinement of the capability requirements during development, and to describe any updates to the threat products which have occurred since validation of the capability requirements. This information also enables threat assessment as part of the intelligence certification provided during CPD review and validation, and facilitates more rapid review and updating of successor documents when/if threat products are updated.

(b) If the CPD is a successor document to one or more previously validated capability requirement documents:

1. Cite the latest DIA- or Service-approved threat products applicable to the capability requirements addressed by the CPD. Ensure the applicable threat information has been updated since validation of the CDD, considering evolving threats identified in the most current threat products.

Clearly identify threats which were factors in setting the development KPP, KSA, and APA values in the CDD.

a. For CPDs associated with ACAT ID programs, ensure the most current DIA-approved threat products are used to develop the CPD and any associated studies or analysis.

b. For all other CPDs, ensure the most current DIA- or Service-approved threat products are used to develop the CPD and any associated studies or analysis.

2. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed by the CPD. Also consider evolving threats to on-going and follow-on research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts.

3. Summarize CIPs identified in the ICD and CDD which are applicable to the KPPs, KSAs, or APAs identified in the CPD.

(c) If the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, approves an ICD and CDD waiver and the CPD is not based upon a previously validated capability requirement document, provide the threat summary as outlined for Section (2) of an ICD.

(3) Capability Discussion

(a) The purpose of this section is to identify the validated capability requirements and associated capability gaps addressed by the CPD, and to outline the results of related studies or analysis performed since validation of the capability requirements.

1. Narrative in the capability discussion section, especially the discussion of dependencies, should be derived from and consistent with DODAF SV-8 generated during prior analysis, as modified for the scope and purpose of the CPD.

2. If any refinements to capability requirements have been made in the analysis leading up to the CPD, the Sponsor will update previously submitted DODAF CVs to be consistent with the CPD and the DODAF SV-8.

3. Data for the required DODAF SV-8, and modifications to any previously submitted DODAF CVs, is to be provided in the repository located at the URL specified in the reference section of the document.

(b) If the CPD is a successor document to one or more previously validated capability requirement documents:

1. Summarize all related analyses and/or studies conducted to derive the KPPs, KSAs, and APAs presented later in the CPD. Ensure the summary includes any intelligence-related analyses considered. Include the alternatives, objective, the criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in the KM/DS system are uploaded for reference purposes.

2. Provide a table that briefly describes the contribution this CPD makes to the fulfillment of capability requirements and closing of associated capability gaps described in the applicable ICDs, and the relationships to other CDDs, CPDs, and DCRs that also support these capability requirements, as illustrated in Table D-13. Discuss the relationship of the capability solution described in the CPD to other materiel and non-materiel capability solutions contributing to satisfying the capability requirements. Discuss dependencies on separate DCRs in this section, and discuss any new/additional DOTmLPF-P changes or required synchronization in Section (11).

Capability Requirement	**CPD Contribution**	**Related CDDs**	**Related CPDs**
Capability 1 from ICD 1	Brief Description of the Contribution	CDD Title	CPD Title
Capability 2 from ICD 2	Brief Description of the Contribution	CDD Title	CPD Title
Other validated source document	Brief Description of the Contribution	CDD Title	CPD Title

Table D-13. Supported ICDs and Related CDDs/CPDs/DCRs

3. The DODAF SV-8 captures, as a function of time, all external dependencies between the capability solution articulated in the CPD and previously fielded and planned capability solutions, including interactions with intelligence capabilities where appropriate. This provides insight into the evolution of dependencies and enablers over the planned life-cycle of the capability solution.

a. Use the narrative in this section to discuss particularly critical dependencies, and those with known risks or other issues.

b. In SoS capability solutions, the Sponsor is responsible for ensuring that related capability solutions, specified in other CDDs, CPDs, and DCRs, remain compatible and that the development is synchronized. These related capability solutions should tie to a common ICD, set of ICDs, or approved substitute(s). In cases where development of SoS capability solutions

involves multiple solution Sponsors, a lead Sponsor should be identified to coordinate efforts across organizations.

c. Address whether the capability solution will be subject to, or affected by, any undeveloped (or underdeveloped) intelligence technologies, or will be affected by the deactivation of previously fielded intelligence programs. Consider whether this will affect the effectiveness and timely delivery of the capability solution or increment. Ensure intelligence-related dependencies between these capabilities are defined (e.g., information exchange) and are consistent with the related documents. Ensure all timeframes for any enabling or program-required/dependent intelligence capabilities (previously fielded and future) are consistent with the capability solution's development schedule and planned IOC and FOC.

(c) If the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, approves an ICD and CDD waiver and the CPD is not based upon a previously validated capability requirement document, provide the capability requirement and associated capability gap information outlined for Section (3) of an ICD.

(4) Program Summary

(a) The purpose of this section is to outline the overall approach for producing and fielding one or more capability solutions to satisfy the validated capability requirements and associated capability gaps, and to identify related interdependencies which must be satisfied to provide a successful capability solution.

(b) Provide a summary of the overall program strategy for reaching full capability and, if applicable, the relationship between the production increment addressed by this CPD and any other increments of the program. Carefully address the considerations (e.g., technologies to be developed, other systems in the FoS or SoS, inactivation of legacy systems) that are relevant to the incremental delivery plan. For follow-on increments, provide an update on the acquisition status of previous increments, and discuss any updates to the program strategy to reflect lessons learned from previous increments, changes in approved Service and joint concepts, CONOPS, or the DOD IEA and the solution architecture or other pertinent information.

(c) Define what actions, when complete, will constitute attainment of IOC and FOC of the current increment. Specify the target date for IOC and FOC attainment based on discussions and coordination between the requirement Sponsor and the acquisition community. Describe the types and quantities of assets required to attain IOC and FOC.

1. Identify the operational units, including other DOD Components, government agencies, or allied/partner nations if applicable, that will employ the capability solution, and define the quantities required for each organization. This information should leverage and be consistent with the DODAF OV-4 generated during prior analysis, as updated for the scope and purpose of the CPD.

2. Total quantities must include the required operational inventory, as well as quantities required for training, spares, scheduled repair/overhaul pipeline, and anticipated attrition over the projected life cycle, to maintain the required operational and training inventory. Initial production planning should be based upon these quantities, and changes to these quantities may trigger a JROC/JCB Tripwire review in accordance with Enclosure B of this manual.

(5) Production KPPs, KSAs, and APAs

(a) The purpose of this section is to outline the production KPPs, KSAs, and APAs intended to satisfy the validated capability requirements and associated capability gaps. Sponsors should avoid over specification of KPPs, KSAs, or APAs, or inclusion of technical specifications as KPPs, KSAs, or APAs, unless essential to addressing a specific capability requirement. In accordance with reference bb, CPD KPPs are inserted verbatim into the performance section of the APB.

(b) Provide tables summarizing production KPPs, KSAs, and APAs in threshold/objective format, as illustrated in Tables D-14 through D-16. If detail associated with each KPP, KSA, and APA cannot be adequately captured within the tables, detail may be provided in separate numbered subparagraphs. Note that the tables shown here are examples, and Sponsors may adapt the table formats as needed, provided the required information is clearly understandable to stakeholders.

Tier 1 to 3 JCAs	**Key Performance Parameter**	**Production Threshold**	**Production Objective**
	KPP 1	Value	Value
	KPP 2	Value	Value
	KPP 3	Value	Value

Table D-14. Example KPP Table

Tier 1 to 3 JCAs	**Key System Attributes**	**Production Threshold**	**Production Objective**
	KSA 1	Value	Value
	KSA 2	Value	Value
	KSA 3	Value	Value

Table D-15. Example KSA Table

Tier 1 to 3 JCAs	Additional Performance Attribute	Production Threshold	Production Objective
	APA 1	Value	Value
	APA 2	Value	Value
	APA 3	Value	Value

Table D-16. Example APA Table

1. Correlate each KPP, KSA, and APA to the operational attributes of the capability requirements defined in the ICD and/or CDD, and the Tier 1 through 3 JCAs to which they contribute directly. In accordance with Appendix A of this enclosure, ensure the parameters most critical to mission effectiveness are captured as KPPs. The narrative in this section should be derived from and consistent with DODAF CV-3, SV-7, and SV-8 generated during prior analysis, as modified for the scope and purpose of the CPD. Changes to KPP values or added KPPs from the predecessor capability requirement documents must include analysis, including resultant cost and schedule impacts, justifying the changed/added performance parameters or values.

a. If degraded levels of performance are acceptable under certain mission environments or conditions, articulate separate production threshold/objective values for the affected KPPs, KSAs, and APAs.

b. If the CPD is part of a SoS solution, it must describe the KPPs, KSAs, and APAs for the SoS level of performance as well as any unique KPPs, KSAs, and APAs for the constituent system described in the CPD.

c. Ensure identification of KPPs, KSAs, and APAs that are dependent upon or enabled by intelligence resources or support, including CIPs which must be tracked by the IC to ensure continuing relevance of the production threshold and production objective values associated with KPPs, KSAs, and APAs. Ensure that intelligence-related KPPs, KSAs, and APAs are supported by adequate information and analysis, and rationale for each is consistent with the analysis and findings of the applicable intelligence ICDs.

2. Present each KPP, KSA, and APA in terms of parameters needed to address the validated capability requirements, consistent with the DODAF CV-3.

a. These parameters should reflect MOP for the system rather than MOE in conducting the mission, as the latter should instead be evaluated against the capability requirements identified in the DODAF CV-3. Ensure parameters chosen are measurable, testable, and support efficient and effective T&E.

a. Provide production threshold values for each which represent the value below which performance would require re-evaluation of military utility in the applicable CONOPS. Provide production objective values in cases where the increased performance level of a parameter provides significant increases in operational utility. If the production threshold/objective values are the same, indicate this by including the statement "threshold = objective."

c. Differences between production threshold/objective values also provide trade space for the Sponsor to accommodate changes during production or after fielding without having to revalidate the CPD to pursue different levels of performance. The PM may use this information to provide incentives for the production contractor to enhance performance through production improvements or to weigh capability tradeoffs between production threshold/objective values.

(c) In addition to KPPs, KSAs, and APAs essential to the capability requirements being addressed by the CPD, Sponsors must address the six mandatory KPPs detailed in Appendix A to this enclosure.

1. For each mandatory KPP, provide specific attributes related to the KPP which must be met rather than a generic statement that the certifications or endorsements for the KPPs will be obtained.

2. Not all mandatory KPPs will be applicable to every capability requirement, so Sponsors may either implement the KPPs or articulate why a particular KPP is not applicable to their operational context.

3. Exclusion of a mandatory KPP is subject to the approval of the certifying or endorsing organization as identified in Enclosure E of this manual. Early coordination with the appropriate certifying or endorsing organization of proposals to exclude a mandatory KPP is essential to avoiding delays during staffing.

(6) Other System Attributes

(a) The purpose of this section is to identify any other system attributes not identified elsewhere in the document, especially those that tend to be design, life cycle cost, or risk drivers. Attributes which are critical to mission success should be identified as KPPs rather than as attributes in this section.

(b) Other system attributes may include, but are not limited to, the following:

1. Embedded instrumentation, EA, and WARM requirements.

2. HSI considerations that have a major impact on system effectiveness, suitability, and affordability.

3. Natural environmental factors, including climatic design type, terrain, METOC factors, and impacts and effects.

4. Physical and operational security needs, including technology security, foreign disclosure, defense exportability features, and anti-tamper.

5. Weather, oceanographic and astro-geophysical support needs throughout the program's projected life cycle, including data accuracy and forecast needs.

6. For systems that may be used in combined allied and coalition operations, issues relating to the potentially applicable US-ratified international standardization agreements. Provide an initial indication of which ones will be incorporated in the derived system requirements, in accordance with references dddd through gggg.

7. Transportability and deployability considerations, in accordance with reference hhhh, will include how the capability solution and related materiel will be moved either to or within the theater, and identify any lift constraints.

8. SWaP-C margin requirements and open system attributes, to ensure future flexibility and upgradability of systems and sub-systems to changing technologies and threats.

(7) Spectrum Requirements

(a) The purpose of this section is to identify EM spectrum requirements and to ensure compliance with appropriate policy and guidance. This information also informs the NR KPP review and certification conducted during staffing of the CPD.

(b) All IS must comply with the spectrum management and E3 direction. The spectrum supportability process includes joint, DOD, national and international policies and procedures for the management and use of the EM spectrum. The spectrum supportability process is detailed in Appendix E of this enclosure, with details on compliance available at reference iiii.

(c) If the capability will interface with, or use, the JWICS or other intelligence-managed dissemination systems to receive or transmit information, ensure bandwidth requirements and quality of service requirements are addressed. If there are potential issues regarding E3 interference from threat

emitters, ensure these issues are identified in this section. Ensure this section is consistent with the threat discussion in paragraph 2 and in the DIA- or Service-approved threat products, including but not limited to the related STAR/STA.

(8) Intelligence Supportability

(a) The purpose of this section is to identify intelligence support requirements and to ensure compliance with appropriate IC policy and guidance. This information also informs the Intelligence review and certification conducted during staffing of the CPD.

(b) Identify, as specifically as possible, all intelligence support requirements throughout the projected life cycle in accordance with Appendix I of this enclosure.

(9) Weapon Safety Assurance

(a) The purpose of this section is to ensure compliance with appropriate weapon safety policy and guidance, and when appropriate, to document specific tailoring of weapon safety requirements driven by unique aspects of the operational context. This information also informs the weapon safety review and endorsement conducted during staffing of the CPD.

(b) In accordance with reference jjjj, all munitions capable of being used, packaged, handled, stored, or transported by any Service in joint warfighting environments are considered to be joint weapons and require a joint weapons safety review and WSE in accordance with Appendix A to Enclosure F of this manual and references jjjj and kkkk. See Appendix J of this enclosure for baseline weapon safety requirements and additional guidance on setting tailored weapon safety requirements if required.

(10) Manufacturing Readiness

(a) The purpose of this section is to highlight known manufacturing challenges which may impact the ability to produce the capability solution as designed to reach the level of performance identified in the KPPs, KSAs, or APAs, or represent risk to delivering capabilities on schedule and within budget. This information may be used to inform life cycle cost, performance, schedule, and quantity tradeoff discussions during review and validation of the CPD.

(b) This section should be consistent with the Manufacturing Readiness Assessment (MRA), performed in accordance with references bb and oooo prior to Milestone C, if the MRA has been completed in time to inform the CPD. In cases where a MRA has not been completed in time to inform the

CPD, the Sponsor shall ensure that MRA-like analyses are used to develop this section of the CPD.

(c) For each critical manufacturing challenge, discuss potential workaround(s) to achieve partial or complete program success in the event that manufacturing challenges persist in the critical areas. Where known, include decision points and criteria for implementing the potential workaround(s).

(11) DOTmLPF-P Considerations

(a) The purpose of this section is to outline DOTmLPF-P changes which are required to successfully implement the materiel capability solution. This information also informs the DOTmLPF-P review and endorsement conducted during staffing of the CPD. See Appendix H to this enclosure for more guidance on DOTmLPF-P content.

(b) Sponsors must address all DOTmLPF-P considerations in a CPD unless not applicable in a particular case. In cases where one or more of the DOTmLPF-P factors may not applicable, the Sponsor shall coordinate with the applicable organization identified in Appendix H to Enclosure F of this manual to ensure that the DOTmLPF-P endorsement is not withheld due to missing information.

(c) Discuss any DOTmLPF-P changes associated with fielding the system, to include those approaches that would impact Service and joint concepts, CONOPS, or plans within a CCMD AOR. Describe the implications for all recommended changes. DOTmLPF-P changes should be considered from two perspectives:

1. Enabling – changes that enable the implementation, operations and support of the specific system;

2. Integrating – changes that must be made to support integration of this system with previously fielded capability solutions.

(d) Include each of the DOTmLPF-P areas if impacted by the capability solution addressed in the CPD. For DOTmLPF-P changes already addressed in separate DCRs, cite the DCR which applies and provide status. For DOTmLPF-P changes not already addressed in separate DCRs, provide details of the recommended changes and implementation plans in the following areas:

1. Doctrine. Identify changes to doctrine which may be required to fully implement the capability solution.

2. Organization. Identify changes to organizational structures which may be required to fully implement the capability solution.

3. Training

a. Specify non-materiel considerations related to training required to fully realize the operational utility of the system. Outline changes or updates to current training practices which enable a new system to replace a legacy system. Training implications must be addressed from the beginning of the acquisition process, integrated with the planning, materiel development, and production, and updated throughout the capability solution's life cycle.

b. In cases where the mission of the system is training, or operational context requires the warfighter to dictate specific materiel training requirements or approaches, the Sponsor should include training KPPs, KSAs, and/or APAs in Section (5) of the CPD.

4. Previously fielded materiel. Include "little-m" changes in quantities to, or new applications of, other materiel capability solutions.

5. Leadership and Education. Identify changes to leadership and education programs which may be required to ensure personnel are capable of fully implementing the capability solution.

6. Personnel. Identify changes to personnel quantities, types (officer, enlisted, civilian, and/or contractor), and skill sets required to fully implement the capability solution.

7. Facilities. Specify facility, shelter, supporting infrastructure, and ESOH asset requirements, and the associated life cycle costs, availability, and acquisition MS schedule(s) related to supporting the system. Detail any basing needs (forward and main operating bases, institutional training base, and depot requirements).

8. Policy. Identify changes to policy which may be required to fully implement the capability solution.

(e) Ensure any intelligence-related DOTmLPF-P considerations, identified through related ISP processes or during analysis done for section 8 of the CPD, are addressed.

(12) Program Affordability

(a) The purpose of this section is to update the overall resources associated with pursuing the capability solution, including materiel and non-materiel costs over its projected life cycle, and to ensure those resources are

planned to be available for successful execution of the program. This information informs life cycle cost, performance, schedule, and quantity tradeoff discussions. Cost estimation used in CPDs shall be consistent with methods outlined in reference bb.

1. Program affordability in a CPD represents an update to resources identified in the CDD, based upon knowledge gained during earlier acquisition activities as well as fact of life changes to priorities and projected budgets since the validation of the CDD.

2. For programs proceeding directly to a CPD without an associated CDD, this section provides the initial identification of overall resources associated with pursuing the capability solution.

(b) Cite applicable life cycle cost analyses conducted to date, to include other cost models that may include other US government agency/department or exportable-based business cases to reduce DOD life cycle costs. Ensure that resource estimates have been reviewed by the Sponsor's cost analysis organization to ensure best practices are being followed. Also ensure that any final reports or other results documentation, not already present in the KM/DS system, are uploaded for reference purposes.

(c) Show projected life cycle costs as shown in Table D-17, including cost by FY and type of funding based upon threshold levels of performance. Show cost factors used to determine ACAT level, per reference bb. Present key results from sensitivity and uncertainty analyses, including the confidence levels associated with resource estimates, based on the program's current level of knowledge. The affordability determination is made as part of the life cycle cost assessment in the analysis supporting the CPD development, which may include updates to earlier cost analyses. Ensure that life cycle cost in the CPD includes all associated DOTmLPF-P and intelligence support considerations.

(d) In a similar manner to what is required by references bb, mmmm, and nnnn, describe how the resources outlined in Table D-17 are affordable under the constraints of the Component's expected TOA over a 30-year timeframe, including identification of legacy capabilities which will be reduced in scope or eliminated to allow funding of the proposed new capability. The 30-year "sand chart" data will be generated using the same OSD inflator values used to comply with affordability in reference bb, and will be provided either within the CPD or as supplemental data uploaded to the KM/DS system.

Acquisition Resources Required (Note 2)									
BY$$ (Note 1)	**FYxx**	**FYxx+1**	**FYxx+2**	**FYxx+3**	**FYxx+4**	**FYxx+5**	**FYDP Total**	**Post-FYDP (FYyy-FYzz)**	**To Complete (FYxx-FYzz)**
RDT&E									
Procurement									
MILCON									
O&M (Acq)									
MILPERS (Acq)									
Total (Acq)									
Acq. Quantity									

Warfighter Resources Required for System Operations and Support (Note 3)					
BY$$ (Note 1)	**Pre-IOC Ops (FYxx-FYaa)**	**IOC to FOC Ops (FYaa-FYbb)**	**Post-FOC Ops (FYbb-FYcc)**	**Operational Life (FYxx-FYcc)**	**Note 1: All resources normalized to a standard budget year reference – BY$$.** **Note 2: Current year is FYxx. First post-FYDP year is FYyy. End of planned production run is FYzz.** **Note 3: Planned IOC is FYaa. Planned FOC is FYbb. Planned end-of-life is FYcc.**
O&M (Ops)					
MILPERS (Ops)					
Total (Ops)					

Table D-17. Summary of Resources Required

d. Appendices. Only the following four appendices are allowed in the document. Additional reference documents or data may be submitted in accordance with procedures outlined in Enclosure E of this manual.

(1) Appendix A: References. Ahead of other references provided in this appendix, provide a URL for required architecture data and associated artifacts/views identified in Table D-1 and, if applicable, Table D-E-3.

(2) Appendix B: Acronym List.

(3) Appendix C: Glossary. As the sponsor develops the document glossary, they should leverage applicable terms from the DODAF AV-2 to the greatest extent possible. The document glossary and the DODAF AV-2 do not have to be identical, as some terms will only apply to the document or the DODAF architecture. Terms that apply to both must be consistent between the document and the architecture products.

(4) Appendix D: (Optional) Classified Annex. A classified annex may be used in cases where only a small subset of the document needs to be protected

at a higher classification level. When a classified annex is used, its content will count toward the document body page limits and will be indexed to align with the baseline document sections. Except where existence of the classified content cannot be acknowledged at the lower classification level, each section of the baseline document modified or augmented by the classified annex will refer the reader to the classified annex for additional detail. If used, classified annexes shall be provided to the Joint Staff Gatekeeper or Joint Staff J-8, Special Access Program Coordinator (J-8/SAPCOORD) in accordance with the classification of the annex.

DRAFT

8. JUON, JEON, and DOD Component UON

a. Background

(1) The purpose of JUONs, JEONs, and DOD Component UONs is to facilitate rapid identification, prioritization, validation, documentation, and communication of urgent or emergent capability requirements and associated capability gaps which represent significant risk to mission success or safety of forces. These capability requirements and associated capability gaps may be associated with an ongoing contingency operation, or may represent such a significant risk to future missions that urgent out-of-cycle requirements, resourcing, and acquisition actions are justified. These documents serve as the basis for expedited validation by the appropriate validation authority identified in Enclosure G of this manual. Warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed in accordance with reference gg.

(a) DOD Component UONs are applicable to only one DOD Component and are driven by ongoing or anticipated contingency operations. DOD Component UONs are submitted, staffed, and validated in accordance with references hh through oo. After validation, DOD Component UONs are uploaded to the KM/DS system for information and visibility in the capability requirement portfolios.

(b) JUONs are UONs affecting two or more DOD Components and are driven by ongoing contingency operations. JUONs are submitted by CCMDs or the CJCS/VCJCS in accordance with this enclosure, and reviewed and validated in accordance with Enclosure G.

(c) JEONs are UONs affecting two or more DOD Components and are driven by anticipated contingency operations. JEONs are submitted by CCMDs or CJCS/VCJCS in accordance with this enclosure, and reviewed and validated in accordance with Enclosure G.

(d) While JUONs and JEONs are primarily submitted by the CCMDs, the CJCS/VCJCS may generate a JUON or JEON directly in support of CJCS or VCJCS responsibilities, or to facilitate timely validation of urgent or emergent needs identified by multiple CCMDs or DOD Components.

(e) DOD Components not covered by references hh through oo, may submit urgent and emergent capability requirements as JUONs or JEONs for validation through the processes in this manual, or may coordinate with the cognizant organizations for potential use of the processes in references hh through oo.

(2) JUONs, JEONs, and DOD Component UONs are used ONLY when the deliberate requirement validation and deliberate acquisition processes, or other means such as the GFM process, JMVP, etc., are not practical for satisfying the capability requirement in the operational timelines.

(3) Capability requirements associated with ongoing or anticipated contingency operation and intended to prevent loss of life or critical mission failure that do not require out-of-cycle funding to initiate program execution, should not use a JUON, JEON, or DOD Component UON to document and validate the capability requirement and associated capability gaps, but rather generate an ICD, CDD, or CPD for review and validation in the deliberate staffing process. In these cases, the Sponsor may request expedited timeliness from the validation authority and/or the MDA through tailoring of the deliberate processes.

(4) Capability solutions for JUONs, JEONs, and DOD Component UONs do not require associated ICDs, CDDs, or CPDs for initial fielding, but may require appropriate CDDs or CPDs to support validation of enduring capability requirements and transition for sustainment and/or further development of capability solutions for enduring use. See Enclosure B of this manual for transition of JUONs and JEONs to enduring capability requirements. See references hh through oo for transition of DOD Component UONs to enduring capability requirements.

b. Format. JUON and JEON format is addressed in this section. See references hh through oo for format of DOD Component UONs.

(1) Cover Page. JUONs and JEONs do not require a cover page.

(2) Validation Page. JUONs and JEONs do not require a validation page.

(3) Executive Summary. JUONs and JEONs do not require an executive summary.

c. Document body. JUONs and JEONs will be in memo format and generally not to exceed three pages.

(1) Administrative Data

(a) Title: (Unclassified version)

(b) Submitted by: (e.g., CENTCOM)

(c) Authorized by: Release authority's name, rank and title. New JUONs and JEONs, and modifications to the capability requirements in

previously validated JUONs and JEONs, must be endorsed by the CCMD Commander, Deputy Commander, or Chief of Staff. Administrative modifications to previously validated JUONs or JEONs may be endorsed by the CCMD J8.

(d) Primary and secondary POCs for the document Sponsor: Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure A of this manual.

(e) Date submitted by the CCMD.

(2) Operational Context and Threat Analysis. What is the target, threat, or operational deficiency? What cannot be done without a new or improved capability solution? Identify where the operational deficiency exists, describing the mission deficiency or capability gap. Describe in detail the nature of the urgency and the operational impact, if not immediately resolved, in terms of critical mission failure or loss of life. Provide a CONOPS for which the capabilities requested in the JUON or JEON contribute, including information regarding the coalition environment within which the capability solution will need to operate.

(3) Required Capability. Describe what capabilities are required, as opposed to specific capability solutions which will be addressed later, and whether they support a discrete operation, must be sustained for an extended period of time, or must be sustained until the end of the conflict. The capability requirements must be specifically articulated in light of the operational context, and cannot involve broad/unquantified requests. Include threshold/objective performance requirements for any key attributes. This description must also specify the latest acceptable date to address the capability requirements and associated capability gaps.

(4) Flexibility. In the event of technological or other challenges, indicate whether receiving a partial capability solution on schedule is preferred to a delayed capability solution which satisfies a greater portion of the capability requirement. Estimate acceptable percentages of reduced performance and/or acceptable delay timeframes.

(5) Potential Non-Materiel Capability Solutions. Describe any non-materiel options and alternatives that were considered or which provide partial mitigation of the capability requirement.

(6) Potential Materiel Capability Solutions. If known, identify and discuss viable capability solutions – including those from other DOD Component, other US government agency/department, or allied/partner nation sources in addition to commercial sources – that could improve operational

capabilities or system performance. Discuss any impacts to safety, survivability, personnel, training, logistics, communications, etc. If applicable, discuss any market survey or similar related information developed by the document Sponsor or during the validation process. If market research details are available, provide along with the JUON or JEON to facilitate reuse during rapid acquisition activities.

(7) Required Quantities. For materiel capability solutions, identify quantities required and distribution among applicable DOD Components.

(a) Total quantities must include both the required operational inventory, as well as quantities required for training, spares, scheduled repair/overhaul pipeline, and anticipated attrition over the projected life cycle, so that the required operational inventory is maintained.

(b) Changes to quantities intended solely to accommodate unexpected attrition, or expenditure in the case of munitions, and maintain the required operational inventory, do not require re-validation of the capability requirements.

(c) Changes to production quantities, or absence of changes to production quantities when consumption or attrition rates change from original planning which result in changes to the operational inventory, will require revalidation of required operational inventory quantities and/or acceptance of the altered operational risk.

(8) Constraints. Identify any known constraints that could inhibit satisfying the need -- such as arms control treaties, logistics support, transportation, manpower, training or non-military barriers.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX A TO ENCLOSURE D

DEVELOPMENT OF KEY PERFORMANCE PARAMETERS, KEY SYSTEM ATTRIBUTES, AND ADDITIONAL PERFORMANCE ATTRIBUTES

1. Overview

a. KPPs. Performance attributes of a system considered critical or essential to the development of an effective military capability. The number of KPPs specified by a Sponsor should be kept to a minimum to maintain program flexibility. Failure of a system to meet a validated KPP threshold value triggers a review by the validation authority and evaluation of operational risk and/or military utility of the associated system(s) if KPP threshold values are not met. The review may result in validation of an updated KPP threshold value, modification of production increments, or recommendation for program cancellation. Post-validation change authority for KPPs is generally retained by the validation authority, unless specifically delegated in the validation memorandum.

b. KSAs. Performance attributes of a system considered important to achieving a balanced solution/approach to a system, but not critical enough to be designated a KPP. The number of KSAs specified by a Sponsor should be kept to a minimum to maintain program flexibility. Post-validation change authority for KSAs is generally delegated to the Sponsor, unless specifically retained in the validation memorandum.

c. APAs. Performance attributes of a system not important enough to be considered KPPs or KSAs, but still appropriate to include in the CDD or CPD are designated as APAs. Post-validation change authority for APAs is generally delegated to the Sponsor, unless specifically retained in the validation memorandum.

2. Threshold and Objective Values

a. Designating MOPs. KPPs, KSAs, and APAs are expressed using a threshold/objective format and, in accordance with reference bb, KPPs are included verbatim in the acquisition program baseline. They are expressed in terms of parameters which reflect MOP for the system rather than MOE in conducting the mission, as the latter should instead be evaluated against the capability requirements identified in the DODAF CV-3. They are chosen to be measurable, testable, and support efficient and effective T&E.

(1) Thresholds. Performance below the threshold value is not operationally effective or suitable or may not provide an improvement over current capabilities. Context must be provided to articulate what specific

operational impact or risk is unacceptable if the performance were to fall below the threshold value. The threshold value for a KPP, KSA, or APA must also be considered achievable within the projected life cycle cost, schedule, and technology at low-to-moderate risk.

(2) Objectives. The objective values are applicable when a higher level of performance represents significant increase in operational utility. Context must be provided to articulate what specific operational impact or risk is further mitigated if the performance were to reach the objective value. If applicable, the objective value is the desired operational goal achievable but at higher risk in life cycle cost, schedule, and technology. Performance above the objective value does not justify additional expense.

b. Tradespace. The difference between threshold and objective values sets trade space for balancing multiple KPPs, KSAs, and APAs while remaining above the threshold values. Advances in technology or changes in approved Service and joint concepts may result in proposals to change threshold and objective values in future increments of a capability solution.

3. Mandatory KPPs. In addition to KPPs, KSAs, and APAs essential to the capability solution being developed, Sponsors shall address the KPPs detailed in the following paragraphs.

a. Force Protection (FP) KPP. The FP KPP is intended to ensure protection of occupants, users, or other personnel (other than the adversary) who may be adversely affected by the system or threats to the system. Although a FP KPP may include many of the same attributes as those that contribute to the System Survivability KPP, the intent of the FP KPP is to address protection of the system operator or other personnel against kinetic and non-kinetic fires, CBRN, and environmental effects, rather than protection of the system itself and its capabilities.

(1) The FP KPP is applicable to CDDs and CPDs addressing manned systems, or systems designed to enhance personnel survivability.

(2) Additional guidance on the FP KPP is provided in Appendix B to this enclosure.

b. System Survivability (SS) KPP. The SS KPP is intended to ensure the system maintains its critical capabilities under applicable threat environments. The SS KPP may include reducing a system's likelihood of being engaged by hostile fire, through attributes such as speed, maneuverability, detectability, and countermeasures; reducing the system's vulnerability if hit by hostile fire, through attributes such as armor and redundancy of critical components; enabling operation in degraded EM, space, or cyber environments; and allowing

the system to survive and continue to operate in, or after exposure to, a CBRN environment, if required. In SoS approaches, it may also include resiliency attributes pertaining to the ability of the broader architecture to complete the mission despite the loss of individual systems.

(1) The SS KPP is applicable to all CDDs and CPDs.

(2) Additional guidance on the SS KPP is provided in Appendix C to this enclosure.

c. Sustainment KPP. The Sustainment KPP is intended to ensure an adequate quantity of the capability solution will be ready for tasking to support operational missions. The supporting Reliability KSA and O&S Cost KSA, ensure that the Sustainment KPP is achievable and affordable in its operational environment. Together, the KPP and supporting KSAs ensure early sustainment planning, enabling the requirements and acquisition communities to provide a capability solution with optimal availability and reliability to the warfighter at an affordable life cycle cost.

(1) The Sustainment KPP is applicable to all CDDs and CPDs.

(2) Additional guidance on the Sustainment KPP is provided in Appendix D to this enclosure and in reference pppp.

d. NR KPP. The NR KPP is intended to ensure new and modified IS fits into DOD architectures and infrastructure to the maximum extent practicable.

(1) The NR KPP is applicable to IS-ICDs, and all CDDs and CPDs addressing IS, regardless of classification or sensitivity of the data handled by the IS, unless defined as non-DODIN IT by reference qqqq.

(2) Additional guidance on the NR KPP is provided in Appendix E to this enclosure and in reference iiii.

e. Energy KPP. The Energy KPP is intended to ensure combat capability of the force by balancing the energy performance of systems and the provisioning of energy to sustain systems/forces required by the operational commander under applicable threat environments. The Energy KPP includes, but is not limited to, optimizing fuel and electric power demand in capability solutions, in the context of the logistical supply of energy to the warfighter, as it directly affects the burden on the force to provide and protect critical energy supplies. The Energy KPP includes both fuel and electric power demand considerations in systems, including those for operating “off grid” for extended periods when necessary, consistent with SSA products. In cases where energy demand reduction is impractical or insufficient to align with projected energy supply,

complementary DOTmLPF-P changes to the energy supply chain must be addressed in the document to accommodate the increased energy demands and satisfy the Energy KPP.

(1) The Energy KPP is applicable to all CDDs and CPDs where the balance of energy performance of the system and the provision of energy to the system, including both fuel and electric power, impacts operational reach, or requires protection of energy infrastructure or energy resources in the logistics supply chain.

(2) Additional guidance on the Energy KPP is provided in Appendix F to this enclosure.

f. Training KPP. The Training KPP is intended to ensure that materiel aspects of training capabilities, when applicable, are addressed as part of the development of the capability solution outlined in the CDD or CPD. Non-materiel aspects of training are to be captured as part of the DOTmLPF-P section of the CDD or CPD. For example, the long mission durations of submarine operations may necessitate that the warfighter use the Training KPP to specify certain training and simulation capabilities be integrated into the weapon system. Other weapon systems with shorter mission durations may have greater flexibility so the specific training approaches do not need to be dictated by the warfighter, leaving the most effective training approach to be determined by the training experts.

(1) The Training KPP is applicable to all CDDs and CPDs with materiel training requirements which dictate specific operational performance characteristics of the capability solution.

(2) Additional guidance on the Training KPP is provided in Appendix G to this enclosure.

g. Required certification or endorsement of mandatory KPPs. Prior to validation of CDDs and CPDs, assessing organizations will provide the lead FCB with a certification or endorsement of the KPP, concurrence that the KPP is not required, or changes the Sponsor must make in order to receive the certification or endorsement.

h. Waiving mandatory KPPs. All of the mandatory KPPs are generally required unless specifically waived prior to validation of a capability requirement document. In cases where a Sponsor proposes that a KPP is not appropriate to the operational context of a capability solution, the Sponsor shall justify why the KPP is not appropriate. See Enclosure E to this manual for information about certifying and endorsing organizations for each of the

Mandatory KPPs, and see the individual KPP appendices in this enclosure for specific means of requesting waiver or exemption to mandatory KPPs.

(1) To ensure there is general agreement of whether or not the KPP can be excluded and thus prevent potential staffing delays, Sponsors proposing that a mandatory KPP does not apply to their situation are required to seek approval, from the appropriate certifying or endorsing organization identified in Enclosure E of this manual, prior to submitting a capability requirement document for staffing and validation.

(2) In cases where a predecessor document did not include a mandatory KPP because it was not defined or was not mandated in an earlier version of JCIDS, the Sponsor will either include the KPP in the successor document, or work with the appropriate certifying or endorsing organization to ensure the intent of the KPP is otherwise captured in the document.

4. CONOPS Update and/or OMS/MP documentation

a. Additional data required. If not already contained within the CONOPS used during the CBA, the following information must be provided – as an update to the associated CONOPS and/or as OMS/MP documentation:

(1) Typical mission scenarios or profiles for each mission. The profiles should state specific amounts of operation (hours, rounds, miles, cycles, etc.) for each mission essential function within the mission.

(2) When appropriate, the CONOPS should address special conditions of use, such as any unique high-intensity cycles of use within a mission.

(3) Expected breakdown of environmental conditions.

(4) Total operating time for expected missions.

b. Data submission. Updates to CONOPS and/or OMS/MP documentation will be provided with the submission of CDDs and CPDs unless already available on the KM/DS system.

c. Follow-on usage. The additional detail provides traceability for the combinations of KPPs, KSAs, and APAs in the CDD (including the draft CDD supporting MS A) and the CPD. It also provides a baseline of specific mission performance to ensure T&E later in the acquisition process can directly measure missions intended by the warfighter.

5. Development of KPPs, KSAs, and APAs. The Sponsor designates appropriate attributes as KPPs, KSAs, and APAs dependent upon the nature of

the system and its intended capabilities. For documents with JSDs of JROC Interest or JCB Interest, the JCB or JROC may designate additional attributes as KPPs, KSAs, or APAs, or modify threshold or objective values, on the recommendation of the FCBs.

a. Initial questions. The following questions should be answered in the affirmative before a performance attribute is selected as a KPP, KSA, or APA for the increment being defined:

(1) Is the performance attribute traceable to, and a necessary component of satisfying, one or more operational attributes of capability requirements validated in the ICD, or one of the mandatory KPPs of the system being documented in the CDD or CPD?

(2) Does the threshold value of the performance attribute contribute to significant improvement in warfighting capabilities, operational effectiveness, and/or operational suitability, where an inability to meet the threshold value should call into question the continued value of the program?

(3) Are the necessary combinations of KPPs, KSAs and/or APAs, and their threshold/objective values, identified in a manner which allows assessment of ability to achieve mission success in the operational context? Are the combinations of KPPs, KSAs and/or APAs consistent with the CONOPS and/or the OMS/MP documentation? For example:

(a) If an individual system includes KPPs, KSAs, and/or APAs such as range, payload, and loiter time, different missions intended for the system may require the KPPs, KSAs and/or APAs in different combinations.

(b) Meeting each KPP, KSA and/or APA in isolation might not provide any mission value and not allow operations consistent with the OMS/MP. I.e. – meeting required range without any munitions or loiter time, meeting required payload without any range or loiter time, or meeting required loiter time without any range or payload.

(c) Meeting each KPP, KSA and/or APA in combination, using the maximum values required for any one mission but without the context of the individual missions may allow operations consistent with the OMS/MP, but lead to an unreasonably expensive or unachievable capability solution. I.e. – combining the payload required for short heavy lift missions, with the range required for an empty ferry flight mission, with the loiter time required for a lightly armed surveillance mission, does not properly reflect the capability requirements of the system nor the set of conditions against which it should be tested.

(4) Are the recommended threshold and objective values of the KPP, KSA, or APA reflective of reasonable operational risks, applicable technology maturity, timeframe the capability is required, and supported by analysis?

(5) Is the threshold value of the KPP, KSA, or APA achievable and affordable, considering projected life cycle costs and constraints of Service and DOD projected TOA over the FYDP and 30-year projections?

b. KPP change authority. While change authority for KPPs is generally retained by the validation authority, KSAs and APAs may generally be traded off against each other as long as KPP thresholds are achieved and change authority for KSAs or APAs has not been retained by the validation authority.

c. T&E considerations. Sponsors must establish KPPs, KSAs, and APAs which are measurable and testable, and are defined in a manner which supports efficient and effective T&E.

(1) Very tightly specified KPPs, KSAs, and APAs are resource intensive to test with confidence. When such specificity is needed, the Sponsor must consider the T&E resource implications of requiring capabilities to perform to such high tolerances.

(2) Avoid specifying all-inclusive values for parameters, such as all/never, 0%/100%, all-sensors, all-weather, all/none of the time, no/every situation, etc. These kinds of values are generally impossible to achieve and requires an infinite amount of testing to prove statistically.

(3) Other choices made when specifying KPPs, KSAs, and APAs may require higher or lower T&E resources. For example, probability metrics are expensive to test because they require large sample sizes to gain statistical confidence in the results. However, if meaningful continuous metrics that relate to the probability metrics can be derived, T&E resources may be significantly reduced.

(4) Interactions between Sponsors and the T&E community during development of KPPs, KSAs, and APAs can help identify more testable alternatives.

d. Example development methodology. The following set of steps is one methodology for developing KPPs, KSAs, and APAs:

(1) List capability requirements for each mission or function as described in the proposed CDD or CPD. This review should include all capability requirements that the system described in the CDD/CPD is projected to meet, including those related to other systems in a FoS or SoS

context. It shall also include all relevant performance metrics identified in ICDs for which the CDD/CPD is providing a capability.

(2) Review the list of performance attributes associated with each of the joint functions in this enclosure for potential applicability. Compile a list of potential performance attributes using this enclosure as a starting point and include any other performance attributes that are essential to meeting the operational attributes and associated values of the capability requirements validated in the ICD.

(3) For each critical mission or function, build at least one measurable performance attribute, without yet designating as a KPP, KSA, or APA, using the list from the previous step as a starting point.

(4) Determine the performance attributes that are most critical or essential to the system(s) and designate them as KPPs. Other important performance attributes can be assigned as KSAs or APAs. Note that a KPP need not be created for all missions and functions for the system(s), as a KSA or APA may be used without an overarching KPP. In contrast, certain missions and functions may require two or more KPPs.

(5) Document how the KPPs, KSAs, and APAs are traceable to the operational attributes and associated values of the capability requirements identified in the ICDs or other predecessor documents. This ensures that KPPs, KSAs, and APAs are aligned to support the mission outcomes and associated desired effects.

(6) Set threshold and objective values for KPPs, KSAs, and APAs.

(a) Threshold values should be based upon the minimum performance required to achieve the required operational effect, while being achievable through the current state of technology at an affordable life cycle cost of the system. Technology achievability is based upon the technology behind delivery of the performance having achieved technology maturation sufficient for MS B; or system or sub-system performance being on track to achieve TRL six or greater prior to MS B.

(b) Objective values should be defined where an increased level of performance delivers significant increased operational effect, or decreased operational risk, if it can be delivered at an affordable life cycle cost of the system. Not every KPP, KSA, or APA must have an objective value which differs from the threshold value.

e. Refinement of threshold and objective values. Threshold and objective values of an KPP, KSA, or APA may change between the CDD and the CPD.

The development threshold and development objective values specified for the KPP, KSA, or APA in the CDD are used to guide the acquisition community during EMD.

(1) During EMD, tradeoffs are made between the threshold and objective values to optimize performance, given the available technology for the increment and the competing demands introduced by combining subsystems into the overall system.

(2) A deeper analysis of cost-capability trade-offs at and around threshold and objective values may be beneficial to decision makers, by exploring incremental return on investment where particular KPPs, KSAs, and APAs might be insensitive to small deviation at great advantage in life cycle cost, performance, schedule, and quantity reviews.

(3) After the CDR, these tradeoff decisions are essentially completed and a more precise determination of acceptable performance can be stated in the CPD.

(a) Figure D-A-1(a) shows a performance attribute (A) of a system with threshold and objective values (1 and 10, respectively) determined during the TMRR phase of acquisition and presented in the CDD. During EMD, optimum performance values may be identified on the basis of life cycle cost, performance, or other considerations, as shown in Figure D-A-1 (b).

(b) Further design tradeoffs among the collective performance attributes may necessitate settling for design performance values higher or lower than the optimum values for the individual performance attributes. Figure D-A-1 (c) shows an example in which optimum performance was traded off because of other considerations, resulting in reduced performance within performance attribute A.

(c) The production threshold and production objective values specified for the performance attribute in the CPD will be a refined version of the development threshold and development objective values documented in the CDD. Figure D-A-1 (d) shows an example of the revised performance attributes that would be included in the CPD. Note that the production threshold and objective values are not necessarily bounded between the original development threshold and objective values.

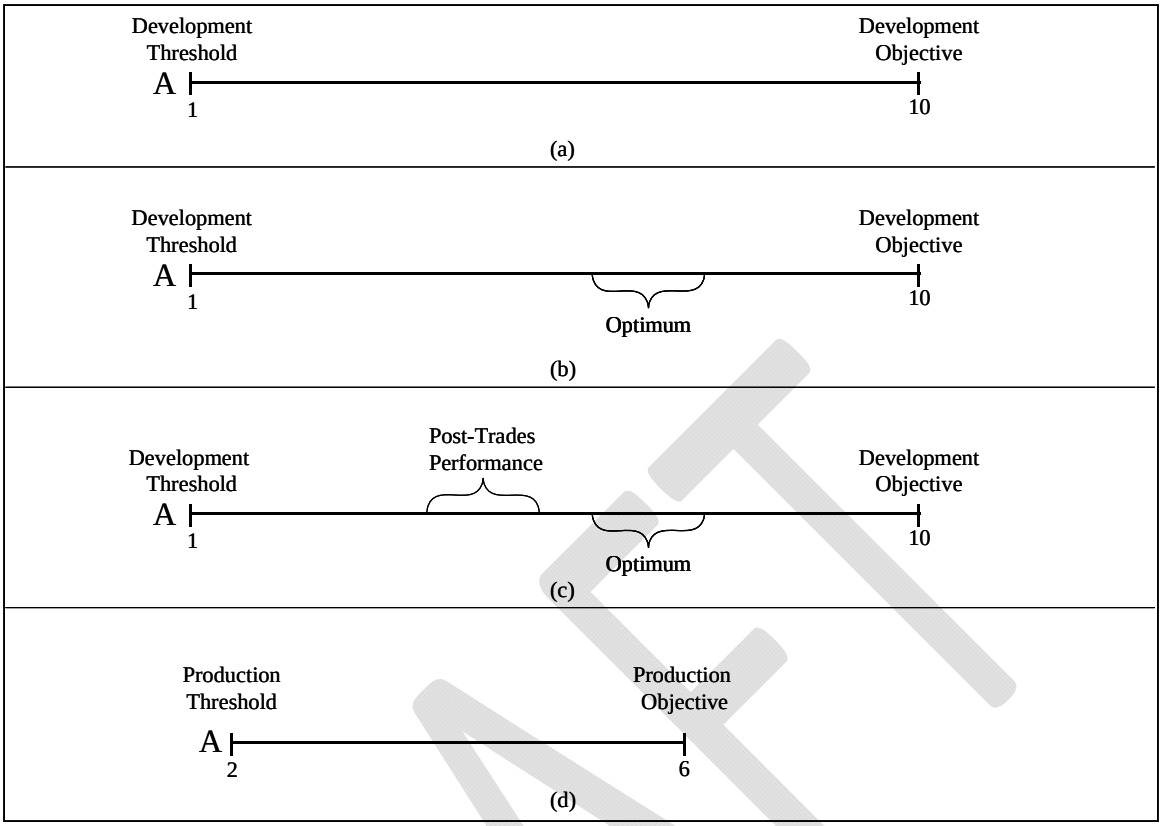

Figure D-A-1. CDD and CPD Performance Attributes

(d) Each production threshold value should be assessed against knowledge gained during the EMD phase of acquisition. KPP and non-KPP threshold values in the CPD will generally denote equal or increased performance over the corresponding CDD threshold values. In cases where CDD KPP or KSA threshold values are to be reduced in a CPD, the following issues must be addressed in the CPD:

1. What are the impacts to military utility and operational risk from performance below the original threshold value?

2. If the new capability solution is intended to replace a fielded capability solution, will it still provide more overall military utility than the fielded capability solution?

3. Is the reduced performance of this capability solution still a good way to address the capability requirement and close the associated capability gap, or should a different materiel or non-materiel alternative approach be considered?

4. Is the reduced performance of the capability solution worth the additional investments required to continue the program to completion?

5. What level of increased investment might be required to maintain the original threshold performance? If pursued, where will the additional funds come from while remaining below projected TOA, and what operational risks are involved with the source of the additional funds?

(e) For an early increment in an incremental approach to acquisition, the production objective value for the increment could be less than the development threshold value, with later increments providing performance at or above the threshold. In that case, plans must be in place to upgrade early increments to meet threshold values, or to use early increments to support less demanding missions, and later increments to support more demanding missions.

(4) Trade space between threshold and objective values of KPPs, KSAs, and APAs may also be exercised by Sponsors to support later upgrades of a capability solution without revalidation of a capability requirement document, as long as there are no changes to operational context or threats that would otherwise require revalidation.

6. Requesting KPP Relief. To fulfill the JROC's Title 10 responsibilities for tradeoffs between cost, schedule, and performance when validating military requirements, the JROC encourages the requirements Sponsor, in coordination with the MDA, to request requirements relief from the validation authority when cost-benefit analyses indicate previously validated KPPs may drive costs out of proportion with the capability delivered to the operational user.

a. Changing context over time. While the KPPs (and KSAs and APAs) documented and validated in capability requirement documents represent the validation authority's best military advice at an instant in time, knowledge gained through acquisition activities, changes to strategic guidance, external threats, mission requirements, or budgetary realities may make relief from previously validated KPPs appropriate.

b. Budgetary considerations. While there are no limitations for requesting requirements relief, KPP relief should be considered especially appropriate in cases where significant cost savings may be achieved with marginal impact to operational capability. I.e. – spending 15 percent of a program's budget to get the last 3 percent of a KPP threshold, if the operational risk involved with a reduced threshold is minimal.

7. Potential KPP, KSA, or APA Performance Attributes. The following list is provided to assist in identifying potential KPPs, KSAs, and APAs for a system based on the joint functions defined in reference rrrr. For each characteristic, a definition is provided as well as a list of potential performance attributes.

The list is not intended to be all encompassing, and Sponsors may identify other performance attributes as part of the process delineated in this enclosure.

a. Command and Control (C2) – C2 encompasses the exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of the mission.

(1) Contact – detection range/time, time to discriminate, time to classify type, time to identify as adversary/non-adversary

(2) Information – ability to create, store, discover, access, modify, or reconfigure

(3) Accurate engagement decision/engagement sequence

(4) Automated mission planning – quality, timeliness, useability

(5) Initial report – accuracy, speed

(6) Communication throughput while mobile/non-mobile

(7) Interoperable – with new and/or legacy systems

(8) Net ready

(9) Networked with specific sensors/units

(10) Waveform compatibility

(11) Internal growth

(12) Types of broadcast supported/scalability

(13) Data – transfer-distribution rate/update rate

(14) Multi-channel routing/retransmission/operation on the same net

(15) Data variable rate capability

(16) Coded message error probability

(17) Frequency range

(18) Transmitted data accuracy

DRAFT

(19) Security of C2 data

b. Battlespace Awareness (BA) – The ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision-making, and weapon system operational employment, by leveraging all sources of information to include intelligence, surveillance, reconnaissance, and METOC.

(1) Coverage/focus areas

(a) Contiguous area (wide and narrow field of view)

(b) Simultaneity

(c) Synoptic area coverage

(2) Range of surveillance systems/sensors/communications

(a) Platform range and operational characteristics (operating altitudes, refueled and unrefueled range, time on station (TOS), etc.)

(b) Effective range to target for all onboard sensors under differing weather conditions

(c) Required infrastructure (ground stations, relays, satellite communication (SATCOM), etc.)

(3) Persistence

(a) Time on target

(b) Endurance once on target

(c) Vulnerability to natural environment – day/night/adverse-weather

(d) Vulnerability to countermeasures – denied or opposed access

(e) Revisit rates or intervals

(4) Timeliness

(a) Time to target or re-target sensors

(b) Time to report; once data is collected, time to requested user

(5) Sensor Performance

(a) Bandwidth range collected against

(b) Geolocation accuracy

(c) Resolution in National Imagery Interpretability Rating Scale (NIIRS) or Ground Sample Distance (GSD)

(d) Spectrum covered by sensor collection

(6) Tracking Sensors

(a) Minimum detectable velocities

(b) Geolocation accuracy

(c) Ability to hold track – time, types of targets, multiple target capability

(7) Processing/Exploitation

(a) Images processed per hour

(b) Image quality

(c) Image interpretability

(d) Geospatial accuracy

(e) Accuracy of data tags and classification markings

(8) Analysis, Prediction, and Production

(a) Ability to integrate, evaluate, interpret, and predict knowledge and information from available sources to develop intelligence and forecast the future state

(b) Data fusion – number of data sources able to be fused together, types of INTs able to be fused together, accuracy of fused data

(c) Time spent data mining vs. time spent performing analysis, prediction, and production

DRAFT

(9) BA Data Dissemination and Relay

(a) Ability to discover and retrieve information for all appropriate data sources – time to retrieve information, quality of information retrieved

(b) Ability to authenticate users and machines and make authorization decisions for their access to information

(c) Ability to transmit data from collector through a media link to a processing site

(d) Ability to support the data relay with adequate capacity, continuity, and reliability

(10) Meteorology and oceanography including space weather and astro-geophysics

(a) Atmospheric vertical moisture profile – time to produce profile, accuracy of profile

(b) Global sea surface winds – time to produce profile, accuracy of profile

(c) Atmospheric vertical temperature profile– time to produce profile, accuracy of profile

(d) Imagery – quality of imagery

(e) Sea surface temperature horizontal resolution

(f) Soil moisture (surface) sensing depth

(g) Sea state – wave height, currents, storm effects

(h) Bathymetry, sea mounts, other navigational hazards

(11) Intelligence Mission Data (IMD). Intelligence and other data required to enable accurate characterization, identification, and response to the battlespace (White, Red, Grey, Blue):

(a) Geospatial Intelligence (GEOINT) data types, regional or country-related specifications

(b) Characteristics and Performance (C&P) data types, regional or country-related specifications

(c) Signature data types, emitter parametric data for each platform with regional or country-related specifications

(d) Order of Battle (OOB) types, regional or country-related specifications

(e) Electronic Warfare Integrated Reprogramming (EWIR) Intelligence data types, emitter parametric data for each platform with regional or country-related specifications.

c. Fires – To use available systems to create a specific lethal or nonlethal effect on a target.

(1) Weapon – launch envelope/weight/number on launchers

(2) Platform – systems/launchers/firing-storing capacity

(3) Weapon – off axis launch angle, off bore sight angle, adverse weather, day-night

(4) Intercept/circular error probable

(5) Acceptable engagement sequence time

(6) Mission response time

(7) Power-up/fire/re-fire/weapon launch rate

(8) Sortie rate – generated/sustained/surge

(9) Weapon in-flight re-targeting

(10) Detect to engage scenarios

(11) Expected fractional damage

(12) Probability of kill/mission kill – probability of hit, maximum allowable CEP or miss distance

(13) Weapon range

(14) Dud or unexploded ordnance (UXO) rate

DRAFT

d. Movement and Maneuver – Disposing joint forces to conduct campaigns, major operations, and other contingencies by securing positional advantages before combat operations commence and by exploiting tactical success to achieve operational and strategic objectives.

(1) Air vehicles – land-takeoff distance/ship launch-recover parameters/deck spot factor

(2) Air vehicle – climb rate-gradient/G-load capability

(3) Air vehicles – vertical-short take-off and landing/aerial refueling/classes of airspace/altitude (max-min-on station-intercept)

(4) Water vehicles – land-launch spots/compatibility with other water vehicles

(5) Ground vehicle – maneuverability, stability, fording depth

(6) Platform range – maximum/minimum/combat-mission radius

(7) Water vehicles – draft/weight/stability/electrical generating capacity/test depth/sea state limitations

(8) Compatible on aircraft/aircraft carriers/ships

(9) Physically interoperable with other platforms/systems/subsystems/ warheads/launchers

(10) Platform speed – maximum/minimum/cruise/flank/sustained/ acceleration/land-sea-air

(11) Weight/volume to fit expected carrying platforms

(12) Ability to transport aircraft/vehicles/cargo/fuel/passengers/ troops/crew

(13) Lift capacity

(14) Platform transportability

(15) Self-deployment capability – range, time to prepare/recover.

(16) Cargo transfer rate

DRAFT

(17) Platform specified timelines

e. Protection – Conserving the joint force's fighting potential through active defensive measures, passive defensive measures, applying technology and procedures, and emergency management and response.

(1) Access and control

(2) Threat challenges – countermeasures/radar cross section-size/ multiple numbers

(3) Ability to withstand hit/blast/flood/shock/CBRN effects

(4) Assured communications to national, missile defense, and nuclear forces

(5) Covertness – radiated noise/active target strength/radar cross section/EM quieting/radio frequency signature

(6) Cybersecurity – ability to protect or secure and defend information and IS by ensuring information availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities.

(7) Jam resistance – ability to resist or deny adversarial attempts to disrupt or disable our systems within operations

(8) Tactics, techniques, and procedures/countermeasures

(9) Jamming capability – reduction in adversary tracking time, reduction in adversary detection range

f. Sustainment – The provision of logistics and personnel services necessary to maintain availability of materiel and support operations until mission accomplishment.

(1) Logistics footprint – Materiel, mobility, and space required to effectively sustain the system in the field.

(2) Sustained operations – The ability of the system to be employed in an operational context for a given timeframe without logistics resupply or support.

(3) Time – The ability of the system to support operational logistics considerations, e.g., logistics closure rate for limited operations and full operations.

(4) Maintainability – The ability of the system to be brought back to a state of normal function or utility. Normally expressed as Mean Down Time, Mean Time To Repair or a calculation of ease of maintainability. Subordinate attributes which may be considered as KSAs or APAs:

(a) Corrective Maintenance – All actions performed as a result of any failure, to restore a system, subsystem, or component to a required condition.

(b) Mission Maintainability – The ability of the system to be retained in or restored to a specified mission condition.

(c) Maintenance Burden – A measure of maintainability related to the system's demand for maintenance manpower.

(5) Supportability – The ability of the system to identify and/or predict failures down to a certain subsystem level within a given percentage of accuracy. Potential attributes include health management, prognostics and diagnostics capabilities, Condition-Based Maintenance + enablers, support equipment, and parts commonality. Subordinate attributes which may be considered as KSAs or APAs:

(a) Built-In Test (BIT) Fault Detection – A measure of recorded BIT indications which lead to confirmed hardware failures.

(b) BIT Fault Isolation – A measure of recorded BIT indications which correctly identify the faulty replaceable unit, either directly or through prescribed maintenance procedures.

(c) BIT False Alarms – A measure of recorded BIT indications showing a failure when none has occurred.

(6) Cost – Included as part of the O&S Cost KSA, normally expressed as the total O&S costs regardless of funding source over the projected life cycle of the capability solution in Base Year Dollars.

(7) Transportability & Deployability – The ability of the system to be moved and deployed within the Department's transportation infrastructure in accordance with reference hhhh.

(INTENTIONALLY BLANK)

DRAFT

APPENDIX B TO ENCLOSURE D

CONTENT GUIDE FOR THE FORCE PROTECTION KPP (FP KPP)

1. Overview

a. Purpose. Force protection attributes are those intended to protect the human occupants of manned systems, humans that interface with unoccupied systems, and non-adversary personnel subjected to hostile actions. Use of the FP KPP in CDDs and CPDs is expected for all manned systems, unmanned systems which interface with or operate in the proximity of personnel, and for systems designed to enhance personnel survivability.

b. Synergy/overlap with SS KPP. The FP KPP may include some of the same attributes as those in the SS KPP, but the emphasis is on protecting system occupants or other personnel rather than protecting the system itself. As such, the level of performance attributes in the FP KPP are generally higher than those in the SS KPP. (i.e. – inability to continue the mission where the occupants or other non-adversary personnel are protected from becoming casualties is generally preferable to cases where the system remains mission capable but the occupants or other non-adversary personnel in the vicinity become casualties.)

c. Exclusion of Offensive Capabilities. Offensive capabilities that are primarily intended to defeat adversary forces before they can engage non-adversary forces are not included in the FP KPP.

d. Tailoring of Standards. For attributes listed below which have an associated protection standard identified, compliance with the standard is expected unless specific operational context for the capability solution indicates that a higher or lower standard of force protection is more appropriate. In cases where a deviation from the standard is appropriate, the FP KPP will identify the tailored levels of force protection required, along with rationale as to why the operational context makes a different level of protection appropriate.

2. Force Protection Attributes. Attributes for the FP KPP fall into five general categories which must be addressed when applicable to the system under consideration – either as a feature designed into the system or mandated as protective equipment used by personnel exposed to the applicable threats.

a. Protection from kinetic fires

(1) Level of armor protection.

(2) Munitions (sizes) which are ineffective.

(3) Level of shock/blast which is survivable.

(4) Level of fire/flame resistance of components.

b. Protection from non-kinetic fires (other than CBRN)

(1) Standards for protection from lasers/dazzlers/eye-safety (with or without specific PPE) are outlined in reference ssss.

(2) Protection from EM attack physiological effect, including ability to maintain functionality during high level EM exposure or electromagnetic pulse (EMP) conditions.

c. Protection from CBRN effects. Applicable to systems required to operate through CBRN environments in accordance with reference tttt.

(1) Detection and identification.

(2) Air filtration and/or pressurization.

(3) Medical prophylaxes and/or countermeasures.

(4) Decontamination/recovery capabilities.

(6) For systems covered under reference uuuu, nuclear survivability.

d. Protection from environmental effects. General standards are outlined in references vvvv and wwww.

(1) Standards for acceptable pressure/oxygen levels for personnel, including pressurization and/or supplemental oxygen are outlined in reference xxxx.

(2) Acceptable temperature limits for personnel (with or without specific PPE).

(3) Standards for acceptable vibration/acoustic limits for personnel (with or without specific PPE) are outlined in reference yyyy.

(4) Acceptable G-force loading limits for personnel (with or without specific PPE) under normal operations.

e. Protection from crash events

DRAFT

(1) Standards for crash survivable G-force loading limits for personnel (with or without specific PPE) are outlined in reference zzzz.

(2) Protection from impact trauma, including seats and retaining systems.

(3) Preservation of occupied space.

(4) Preservation of post-crash fuel spills and fires.

3. Proponent. The FP KPP proponent is the Protection FCB, with advisory support from the Office of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)). For questions, please contact the Protection FCB at 703-693-7116.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX C TO ENCLOSURE D

CONTENT GUIDE FOR THE SYSTEM SURVIVABILITY KPP

1. Overview

a. Purpose. SS KPP attributes are those that contribute to the survivability of a system's capabilities from kinetic and non-kinetic fires. These include attributes which support:

(1) Reduced likelihood of being hit by kinetic or non-kinetic fires.

(2) Reduced vulnerability if hit by kinetic or non-kinetic fires, including cyber effects.

(3) Resiliency of the overall force (broader than a single system architecture) to complete the mission despite the loss of individual platforms.

(a) Resilience is the ability of the collection of systems to support the functions necessary for mission success in spite of hostile action or under adverse conditions.

(b) An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities.

(c) Include whether or not the system must be able to survive and operate in, or after exposure to, CBRN environments in accordance with reference tttt. If the system is covered under reference uuuu, nuclear survivability attributes must be designated as part of the SS KPP.

(d) Include whether or not the system must be able to survive and operate in a cyber-contested environment or after exposure to cyber threats which prevent the completion of critical operational missions by destruction, corruption, denial, or exposure of information transmitted, processed, or stored.

b. Synergy/overlap with FP KPP. The SS KPP may include some of the same attributes as those in the FP KPP, but the emphasis is on maintaining the mission capabilities of the system through the applicable threat environment rather than protecting system occupants or other personnel.

c. Exclusion of Offensive Capabilities. Offensive capabilities that are primarily intended to defeat adversary forces before they can engage non-adversary forces are not included in the SS KPP.

d. Tailoring of Standards. For attributes listed below which have an associated standard identified, compliance with the standard is expected unless specific operational context for the capability solution indicates that a higher or lower standard of system survivability is more appropriate. In cases where a deviation from the standard is appropriate, the SS KPP will identify the tailored levels of system survivability required, along with rationale as to why the operational context makes a different level of system survivability appropriate.

2. Potential Attributes or Considerations. Depending upon the aspect of system survivability addressed by the attribute, these may be applicable to the overall system, only applicable to certain subsystems, or applicable at different levels of survivability to different parts of the system.

a. For reduced probability of hit. Reduced likelihood of being hit by kinetic or non-kinetic fires:

(1) Situational awareness, such as missile warning, laser warning, radar warning, or hostile fire indication capabilities.

(2) Speed.

(3) Maneuverability.

(4) Visual, acoustic, and/or electronic detectability, including EM spectrum control.

(5) System countermeasures, such as RF jammers, laser dazzers, and expendable dispensing systems.

(6) Accurate engagement - lethal and non-lethal.

(7) Electronic protection.

(8) Access control.

b. For reduced vulnerability if hit. Reduced vulnerability of critical system components or structures (i.e., radars, weaponry, or command & control devices) if hit by kinetic or non-kinetic fires.

DRAFT

(1) Durability – inherent ability of components or structures to withstand hit/blast/flood/shock for kinetic fires, or resistance to EM or cyber effects from non-kinetic fires.

(2) Added protection – armor for components or structures without sufficient durability to survive kinetic fires, or shielding/hardening for components without sufficient resistance to EM or cyber effects from non-kinetic fires.

(3) Redundancy – ability of individual components or structures to be compromised, from kinetic or non-kinetic fires, without loss of the system's capabilities.

c. For increased resiliency of the force

(1) Robust architecture – ensuring capabilities remain available despite losses of specific numbers of systems, or losses of specific enabling systems.

(a) Systems dependent upon PNT capabilities shall be compliant with PNT survivability policies in reference aaaaa, or obtain a waiver in accordance with the process outlined therein.

(b) Survivability under loss of other enabling systems may be governed by other policies and will be evaluated on a case-by-case basis.

(2) Networked – ensuring data remains available despite losses of specific numbers of systems, or losses of specific enabling systems.

(3) Survival and operation through CBRN effects in accordance with reference tttt, if applicable to the operational context:

(a) Protection from CBRN effects, including EMP. If CBRN survivability is required, include appropriate CBRN attributes to the SS KPP.

(b) Designation as CBRN mission critical. State whether the system has been designated as mission-critical, and if so, whether it has been designated as CBRN mission-critical, including brief rationale.

(c) If the system is covered under reference uuuu, include nuclear survivability attributes.

(d) As applicable, address operational and maintenance requirements related to ensuring continuing hardness against CBRN environments.

(4) Survival and operation in a cyber-contested environment or after exposure to cyber threats, if applicable to the operational context:

(a) In accordance with reference bbbbb, state the system's cybersecurity categorization for availability, integrity, and confidentiality and whether the system is an applicable system in accordance with reference ccccc.

(b) If cyber survivability is required, include appropriate cyber attributes in the SS KPP based on applicable cybersecurity controls as directed by reference bbbbb and strength of implementation required to protect against cyber threats likely to be encountered in the operational environment.

(c) If applicable, address operational and maintenance issues related to ensuring continuing resilience against cyber threats.

3. Proponent. The SS KPP proponent is the Protection FCB. For questions, please contact the Protection FCB at 703-693-7116.

DRAFT

APPENDIX D TO ENCLOSURE D

CONTENT GUIDE FOR THE SUSTAINMENT KPP

1. Introduction

a. Purpose. This guide provides requirements managers, with support from the acquisition community, a guide to assist them in ensuring that effective sustainment is addressed and achieved. This is accomplished through compliance with the sustainment metrics as identified in the capability requirement documents. This guide does not prescribe what will be provided to satisfy sustainment requirements, but provides factors to be considered when determining if the rationale being provided meets the rigor needed for programs requiring a sustainment metric. The methodology utilized to establish the Sustainment KPP will be reviewed and shall include sufficient supporting documentation. Reference pppp will assist Sponsors and PMs in developing the Sustainment KPP.

a. Sustainment as a key component of performance. Including sustainment planning early during design and procurement enables the requirements and acquisition communities to provide a system with optimal availability and reliability to the warfighter at an affordable life cycle cost.

b. Value. The value of the Sustainment KPP is derived from the capability requirements of the system, assumptions for its operational context and intended use, and the planned logistical support. Fully-developed sustainment objectives allow the PM to develop a solution to satisfy the warfighter requirements and system performance to be measured against standardized metrics.

2. Background. The tenets of life cycle management emphasize sustainment planning early in the capability solution's life cycle, to include requirement generation activities. Life cycle management is the implementation, management, and oversight by the PM of all activities associated with the acquisition, development, production, fielding, sustaining, and disposal of a DOD system. This guide emphasizes those sustainment analyses, activities, and documents necessary to ensure the design, development, testing, production, and fielding of reliable, affordable, and maintainable systems. The criteria, information, and activities listed are not inclusive – that is, they cannot necessarily be applied to all systems. The Sponsor, together with the PM, must determine whether and how each item is applicable to its specific concept, technology, and/or system, although sufficient sustainment metrics to ensure a viable, cost-effective, and supportable system must be incorporated.

3. Overview of the Sustainment KPP Development

a. Derivation of the Sustainment KPP. The Sustainment KPP is derived from system availability requirements to support the required capability, assumptions for its design and operational use, tradeoffs between reliability, maintenance concepts, life cycle cost, and the planned sustainment strategy. In order for the PM to develop a complete system to provide warfighting capability, sustainment objectives must be established and performance of the entire system measured against those metrics. The operational framework for the expected Materiel and Operational Availability must be clearly articulated during the AoA or similar studies, and based upon the operational context in the validated ICD. For example, if a CCMD has capability requirements which lead to the development of a new medium lift transport vehicle, knowledge of the range of missions and required duration; constraints on loading and capacities; knowledge of operating environments and other related mission criteria are essential to ensure developers consider the variables that affect the Sustainment KPP.

b. Operational Framework. During the AoA or similar study, the operational framework should guide the development of alternative materiel and non-materiel solutions (including hardware/software systems) and alternative sustainment approaches. Assessment of capability requirements and performance metrics must consider both the system and its sustaining support at the same time. Additionally, the AoA or similar study should be influenced by the sustainment requirements of the system, particularly availability, reliability, maintainability, and O&S costs.

c. Elements of the Sustainment KPP. The Sustainment KPP is supported by several elements that provide an integrated structure that balances sustainment with capability and affordability across a capability solution's life cycle, and informs decision makers in trade-off analysis. KSAs may be traded off against each other without revalidation as long as the Sustainment KPP is still met. If changes to the KSAs result in the Sustainment KPP threshold not being met, the document will be resubmitted to the validation authority for revalidation. See reference pppp for additional guidance on the following elements:

(1) Materiel Availability and Operational Availability. The Sustainment KPP consists of two primary components: Materiel Availability and Operational Availability. Respectively, they provide fleet-wide availability and operational unit availability. The following provides guidance for development of both metrics:

(a) Materiel Availability. Materiel Availability is the measure of the percentage of the total inventory of a system operationally capable, based on materiel condition, of performing an assigned mission. This can be expressed

mathematically as the number of operationally available end items/total population. The total system population includes all operational systems necessary to support the Operational Context of the CDD/CPD to include operational systems for training (vice mock-ups, partial systems, simulators), systems for attrition reserve and prepositioning, and systems temporarily in a non-operational materiel condition, such as planned depot maintenance. Materiel Availability covers the timeframe from placement into operational service through the planned end of service life. Materiel Availability should take into account all calendar time that a system is in the inventory, including "out-of-reporting" status. For single or small-quantity systems, Materiel Availability can represent available time (i.e., up time, when the system is in operational status) as a percentage of total calendar time. Table D-D-1 provides an example of a single location to display total system inventory requirements and may be modified to reflect each system's inventory requirements.

	CONOPS	Training	Attrition	Prepositioned	Average Annual Down*	Total
CONUS						
OCONUS						
TOTAL						
* The average number of unavailable assigned assets, based on assumed planned depot/shipyard cycles.						

Table D-D-1. Total System Inventory

(b) Operational Availability. Operational Availability is the measure of the percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission and can be expressed as (uptime/(uptime + downtime)). Determining the optimum value for Operational Availability requires a comprehensive analysis of the system and its planned CONOPS, including the planned operating environment, operating tempo, reliability and maintenance concepts, and supply chain solutions. Operational Availability may be equivalent to Materiel Availability if the total number of a system or group of systems within a unit is the same as the total inventory.

(2) Reliability KSA. Reliability is a measure of the probability that the system will perform without failure over a specific interval, under specified conditions. Reliability shall be sufficient to support the warfighting capability requirements, within expected operating environments. Considerations of reliability must support both availability metrics.

(a) More than one reliability metric may be specified, as KSAs and/or APAs, for a system as appropriate. See Table D-D-2 for examples of metrics for different types of systems and reference pppp for further

information and instruction. In all cases, the Sponsor shall define specific criteria which constitute failures.

(b) For continuous use systems (such as an aircraft), reliability should be measured in terms of its primary usage metric (such as operating hours, miles or flight hours). For discrete systems (such as a single use munition), reliability should be measured as a probability.

(c) Mission Reliability. The measure of the ability of an item to perform its required function for the duration of a specified mission profile, defined as the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation.

(d) Logistics Reliability. The measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment, including all failures to the system and maintenance demand as a result of system operations.

(3) O&S Cost KSA. Measuring O&S cost provides balance to the sustainment solution by ensuring that the total O&S costs across the projected life cycle associated with availability and reliability are considered in making decisions.

(a) The O&S Cost KSA is to be computed using Base Year dollars. For consistency and to capitalize on other efforts in this area, all CAPE O&S cost elements, outlined in reference ddddd, will be used in support of this KSA. Energy costs shall be included in O&S cost, and will use the base year price throughout the assessment. All O&S costs are to be included regardless of funding source or management control.

(b) The O&S cost should cover the planned O&S timeframe, consistent with the timeframe and system population identified in the Sustainment KPP. As part of the supporting rationale, provide the annual cost per system (for large systems such as aircraft, vehicles, ships, etc.) or fleet of systems (for networks or smaller systems such as munitions) upon which the O&S Cost KSA total is based. The O&S Cost KSA objective values should be calculated in Base Year dollars as 10% less than the threshold value.

(c) Submit documentation of sufficient detail to explain all assumptions, data, and methodologies used to develop the threshold estimate values into KM/DS for archival and reference purposes. Programs must plan for maintaining the traceability of costs incurred to estimates and must plan for testing and evaluation. The Sponsor shall plan to monitor, collect, and validate operating and support cost data to support the O&S Cost KSA.

d. Sustainment KPP for complex systems. For complex systems and SoS, the Sustainment KPP and supporting Reliability KSA should be applied to each major end item or configuration item. For example, for a distributed complex network, the "network availability" (that is, availability of the network function to the user) may be a warfighter requirement but will be difficult to evaluate in test. The Sustainment KPP and Reliability KSA should be derived and applied to individual nodes of the network. Ship platforms, unmanned aircraft systems and satellite constellations are other examples. The O&S Cost KSA, however, should be applied to the whole program and not to individual configuration items, unless there are multiple documented subprograms.

e. Documentation. A Reliability, Availability, Maintainability, and Cost (RAM-C) report, as defined in reference pppp, will document the quantitative basis for the three elements of the Sustainment KPP as well as the tradeoffs made with respect to system performance.

f. Development Guide. A guide for developing the appropriate sustainment metrics for different categories of systems is provided in table D-D-2 as an aid for the Sustainment KPP.

4. Proponent. The Sustainment KPP proponent is the Joint Staff J-4 / Maintenance Division (J-4/MXD), with analytical support from the Office of the Deputy Assistant Secretary of Defense for Materiel Readiness (DASD(MR)). For questions regarding the Sustainment KPP, contact J-4/MXD at 703-614-0161.

DRAFT

	Distinguishing Characteristics	Materiel Availability	Operational Availability	Reliability (Note 1)
Ship Platforms	Naval vessels with multiple missions and multiple large or complex systems. Planned down time.	The availability of the entire population of systems for tasking when a ship is not in a planned maintenance availability or unavailable due to CASREP 4 failure.	Percentage of time an operationally deployed ship is not in a CASREP 4 state over a given operating period.	• Mission Reliability = operating hours / mission failures (e.g. CASREP 4 failures) • Logistics Reliability = operating time / failures
Aircraft Platforms	Aviation programs with integrated systems, multiple missions.	Number of available aircraft/Total aircraft inventory.	Uptime/Total Time.	• Mission Reliability = flight hours / mission failures (e.g. operational mission failure, system abort) • Logistics Reliability = flight hours / failures
Ground Vehicles or Mobile Ground Systems	Wheeled or tracked platforms, either towed or self-propelled.	Number of available vehicles/Total vehicle inventory.	Uptime/Total Time.	• Mission Reliability = hours or miles / mission failures (e.g. system abort) • Logistics Reliability = hours or miles / failures
Weapons	Single use (e.g., air-launched weapons, missiles).	Number of available weapons/total weapon inventory. Repairable devices must include the pipeline or depot inventory.	Number of times system is available/ number of times system is required.	• Mission Reliability = successful launches / total launch attempts • Logistics Reliability = operating hours / failures **(Note 2)**
Satellite Systems (including hosted payloads)	Sub-types include an individual, single purpose satellite, a constellation of two or more satellites, and hosted payloads that share certain satellite infrastructure functions.	Unless unique circumstances exist (e.g., periodic software uploads), once the system is on-orbit Materiel Availability is not applicable.	Functional Availability: the probability of satisfying the minimum level of performance for a specific mission as a function of time. Typically expressed as a probability of success. **(Notes 3 & 4)**	• Mission Reliability: The probability of a satellite to perform a required function under stated conditions for a specified period of time. • Logistics Reliability = Not Applicable
Modification Programs	Replacement or upgrade of existing systems or subsystems. **(Note 5)**	Determine applicability dependent on existing system type.	Up Time/Total Time.	• Mission Reliability = operating hours / mission failures (e.g. operational mission failure, system abort) • Logistics Reliability = operating hours / failures
Subsystems	Clearly defined interfaces, installed in host platform.	Number of available subsystems /Total subsystem inventory.	Up Time/Total Time.	• Mission Reliability = operating hours / mission failures (e.g. operational mission failure, system abort) • Logistics Reliability = operating hours / failures
System of Systems or Unmanned Systems	Collection of distinct system elements that create a combined mission capability. (Define Am, Ao, Reliability parameters for each system element)	Number of available systems/ total system inventory.	Uptime/Total time.	• Mission Reliability = operating hours / mission failures (e.g. operational mission failures, system aborts) • Logistics Reliability = operating hours / failures **(Note 6)**

Notes:
1 More than one reliability metric may be specified as a KSA and/or an APA as appropriate. Mission Reliability is the measure of the ability of an item to perform its required function for the duration of a specified mission profile. Logistics Reliability is the measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment (All system failures regardless of impact to mission).
2 Weapons which are active/on during captive carry (aircraft platforms) or significant on-time (ship and ground launched systems) should consider a KSA for logistics reliability.
3 Hosted payloads: Functional Availability may also be a function of the reliability of shared infrastructure depending on the CONOPS.
4 Constellation: Functional Availability is a function of the reliability of the necessary minimum of satellites and the mission success criteria.
5 Modification Systems should consider the existing system requirements structure.
6 In the case for Unmanned Aerial Systems, the air vehicle would measure reliability in flight hours versus operating time.

Table D-D-2. Recommended Sustainment Metrics

DRAFT

APPENDIX E TO ENCLOSURE D

CONTENT GUIDE FOR THE NET-READY KPP

1. Overview

a. Usage. All IS will follow the NR KPP development process in accordance with this guide and reference iiii.

(1) This applies to all IS acquired, procured, or operated by any DOD Component, including but not limited to: national security systems (NSS), IS acquisition programs, information systems, IS initiatives, IS services, software, electronic warfare devices, DBS, prototypes as described in reference bb, commercial-off-the-shelf (COTS), leased, government off-the-shelf, rapid acquisition in support of validated JUONs, JEONs, and DOD Component UONs as described in reference gg, JCTDs, Coalition Warrior Interoperability Demonstration, CCMD Initiatives Fund (CCIF), IS systems and subsystems that are integral to embedded weapons platforms and non-POR materiel solution efforts.

(2) It does not apply to non-DODIN IT, including self-containted, or embedded IT that is not, and will not be connected to the enterprise network as defined by reference qqqq.

(3) The NR KPP identified in the CDD or CPD will also be used in the ISP to identify support required from external IS. When identified as applicable for a given capability requirement, the NR KPP is required for all program increments.

(4) To accommodate the initial review of the NR KPP for IS-ICDs, Sponsors will include an NR KPP table with initial minimum values in IS-ICDs.

b. Purpose. DOD Components must develop, acquire, test, deploy, and maintain IS that:

(1) Meet the essential operational needs of U.S. forces.

(2) Use architecture data and associated artifacts/views to develop the NR KPP that is:

(a) Certified in capability requirement documents in accordance with this manual.

(b) Reviewed in Information Support Plans (ISPs) in accordance with reference cccc.

(3) Are interoperable and supportable with previously fielded, developing, and proposed (pre-MS A) IS through architecture, standards, defined interfaces, modular design, and reuse of previously fielded IS solutions.

(4) Are supportable over the DODIN in accordance with reference dddd and eeeee.

(5) Are interoperable with host nation, multinational coalition, and federal, state, local, and tribal agency partners.

(6) Provide global authentication, access control, and enterprise directory services; provide information and services to the edge; utilize joint information environment operational reference architecture (JIE ORA); provide unity of command; and comply with common policies and standards in accordance with reference eeeee and fffff.

(7) Leverage emerging capability-based references and methods, including JCAs as described in this manual and references b and vvv, JMTs as described in reference ggggg, and the Joint Common System Function List (JCSFL) as described in reference hhhhh.

(8) Comply with spectrum requirements throughout the capability solution's life cycle.

(9) CCMDs, Services, and other DOD Components ensure capability solutions are aligned and interoperable during the development cycle.

(10) Comply with DOD Interoperability and Supportability (I&S) policy and instruction in accordance with reference cccc.

(11) Complies with DOD Cybersecurity policy in accordance with reference bbbbb.

c. Summary. Net-ready attributes determine specific criteria for interoperability, and operationally effective end-to-end information exchanges which are traceable to their associated operational context, and are measurable, testable, and support efficient and effective T&E.

(1) The NR KPP identifies operational, net-centric requirements in terms of threshold and objective values for MOEs and MOPs. The NR KPP covers all communication, computing, and EM spectrum requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service

exchanges. These exchanges enable successful completion of the warfighter mission or joint business processes.

(2) The NR KPP includes three attributes derived through a three step process of mission analysis, information analysis, and systems engineering. These attributes are then documented in solution architectures developed according to the current DODAF standard in reference ppp.

(a) Attribute 1: Supports military operations.

(b) Attribute 2: Is entered and managed on the network.

(c) Attribute 3: Effectively exchanges information.

2. Attribute Characteristics. General attribute descriptions and detailed steps to develop each attribute are provided below. Detailed directions to develop solution architectures for each attribute are provided later in this enclosure and in reference iiii.

a. Support military operations. This attribute specifies which military operations (e.g. missions or mission threads), as well as operational tasks, a system supports. Threshold and objective values of MOEs are used to measure mission success and are specific to the conditions under which a mission will be executed. Threshold and objective values of MOPs are used to measure task performance and the conditions under which the tasks are performed. Values must be presented in numerical form whenever possible. Since the NR KPP focuses on exchanging information, products, or services with external IS, these tasks may be net-centric operational tasks. Operational tasks are net-centric if they produce information, products, or services for or consume information, products, or services from external IS (including storing information on external IS).

b. Entered and managed on the network. This attribute specifies which networks the IS must connect to in order to support net-centric military operations. Reference iiiii provides guidance for network management to include standardization of objectives that should be used in the development of these attributes. The attribute must also specify performance requirements for these connections. To determine these performance requirements, answer the following questions in the context of the missions and tasks supported:

(1) To what types of networks will the IS connect? (this is more than internet protocol (IP) networks) Will the IS connect to mission partners, or those entities participating in the mission but not under the commander's direct authority? Examples include, but are not limited to, supported/supporting commands, non-DOD organizations such as the

Department of State or intelligence agencies, multinational partners, host nation civil authorities, international organizations, and non-governmental organizations.

(2) What MOPs do the required networks use to measure network entrance and management performance? This includes MOPs to measure the time from system start up to when the system is connected to the network and is supporting military operations.

(3) Who manages the system as it connects to various networks?

(4) How is the system managed? Will management be distributed, centralized, local, or remote?

(5) What configuration parameters does the network have?

(6) Will the IS provide an enterprise or mission service that will be accessed from a core data center or internet processing node?

c. Effective information exchanges. This attribute specifies the information elements produced and consumed by each mission and net-ready operational task identified above. Since the NR KPP focuses on a system's interactions with external systems, including potential interactions with allied, partner nation, and other US government agency/department systems, information elements the IS produces, sends, or makes available to external or joint interfaces and information elements the IS receives from external or joint interfaces are identified. For each information element, MOPs are used to measure the information element's production or consumption effectiveness. The NR KPP MOPs should also describe the information elements' continuity, survivability, interoperability, security, and operational effectiveness and how unanticipated uses are affected.

d. NR KPP Summary Table. Table D-E-1 summarizes the NR KPP attributes and their associated metrics in terms of a standardized framework and data sources to leverage when developing attributes and their threshold and objective values. Threshold and objective performance values should be represented in numerical form whenever possible to preclude subjective interpretation.

NR KPP Development Step	NR KPP Attribute	Attribute Details	Measures	Sample Data Sources	MOE/ MOP
Mission Analysis	Support to Military Operations	Military Operation (e.g., mission areas or mission threads)	MOEs used to determine the success of the military operation	JMETL, JMT, UJTL, and METL	MOE
			Conditions under which the military operations must be executed		
		Operational tasks required by the military operations	MOPs used to determine activity performance	JMETL, JMT, UJTL, and METL	MOP
			Conditions under which the activity must be performed		
Information Analysis	Entered and managed on the network	Which networks do the net-centric military operations require	MOP for entering the network	N/A	MOP
			MOP for management in the network	N/A	MOP
	Effectively exchanges information	Information produced and consumed by each military operation and operational task	MOP to ensure information exchanges are: Continuous Survivable Interoperable Secure Operationally Effective	DODAF OV-3, Operational Resource Flow Matrix	MOP
Systems Engineering and Architecture	Supports all three attributes	Ensures that IS satisfies the attribute requirements Accessed from the enterprise Which services do military operations require.	Provides traceability from the IS MOPs to the derived operational requirements Measures, Sample Architecture Data Sources and MOP	OVs, SVs, and SvcVs	N/A

Table D-E-1. NR KPP Development Example

e. Platform Integration Information Table (PIIT) Alternative. To simplify the NR KPP requirements for platforms, PMs and/or Resource Sponsors, in coordination with Joint Staff J6, may substitute the PIIT for the NR KPP table.

PLATFORM JCA (Tier 1/Other)	NR-KPP Attribute	Capability Contribution	Related ORD	Related CDD	Related CPD	NR-KPP Certification
JCA 1. Force Application 2. Command and Control 3. Battlespace Awareness 4. Net-Centric **KPP** 1. Net Ready **KSA** 4. Hosted Systems Integration	Support military operations	**Mission**: Command and Control (C2) of maneuver and support units **Measure**: The PLATFORM will support integration of the Joint Battle Command - Platform (JBC-P) for command and control applications **Condition**: KGV-72 encryption device	**JBC-P/BFT2** [no known ORD]	**JBC-P/BFT2** Joint Battle Command – Platform, Increment 2, Version 5, CDD, 06 Jul 2012	**JBC-P/BFT2** Waiver to use a revised CDD ILO CPD for MS C, JBC-P CDD Revision 2, final v 7, 23 Oct 12	**JBC-P/BFT2** [NR KPP Cert Date]
		Mission: Provide automated support for planning, coordinating, controlling and executing fires and effects **Measure**: The PLATFORM will support integration of the Advanced Field Artillery Tactical Data System (AFATDS) for fire support **Condition**: AFATDS current interface is not compatible with JTRS HMS Manpack or MNVR	**AFATDS** U.S. Army ORD for AFATDS, 23 Sep 1993	**AFATDS** Advanced Field Artillery Tactical Data System (AFATDS) Increment 2, CDD, Version 1.4, 06 Jun 2011	**AFATDS** [no known current activity]	**AFATDS** [NR KPP Cert Date]
JCA 1. Force Application 3. Battlespace Awareness 4. Net-Centric	Enter and be managed in the network	**Network**: Blue Force Tracking 2 (BFT2) network **Measure**: Must be able to enter the BFT2 network **Condition**: KGV-72 encryption device	**JBC-P/BFT2** [see previous reference]	**JBC-P/BFT2** [see previous reference]	**JBC-P/BFT2** [see previous reference]	**JBC-P/BFT2** [NR KPP Cert Date]
		Network: Upper tier Tactical internet Network **Measure**: Must be able to enter the Upper tier Tactical internet Network **Condition**: No special condition(s) noted	**WIN-T** [no known ORD]	**WIN-T** WIN-T CDD, v4.1, 16 Jun 06	**WIN-T** WIN-T Inc. 2 CPD, 25 Nov 2012	**WIN-T** [NR KPP Cert Date]
JCA 1. Force Application 3. Battlespace Awareness 4. Net-Centric	Exchange information	**Mission**: Exchange C2 data with JBC-P **Measure**: The PLATFORM will support C2 information exchanges with JBC-P required to support operations. **Condition**: KGV-72 encryption device	**JBC-P/BFT2** [see previous reference]	**JBC-P/BFT2** [see previous reference]	**JBC-P/BFT2** [see previous reference]	**JBC-P/BFT2** [NR KPP Cert Date]
		Mission: Exchange Mortar Fire Control System (MFCS) data with AFATDS or external observer **Measure**: The AMPV will support fire control information exchanges with AFATDS or external observer to support operations. **Condition**: MFCS current interface to external observer is not compatible with JTRS HMS Manpack	**MFCS** [to be updated for MS C]	**MFCS** [not done, technology mature and entered at MS C]	**MFCS** MFCS-LHMBC, CPD, Increment 1, Version 1.3, Feb 2009	**MFCS** [NR KPP Cert Date]

Table D-E-2. Example Platform Integration Information Table

(1) A platform is a vehicle, air, sea, or surface, structure, or person that carries, contains or includes multiple information systems. These systems may be integrated or interface within the platform to enable capabilities to perform the platform's assigned military mission. If the IS associated with a platform has interfaces or communicate with other systems, then in most instances the NR KPP is applicable.

(2) The PIIT is a listing of all of the IS associated with a platform that has received Interoperability Test Certification, NR KPP Certification, validated capability requirement document, or approved ISP. For each platform system, the PIIT provides the system name, nomenclature, JCAs, appropriate NR KPP attribute, certifying document (CDD, CPD, ISP, Interoperability Test Certification, and/or NR KPP Certification), and date of certification. Even if all components of a platform system are certified, the overall platform system must also be certified to ensure interoperability. Table D-E-2 is an example of the PIIT.

(3) PMs/Resource Sponsors should coordinate with the Joint Staff J6 for approval of their intent to use the PIIT in a capability requirement document or ISP. Additional details on the PIIT may be found at the URL in reference iiii.

3. NR KPP Functions. The NR KPP is used to address:

a. Requirements. Evaluate interoperability and net-centric requirements for the system.

b. Information Exchanges. Verify IS supports operationally effective producer to consumer information exchanges according to the validated capability requirements and applicable reference models and reference architectures.

c. MOEs and MOPs. Provide MOEs and MOPs to evaluate IS's ability to meet the initial minimum values, for requirements validated under an IS-ICD, or threshold and objective values, for requirements validated under a CDD or IS-CDD, when testing the system for joint interoperability certification.

d. Interoperability Issues. To enable assessment of capabilities and systems, architectures must align with and use the JCSFL. The architecture should also align, if applicable, with the DOD IEA, JIE ORA, Warfighting Enterprise Architecture (WEA), and existing Joint Mission Threads (JMTs). These alignments enable identification of potential interoperability disconnects with interdependent systems or services as well as detailed information exchange and information sharing strategies.

e. Compliance. Determine whether IS complies with network operations (NETOPS) for the DODIN direction, DODIN goals and characteristics, and is integrated into system development, in accordance with reference eeeee.

f. Spectrum Requirements. To obtain a NR KPP certification, all IS must comply with spectrum management and E3 direction. The spectrum requirements process includes joint, DOD, national, and international policies and procedures for the management and use of the EM spectrum. Details on compliance are available at the URL in reference iiii.

4. NR KPP Development. Unless defined as non-DODIN IT by reference qqqq, all IS require a NR KPP that specifies interoperability requirements which are traceable to their associated operational context, and are measurable, testable, and support efficient and effective T&E. Interoperability requirements include both the technical information exchanges and the operational effectiveness of those exchanges.

a. Primary Questions. NR KPP development uses a three step question / answer process to develop threshold/objective values for the NR KPP in a CDD or CPD, or initial minimum values for the NR KPP in an IS-ICD or IS-CDD.

(1) What military operations are being supported?

(2) What networks are being used?

(3) What information needs to be exchanged?

b. NR KPP Example. Table D-E-3 is an example of a completed NR KPP. Additional guidance on NR KPP development is available at reference iiii.

DRAFT

Attribute	Key Performance Parameter	Threshold	Objective
Support to military operations	Mission: Tracking and locating (Finding, Fixing, Finishing) High-Value Target (HVT)		
	Measure: Timely, actionable dissemination of acquisition data for HVT	10 minutes	Near-real-time
	Conditions: Targeting quality data to the neutralizing/tracking entity	Area denial of HVT activities	HVT tracked, neutralized
	Mission Activities: Find HVT		
	Measure: Absolute Location accuracy	100 meter circle at 90% confidence	25 meter circle at 90% confidence
	Conditions: Individual differentiation	Identify armed/not armed	Identify individual
Enter and managed in the network	Network: SIPRNET		
	Measure: Time to connect to an operational network from power up	2 minutes	1 minute
	Conditions: Network connectivity	99.8%	99.9%
	Network: NIPRNET		
	Measure: Time to connect to an operational network from power up	2 minutes	1 minute
	Conditions: Network connectivity	99.8%	99.9%
Exchange information	Information Element: Target Data		
	Measure: Dissemination of HVT biographic and physical data	10 seconds	5 seconds
	Measure: Receipt of HVT data	Line of Sight (LOS)	Beyond LOS
	Measure: Latency of data	5 seconds	2 seconds
	Measure: Strength of encryption	NSA certified type 1	NSA certified type 1
	Conditions: Tactical/Geopolitical	Permissive environment	Non-permissive environment

Table D-E-3. NR KPP Example

5. NR KPP Architecture Development Methodology. Architecture development enables development of the NR KPP. Architecture-based solutions, developed through a strict verification and validation process, are fundamental for improved interoperability, better information sharing, stricter compliance, and leaner processes. They also feed into system engineering processes and ultimately result in reduced life cycle costs and more effective mission accomplishment. Reference ppp describes the six-step architecture

development process for DOD which is shown in figure D-E-1. The six-step architecture development process supports the three-step of NR KPP development process described in this Guide. Solution architectures, conforming to the current DODAF standard, are developed, registered, and used as tools to improve joint operational processes, infrastructure, and solutions and to promote common vocabulary, reuse, and integration. Additionally, architecture development enables compliance with the NR KPP certification requirements. Figure D-E-2 shows the NR KPP development steps in relation to the JCIDS and acquisition processes.

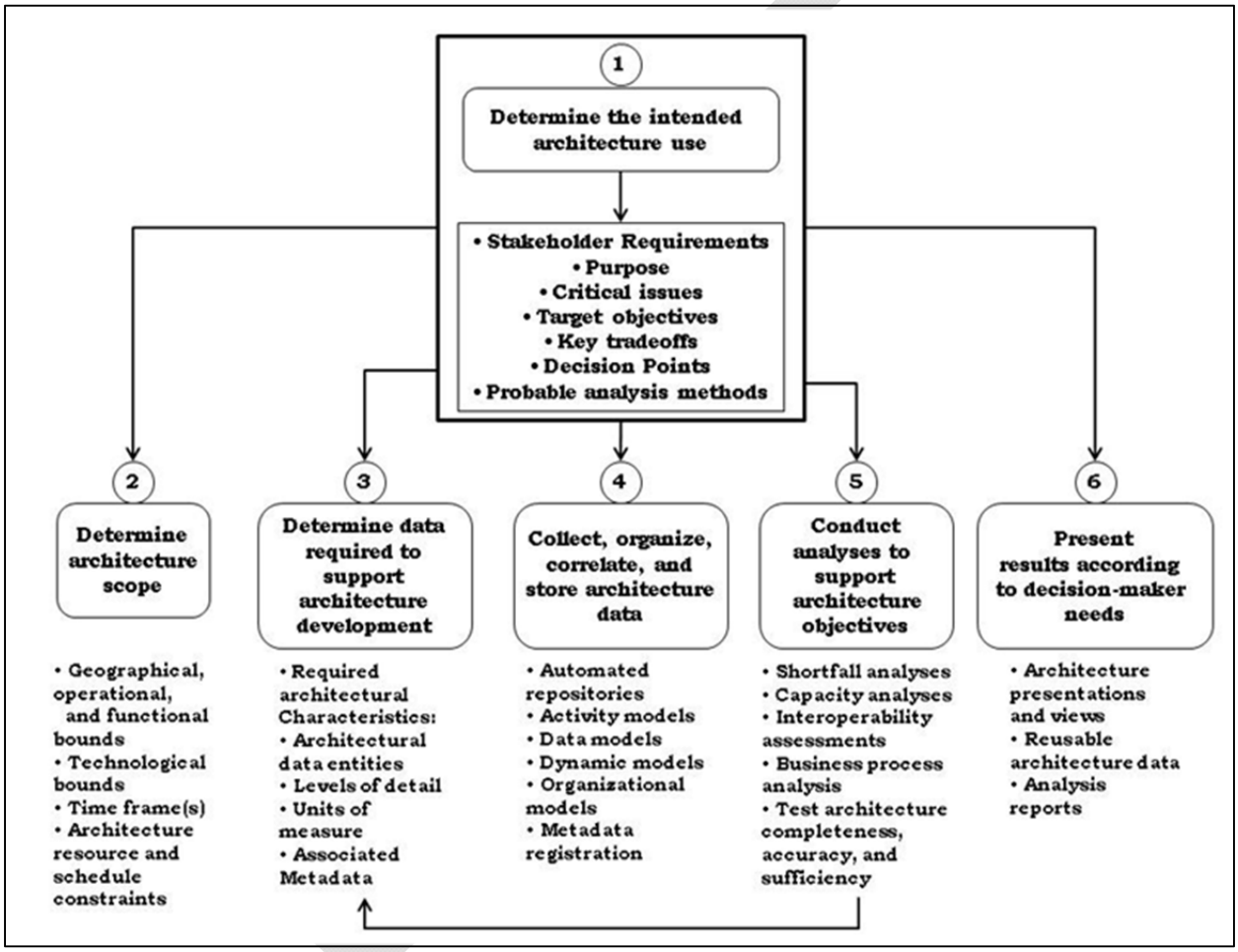

Figure D-E-1. DOD 6-Step Architecture Development Process

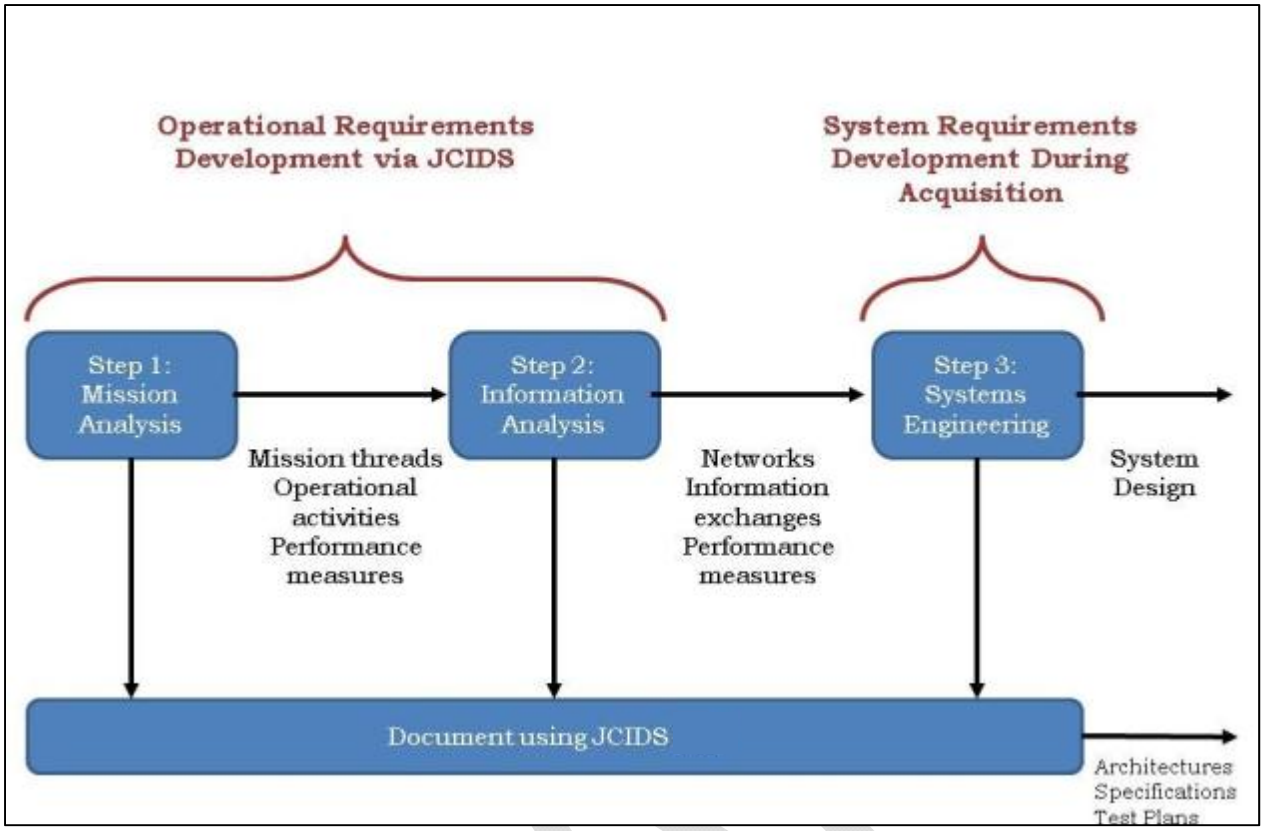

Figure D-E-2. NR KPP Development Applied to the JCIDS and Acquisition Processes

a. Background. With the release of DODAF version 2.0, the architecture focus switched from "products" to "data". Similarly, the NR KPP certification process changes NR KPP architecture development from an architecture product process to a data focus to enable analysis among programs, systems, and services. Architectures for NR KPP certification will be developed using the most current DODAF version or the optional NR KPP Architecture Data Assessment Template. Instructions for the NR KPP Architecture Data Assessment Template are at the URL in reference iiii.

b. DODAF Use for NR KPP. Develop architectures for NR KPP certification using the most current DODAF version. Previously generated architectures will be updated to the most current DODAF version before a successor document is submitted. Data sharing and data interoperability are enabled through architectures. In addition to required architecture data and associated artifacts/views identified in Table D-1 for all capability requirement documents, Table D-E-4 identifies additional artifacts/views for the NR KPP.

Document	AV-2	OV-2	OV-5b	OV-6c	DIV-1	DIV-2	DIV-3	PV-2	SV-1	SV-2 or SvcV-2	SV-4 or SvcV-4	SV-5a or SvcV-5	SV-6 or SvcV-6	SV-7 or SvcV-7	StdV-1	StdV-2
IS-ICD (RDPs/CPs)	S		S						S					P		
CDD/CPD	S/P	S	S	S	S	S	P	P	S/P	P	P	P	S/P	P	P	P
Note 1	The Sponsor uses the OV-4 and OV-5a, required by Table D-1 for all capability requirement documents, together with the OV-2 and SV-2 to determine if the NR KPP is applicable. In cases where the Sponsor proposes that the NR KPP is not applicable, the OV-2 and SV-2 will be provided to the certification authority for review along with the other DODAF views submitted in accordance with Table D-1.															
Note 2	S: The Sponsor, or operational user/representative, is responsible for development of the architecture data. S/P: The Sponsor, or operational user/representative, works jointly with the program office (depending upon program stage), to develop the architecture data. P: The sponsor, or operational user/representative should obtain this architecture data from the program office. DOD Component may have additional architectural/regulatory requirements for CDDs/CPDs. (e.g. – HQDA requires the SV-10c, USMC requires the SV-3, etc.)															
Note 3	The technical portion of the StdV-1 and StdV-2 are built using the DODIN Technical Guidance-DISR standards profiling resources and, within six months of submitting JCIDS documentation, must be current and published for compliance. Use of non-mandated DISR standards in the StdV-1 must be approved by the PM or other duly designated Component official and documented by a waiver notification provided to the DOD CIO.															
Note 4	The DIV-3 must identify system elements that support access to the data source by the DOD enterprise, including Web Service Description Language registration information, service end point, and DOD Meta Data Registry namespace identification.															

Table D-E-4. NR KPP Architecture Data and Associated Artifacts/Views

c. Architecture Tools. Produce architectures using a tool that focuses on architectural data rather than only upon individual artifacts/views. Use of COTS architecture tools that can collect, organize, and store the data, and make architecture data and associated artifacts/views available to the federated repository in a non-proprietary manner, is encouraged.

d. Submitting Architectures. Required architecture data and associated artifacts/views are submitted via a URL identified by the Sponsor in the reference section of the document. Architecture data formats and associated artifacts/views will support staffing, analysis, distribution, and reuse, and must be submitted in formats that can be viewed without specialized or proprietary tools so that it is accessible to and understandable by reviewers. See reference jjjjj for guidance on establishing compliant architecture repositories. DODAF PES compliant COTS tools are available with architecture data exchange standards, and should be used when possible to develop and

submit required architecture data and associated artifacts/views. When using Microsoft products or non-DODAF PES compliant architecture tools, Sponsors will use architecture data templates provided by appropriate mission area leads for submission of architecture data.

6. DOD IEA Alignment. The DOD IEA provides a common taxonomy and lexicon to describe required communications capabilities and align solution architecture with the DODIN as required by reference kkkkk. The DOD IEA provides the DOD-wide context and rules for IT solution architectures. Alignment with the DOD IEA and other relevant architectures provides context for solution architectures.

a. Architecture Alignment. Align solution architectures to the laws, regulations, and policies identified in reference p and according to the compliance criteria in the DOD IEA. Show linkage to parent EAs, and fit within Component and DOD architecture descriptions, using appropriate reference model and reference architectures (DOD IEA, JIE ORA, or WEA).

b. Activity Models. For aligning with DOD IEA, within the activity model, address activities and information inputs/outputs. This activity model will be built in compliance with the DOD IEA. Use DOD IEA activity names and descriptions to the maximum extent possible. An alternative method of compliance permits the use of system unique communications activities in the DODAF OV-5b, but requires a cross-walk table to the DOD IEA activities where a relationship exists and is included in the ISP.

c. NR KPP Information and Architecture Views. The NR KPP architectural developmental process and template is located at the URL in reference iiii.

7. Proponent. The NR KPP proponent is the C4/Cyber FCB. For questions, please contact the C4/Cyber FCB at 703-692-6529.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX F TO ENCLOSURE D

CONTENT GUIDE FOR THE ENERGY KPP

1. Introduction

a. Purpose

(1) This guide provides Sponsors, with support from the acquisition community, a guide to assist in developing Energy KPP values which affordably manage energy demand and related energy logistics and security risks without degrading mission effectiveness of the capability solution. While this guide does not prescribe an exact analytical methodology to establish Energy KPP attributes and values, it provides factors which should be considered to ensure the rationale being provided meets the rigor needed for critical review.

(2) The Energy KPP differs from other KPPs in several ways:

(a) Fuel delivery logistics (tanker aircraft, oilers, and fuel trucks) have a uniquely large presence in the total force structure and in the battlespace.

(b) Fuel, in the large volumes US forces demand it, and, in the timeframe when new systems will come into the force, may become less readily available for procurement in proximity to where it is required for operations.

(c) The Energy KPP does not focus directly on energy-related costs, but rather on mission effectiveness within the context of mission and threat.

b. Operational Implications of Energy

(1) The proliferation and improvement of adversary capabilities to threaten or deny lines of communication, coupled with growing fuel and electrical power demand across the joint force, means operational constraints on energy logistics must be included in the trade space for any new system that demands energy in operations. Further, there is an inherent opportunity cost to the Department and force structure in allowing logistics support, particularly energy-related delivery, to grow without analyzing the value of reducing the demand for their support. The same consideration applies to force protection for those logistics forces.

(2) The Energy KPP is intended to ensure combat capability of the force by balancing the energy performance of systems and the provisioning of energy to sustain systems/forces required by the operational commander in relevant threat environments. Energy performance is a key component of system and

unit performance, and relates to the energy consumption required to perform specific functions or tasks in specific operational modes, mission profiles/durations, and environmental conditions.

(3) The Energy KPP includes, but is not limited to, considerations for optimizing fuel and electric power demand in capability solutions, in the context of the logistical supply of energy to the warfighter, as it directly affects the demand on the force to provide and protect critical energy supplies. The Energy KPP includes both fuel and electric power demand considerations in systems, including those for operating "off grid" for extended periods when necessary, consistent with SSA products.

(4) In cases where energy demand reduction is impractical or insufficient to align with projected energy supply, complementary DOTmLPF-P changes to the energy supply chain and associated logistics capability solutions must be addressed in the document to accommodate the increased energy demands and satisfy the Energy KPP.

c. Applicability

(1) Although the Energy KPP is mandatory, not all programs or systems require full development of an Energy KPP. If a system does not use operational energy, or if energy consumption is not relevant to sustained performance over scenario timelines, the Sponsor may request a waiver of the Energy KPP, and include justification in the CDD or CPD as to why the Energy KPP is not applicable.

(2) See Appendix F to Enclosure F of this manual for details of the review criteria and endorsement process for the Energy KPP by the applicable endorsement authority identified in Enclosure E of this manual.

2. Energy Supportability Analysis

a. General Considerations. Analysis of the system's use of energy to accomplish mission requirements should form the basis of all energy performance attributes and the Energy KPP. This analysis should serve to expose energy demand and supply relationships and thereby influence system design considerations and KPP development.

(1) Energy performance is a key component of system and unit performance, and relates to the energy required to perform specific functions or tasks in specific operational modes, mission profiles, and environmental conditions. Energy KPP values establish the energy performance threshold and objective values for a capability solution, and are derived from the operational

requirements of the system, scenario-based assumptions for its operational use, and the planned logistical and force protection support to sustain it.

(2) Initial analysis should be performed during the concept development phase, using independent energy analysis or the capabilities-based assessment to optimize future system effectiveness. Identifying energy performance considerations "upfront" enables the acquisition and requirements communities to make decisions which balance energy demand and energy supply with other elements of performance, enabling optimal capability solutions for the warfighter.

(3) The analysis should be framed by explicit assumptions such as realistic threat and operations tempo, consistent with the DIA- or Service-approved threat products used for the threat summary section of the capability requirement document.

(a) The analysis underpinning the Energy KPP must be scenario-based, must use the logistics assets programmed for the future force, and should use the most stressing scenario, from an energy demand perspective, outlined during development of the AoA or similar study. The analysis must be derived from SSA products that include not only operation of the system in question but also the energy-related logistics and force protection required in contested operational domains, including considerations for operating "off grid" for extended periods when necessary. All SSA products used by the program for this analysis must be of sufficient duration (multiple days to weeks) to demonstrate the effect of realistic opponent effects on the US and/or coalition logistics force. Such analysis is required because kinetic and non-kinetic capabilities to potentially counter logistics are proliferating and because operational experience has shown the inherent vulnerability and opportunity cost of employing and protecting large logistics forces in contested domains.

(b) The scenario analyses, therefore, must include the logistics forces required as well as realistic threats and disruptions to those logistics. The scenario must account for availability of logistics assets, non-hostile attrition (including reliability), and attrition due to red action against blue logistics systems. Some of the same scenario-based analysis used for the CONOPS or AoA may be leveraged to set Energy KPP thresholds and objectives. This interplay of combat and support forces, based on DOD Component and joint planning factors and SSA products, will help identify the Energy KPP attributes required to be mission capable. It is from these operational metrics that technical system metrics can be established.

b. Three part methodology

(1) The first part of the methodology is to analyze the energy supply capacity available to the entire unit of maneuver, considering other consumers of the same energy logistics. Energy supply capacity is not a single number, but an accounting of the future capacity of the supply chain to deliver energy to the future unit of maneuver over time during the scenario.

(a) The analysis should expose the energy demands of the system during its mission profile in the interval between refueling/recharging events. For all systems, the interval between refueling/recharging events is determined by the tempo and availability of refueling assets as modeled in the context of the most stressing validated operational level scenario.

(b) The analysis should address the ability to transport, distribute, store, and protect the energy supply within the scenario. Specifically, the analysis should consider:

1. Duration of the mission profile for the platform under consideration, using the most stressful scenario from an energy demand perspective

2. Force Structure (to include projected future force structure of scenario and associated support systems across the full unit of maneuver)

3. CONOPS and TTPs

4. Adversary threat to energy logistics assets, and force protection assets required as mitigation

(2) The second part of the methodology involves looking at the energy demands of the platform, the unit of maneuver, and other consumers of the same energy logistics. This analysis should examine the desired performance of the system and its impact on energy sources, either as a receiver (drawing energy from other systems) or as a provider (supplying energy to other systems). Understanding provider/receiver energy relationships and integration requirements of a system is important to scoping the supportability analysis and for refining the energy performance attributes in the operational context, as outlined in with Figure D-F-1.

(a) The system must be considered as a potential end-user; this means that its propulsive, heating and cooling, sensing and firing systems all bear on the energy consumed by the platform as it transports itself and its payload and defends itself.

(b) The system must also be potentially considered as one node in an energy distribution network, in which the platform may function as an

energy provider to receiver systems which are dependent on the platform's store of energy. These potential receiver systems could broadly range from embarked weapons systems (i.e. LCACs, LCUs, helicopters, aircraft, ground vehicles, etc.) to serviced weapon systems (i.e. refueled ships, aircraft underway or in-flight) as well as intrinsic energy demanding components such as radars which must necessarily draw their energy demand from the energy providing platform to complete their mission. The distinction between energy provider and receiver is important when determining how to apply the Energy KPP. Systems which must function as both may require an Energy KPP for each role.

(c) For programs which seek to replace a subsystem, such as an engine upgrade or addition of a drag reduction device such as winglets to a legacy platform, the energy performance comparison can be stated as a % improvement over the legacy system. This comparison must be based on identical missions under identical threats. Testability can be simplified by specifying developmental test conditions under which the legacy subsystem performance is well documented.

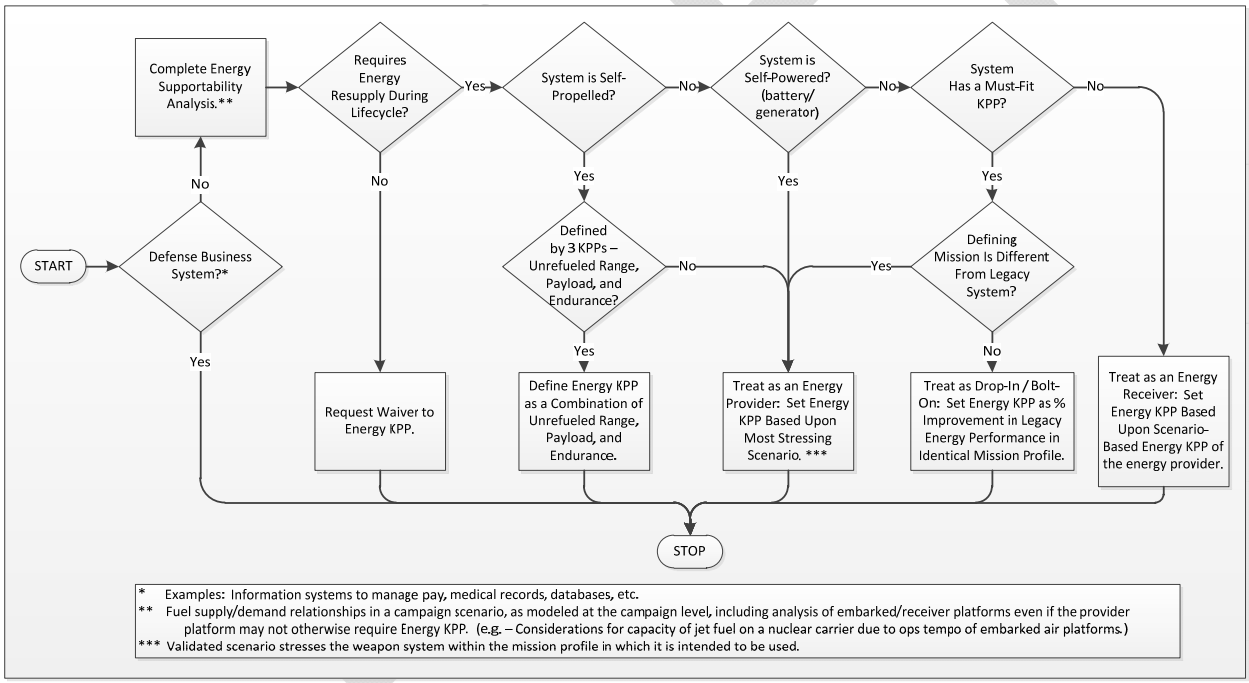

Figure D-F-1. System Roles for the Energy KPP.

(3) The third part of the methodology is to analyze the difference, in the context of the scenario and the threat, between the capacity to supply energy and the energy demand. How this difference is addressed will assist in determining the key attributes to be included in the Energy KPP, and their associated threshold and objective values. The energy supportability analysis will ultimately identify energy performance attributes that directly affect the system's ability to perform its mission. In turn, these energy performance

attributes, when related directly to the system's mission effectiveness parameters, will frame the system's Energy KPP attributes.

(a) The design, technology, life cycle cost, schedule, and quantity trades between each variable that affects energy demand on-board (powerplant, weight, drag, electrical load, etc.) can be used to derive the threshold and objective values for system energy performance.

(b) A Sponsor may find that the required performance of the platform from step two above is not possible given current technological state of the art, the performance limits of a previously fielded platform being modified, or other limiting factors. When the fuel allocation for the weapon system is insufficient given the constraints of the scenario and the technology of the system, the Sponsor must find a means to correct the imbalance. This reinforces the need for a scenario-based analysis for the Energy KPP.

(c) Sponsor options to balance a supply and demand may include decreasing consumption through greater platform efficiency, reducing the number of platforms in the unit of maneuver, increasing the capacity of the supply chain (i.e., increase logistics assets), changing the scheme of maneuver, or modifying CONOPS or TTPs. In cases where a platform consumes more energy than its predecessor, or has no predecessor, a Sponsor must address complementary DOTmLPF-P change(s), including associated resources required to implement the changes, which accommodate the consumption increase above what the energy supply chain can provide.

(d) Regardless of the approach, the Sponsor must balance the planned consumption of the unit of maneuver with the capacity of the supply chain providing energy to the unit of maneuver, considering other consumers of the same energy logistics. Increases in system energy consumption should be mitigated to the maximum extent practicable.

3. Energy Performance Attributes

a. Energy performance attributes relate energy consumed by the system to the operational effect produced by that consumption. Those selected should be the most critical to the mission effectiveness of the system.

(1) Provider Systems. Provider systems include any system that supplies energy to other systems. Sponsors of provider systems may consider potential energy performance attributes that include but are not limited to the following, in order to facilitate development of their Energy KPPs:

(a) Payload-ton-miles/gallon or Payload-ton-miles/kWh where payload weight and combat range are important to mission effectiveness

(b) Payload-ft3-miles/gallon or Payload-ft3-miles/kWh where payload volume and combat range are important to mission effectiveness

(c) Energy consumed (gallons, kWh) per unit of mission accomplished (e.g., square miles of ocean swept for mines at the required depth and level of effectiveness; required targets detected, tracked and engaged at specified range/conditions, etc.)

(d) Energy (gallons, kWh) consumed between refueling events as the system and any receiver systems complete their most stressful, most energy-consuming mission profile

(e) Energy capacity (gallons, kWh) supplied to receiver systems where the provider system is expected to be the sole source over a critical period of time

(2) Receiver Systems. Receiver systems draw energy from their provider systems. Sponsors of receiver systems may consider potential energy performance attributes that include but are not limited to the following, in order to facilitate development of their Energy KPPs:

(a) Energy capacity (gallons, kWh) drawn from the provider over a critical period of time, where the provider is the sole energy source

(b) Energy consumed (gallons, kWh) per unit of mission accomplished (e.g., square miles of ocean swept for mines at the required level of effectiveness, required targets detected, tracked and engaged at specified conditions, etc.)

(c) Peak power demand or maximum fuel delivery rate imposed by receiver systems on their energy provider, where surges of receiver system performance are important to mission effectiveness

(3) Drop-In/Bolt-On Systems or Sub Systems. For programs that seek to replace a powertrain component such as an engine in a legacy platform, or add a drag reduction device such as winglets to a legacy platform, the energy performance comparison can be stated as a percentage improvement over the legacy system, with the comparison based upon identical mission profiles. Sponsors of systems that are being integrated into a legacy platform may consider potential energy performance attributes that include but are not limited to the following, in order to facilitate development of their Energy KPPs:

(a) Ratio of power transmitted to power supplied (kW:kW, HP:HP; can be expressed as percentage) where a subsystem is proposed as a drop-in/bolt-on replacement in a power train.

(b) Drag reduction or propulsive effectiveness gain (decrease in gallons per ton-mile, percentage difference in range/payload or endurance) where a component affects cruise performance.

(c) Thrust-specific or HP-specific fuel consumption improvement.

b. Relationship with other performance attributes. Performance attributes of the system or network that do not address both energy and performance are not considered energy performance attributes. For example, for a radar system the peak power demand that the radar imposes on its host ship/aircraft/vehicle in a specific radar mission mode is an energy performance attribute. Likewise, the ratio of electrical energy the radar demands to the energy emitted from the radar antenna in a specific mission mode is an energy performance attribute. However, the radar's detection range and discrimination accuracy by themselves are not considered energy attributes.

c. Testability. Selection of Energy KPP attributes should take into account any testability issues, and be selected in a way that supports cost effective evaluation. For example, to demonstrate compliance with an attribute that relates energy demand to performance stated in terms of probability, the Sponsor must coordinate with the DOT&E community to determine the required combination of testing and parametric modeling.

4. Proponent. The Energy KPP proponent is the Joint Staff J-4 / Engineering Division (J-4/ED), with analytical support from the office of the Assistant Secretary of Defense (ASD) for Operational Energy Plans and Programs (ASD(OEPP)). For questions regarding the Energy KPP, contact J-4/ED at 703-697-4445.

DRAFT

APPENDIX G TO ENCLOSURE D

CONTENT GUIDE FOR THE TRAINING KPP

1. Overview

a. Purpose. The Training KPP is intended to ensure that materiel aspects of training capabilities, when applicable, are addressed as part of the development of the capability solution outlined in the CDD or CPD. Non-materiel aspects of training are to be captured as part of the DOTmLPF-P section of the CDD or CPD, in accordance with Appendix H to Enclosure D of this manual.

b. Applicability. The Training KPP is applicable to all CDDs and CPDs with materiel training requirements which dictate specific operational performance characteristics of the capability solution.

2. Situations Requiring Training KPP Content

a. Specific materiel performance requirements

(1) An illustrative example is the long mission durations of submarine operations, which may necessitate that the warfighter use the Training KPP to specify certain training and simulation capabilities be integrated into the weapon system. If not able to properly train during operational missions, warfighter performance may be degraded.

(2) Other weapon systems with shorter operational mission durations may have more flexibility to adopt training approaches. In these cases, the most appropriate training approach can be determined by training specialists and the warfighter does not need to set requirements for a particular training approach, such as integration of specific training capabilities into the operational weapon system.

b. Mission of the system is training

(1) The “mission” of some systems is solely the training of personnel who will use a different operational weapon system. For example, use of the T-38 aircraft as a trainer for more advanced aircraft, or use of a flight simulator to substitute for some aspects of training when training events in the actual aircraft would be too dangerous to perform or when events are more cost effective to execute in the simulator.

(2) In these cases, the KPPs (and KSAs and APAs) of the training system must be specified to properly replicate some or all of the performance

aspects of a different system in order to conduct the appropriate level of training.

3. Proponent. The DOTmLPF-P proponent is the Joint Staff J-7, Joint Integration Branch (J-7/JIB), on behalf of the Joint Staff J-7 Deputy Director for Integration (J-7/DDI). For questions, please contact the J-7/JIB at 703-692-0785.

DRAFT

APPENDIX H TO ENCLOSURE D

CONTENT GUIDE FOR DOTmLPF-P

1. Overview

a. Purpose. The purpose of the DOTmLPF-P content in capability requirement documents is to address:

(1) In ICDs and DCRs: Non-materiel approaches that can provide a non-materiel capability solution to capability requirements and which partially or wholly mitigate associated capability gaps.

(2) In CDDs and CPDs: Non-materiel enablers to materiel capability solutions identified in CDDs and CPDs, without which the materiel capability solution cannot be successfully fielded.

b. Usage. This content serves as the basis for the Joint Staff Directorate for Joint Force Development (J-7) DOTmLPF-P review and endorsement described in Appendix H to Enclosure F of this manual.

c. Applicability. Sponsors must address all DOTmLPF-P considerations in capability requirement documents unless not applicable in a particular case. In cases where one or more of the DOTmLPF-P factors may not applicable, the Sponsor shall coordinate with the applicable organization identified in Appendix H to Enclosure F of this manual to ensure that the DOTmLPF-P endorsement is not withheld due to missing information.

d. Coordination with other processes. Implementation of changes to DOTmLPF-P validated in the JCIDS process may require coordination with other impacted organizations and processes as outlined in Appendix H to Enclosure F of this manual. Sponsors are encouraged to coordinate proposed changes with impacted organizations during document development to facilitate timely staffing and validation.

2. Section Content

a. Doctrine

(1) Identify the specific joint or service publications that are applicable and need to be reviewed.

(2) Identify if current doctrine allows the capability to be utilized to its fullest potential. Describe why existing doctrine is insufficient, or reference in the CBA or other study where such a description was provided.

(3) Identify the changes that would be needed in designated joint or service publications to describe how the recommended capability should be captured in doctrine. Identify the OPR(s) for any proposed doctrinal change.

(4) Ensure changes to doctrine are made in accordance with the process outlined in reference ww and any applicable Service doctrine process.

b. Organization

(1) Identify if current organizational structures allow the capability to be utilized to its fullest potential.

(2) If changes to organizational structures are an enabler to implementation of the capability, or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

(3) If costs are associated with organizational changes, ensure that associated costs are captured in resource estimates.

(4) Changes to organization must adhere to the process outlined in reference xx and any applicable Service organization process(es).

c. Training. Training must be properly addressed from the beginning of the acquisition process, integrated with the planning and materiel development, and updated throughout the capability solution's life cycle. Non-materiel aspects of training are addressed in this section of the DOTmLPF-P content. Aspects of training which require specific performance attributes of the materiel capability solution are addressed in the Training KPP in accordance with the content guide in Appendix G to Enclosure D of this manual.

(1) Outline recommended and required training that will enable effective implementation and performance of the capability solution, including training considerations which address concerns documented in reference lllll, and characterized by reference mmmmm.

(2) Training implications are considered in the CBA and the AoA or similar study, where training implications may drive projected life cycle cost of the system or where training costs may be a discriminator between different alternatives pursued. Training not planned, adequately funded, and integrated early, has the potential to be a significant life cycle cost driver for a program, or contribute to a lack of readiness when the system is fielded. This action ensures training and resourcing information is incorporated early in program

planning, enables comparison of life cycle cost, schedule, performance, and quantity, and facilitates development of an optimal solution providing greatest enhancement of user capabilities.

(3) The following questions can assist in determining the importance of training for a specific capability solution. An answer of "yes" to several of these questions suggests how and where training may be relevant.

(a) Is successful application of the system's capabilities critically dependent upon a rigorous training process early on to maximize system capability with the first unit equipped (FUE)?

(b) Are training costs over the capability solution's life cycle a significant part of the projected life cycle costs?

(c) Is a stand-alone system training device or training capability required to support training within integrated live, virtual, or constructive environments to support the program?

(d) Is early system training critical to future program success?

(e) Was the program designated a JUON, JEON, or DOD Component UON, or is it transitioning from a technology initiative such as a JCTD or experiment, where training considerations might not have been robustly addressed?

(f) Are there program inter-dependencies between two or more programs?

(g) Is a system schoolhouse capability required to train to a complex man-machine interface, SoS operation, or maintenance concept?

(h) Does the COTS/GOTS hardware or software integral to the program require a training solution that is not already part of the COTS/GOTS product?

(i) Is embedded training and/or instrumentation feasible and appropriate as part of a stand-alone system training device or as part of integrated live, virtual, or constructive environments? (i.e. - training accomplished through the use of the operational system within a live virtual constructive training environment.)

(j) Will realistic live training be restricted by life cycle cost, environmental, or safety concerns, increasing the reliance on integrated live virtual or constructive training capabilities?

(k) Is there a cost benefit to transitioning certain live training activities to integrated live virtual or constructive training capabilities, while maintaining training capabilities?

(4) Changes to training must adhere to the process outlined in reference yy and any applicable Service training process(es).

d. "Little-m" materiel

(1) Identify any previously fielded materiel required as part of the capability solution or as an enabler to allow the capability solution to be utilized to its fullest potential. Previously fielded materiel may be leveraged in either their original capacity or in an adaptation or repurposing not originally envisioned.

(2) If changes to previously fielded materiel are an enabler to implementation of the capability, or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

(3) If costs are associated with additional quantities or repurposing of previously fielded materiel, ensure that associated costs are captured in resource estimates.

(4) Changes to "little m" materiel must be coordinated with the affected Sponsors.

e. Leadership and education

(1) Identify if current leadership and education allows the capability to be utilized to its fullest potential.

(2) If changes to leadership and education are an enabler to implementation of the capability, or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

(3) If costs are associated with leadership and education changes, ensure that associated costs are captured in resource estimates.

(4) Changes to leadership and education must adhere to the processes outlined in references zz and aaa and any applicable Service leadership and education process(es).

f. Personnel

(1) Identify if current manning – both quantity and type – allows the capability to be utilized to its fullest potential.

(2) If changes to manning are an enabler to implementation of the capability, or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

(3) If costs are associated with manning changes, ensure that associated costs are captured in resource estimates.

(4) Changes to personnel must adhere to the process outlined in reference bbb and any applicable Service personnel process(es).

g. Facilities

(1) Identify if current facilities allow the capability to be utilized to its fullest potential.

(2) If changes to facilities are an enabler to implementation of the capability, or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

(3) If costs are associated with facility changes, ensure that associated costs are captured in resource estimates.

(4) Changes to facilities must adhere to the processes outlined in references ccc and ddd and any applicable Service MILCON processes.

h. Policy

(1) Identify if current policy allows the capability to be utilized to its fullest potential.

(2) If changes to policy are an enabler to implementation of the capability, or would allow greater efficiency or performance of the capability, outline the changes that are recommended or required.

(3) Changes to policy must adhere to the process outlined in reference eee and any applicable Service policy processes.

3. Proponent. The DOTmLPF-P proponent is the Joint Staff J-7, Joint Integration Branch (J-7/JIB), on behalf of the Joint Staff J-7 Deputy Director

for Integration (J-7/DDI). For questions, please contact the J-7/JIB at 703-692-0785.

DRAFT

APPENDIX I TO ENCLOSURE D

CONTENT GUIDE FOR INTELLIGENCE SUPPORTABILITY

1. Overview

a. Purpose. This guide provides general descriptions of intelligence support requirement categories to assist Sponsors and commenters with the identification of intelligence support requirements and sufficiency or risk of shortfalls in intelligence infrastructure required to support a capability solution.

(1) The descriptions of intelligence support requirement categories are not all-inclusive. Sponsors should tailor the categories to satisfy each capability solution's unique intelligence support requirements.

(2) Sponsors must consider and identify support requirements, or state there are no requirements, for each category in the Intelligence Supportability section of capability requirement documents. Sponsors must also identify requirements across the capability solution's life cycle, trace requirements to impacted KPPs, KSAs, and APAs, where applicable, and articulate potential coordination between materiel and non-materiel solutions.

b. Review. Intelligence support requirements will be reviewed by subject matter experts from DoD and Service intelligence organizations for supportability prior to granting intelligence certification. Sponsors should engage their supporting intelligence entities at the earliest stages of development to ensure understanding of the requirements to be levied against the IC.

c. Certification. This guide also provides context for assessing capability solutions during the intelligence supportability review process in support of DIA/TLA threat assessment and intelligence certification outlined in Appendix I to Enclosure F of this manual.

2. Category Descriptions. A list of supportability categories follows to assist the Sponsor in identifying areas where a capability solution will likely need support.

a. Intelligence Manpower Support

(1) This category should be addressed if the capability solution will require intelligence personnel for development, testing, training, and/or operation. Depending on the maturity of the capability solution, a Manpower Estimation Report (MER) may have been completed. If a MER shows that

intelligence manpower changes will be required to support the fielding of the capability solution, a summary of intelligence implications from that report should be included in this support category.

(2) Address whether existing skills and specialties suffice, or if specific skills are required for support. Address how existing intelligence manpower resources will meet the capability solution's intelligence support requirements or whether the capability solution will require additional, dedicated intelligence personnel from within the sponsor's organization, by leveraging support from other organizations, or by training new personnel to fill the anticipated support requirements.

b. Intelligence Resource Support

(1) This requirement category should be addressed if the capability solution or supporting efforts will require, or depend upon, intelligence funding. Specific attention must be given to the requirement for IMD early in the capability life cycle, including the consideration of resourcing for IMD production prior to MS A.

(2) Address whether, and to what extent, the capability solution relies upon intelligence capabilities that have not yet been provided dedicated funding, or have not received necessary approvals to begin operations or remain operational.

c. Intelligence Planning and Operations Support. This category includes support requirements related to the six interrelated categories of intelligence operations included in the Joint Intelligence Process (planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and, evaluation and feedback), and support requirements from the different intelligence disciplines. Sponsors should address interoperability requirements in each Joint Intelligence Process step and intelligence discipline, where applicable.

(1) Planning and Direction

(a) This category includes the receipt, identification, and prioritization of intelligence requirements; the development of concepts of intelligence operations and architectures; tasking appropriate intelligence elements for the collection of information or the production of finished intelligence; and, submitting requests for collection, exploitation, or all-source production support to external, supporting intelligence entities.

(b) Sponsors must address whether mission planning requirements have been considered and identified, to include manpower, systems, tools,

mission planning data (Red, Gray, Blue, and White) or other non-materiel requirements at intelligence units, personnel training on systems architecture, and compatibility with current and future DI2E architecture.

(2) Collection

(a) Collection includes those activities related to the acquisition of data required to satisfy specified requirements. This is managed by collection managers, whose duties include selecting the most appropriate, available asset(s) and associated processing, exploitation, and dissemination (PED) and then tasking selected asset(s) and associated PED to conduct collection missions.

(b) Collection management support refers to the personnel, expertise, training, and systems required to ensure intelligence information requests are submitted through the appropriate channels; that intelligence collection assets (e.g., Service, national, joint, coalition, multinational) are effectively employed to collect the information required; and that the collected information is disseminated to the entity that made the original request and to all other end users requiring such information.

(c) Collection also includes support that the capability solution will require from the different intelligence disciplines:

1. Signals Intelligence (SIGINT), to include communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). SIGINT support should include any requirements for intelligence produced by exploiting foreign communications systems and non-communications emitters.

2. Human Intelligence (HUMINT). The category of intelligence derived from information collected and provided by human sources.

3. Measurement and Signature Intelligence (MASINT). MASINT is information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify them. MASINT techniques are used to support signature development and analysis, to perform technical analysis, and to detect, characterize, locate, and identify targets and events. MASINT is derived from specialized measurements of physical phenomena intrinsic to an object or event, and it includes the use of quantitative signatures to interpret the data. The measurement aspect of MASINT refers to actual measurements of parameters of an event or object such as the demonstrated flight profile and range of a cruise missile. Signatures are typically the products of multiple measurements collected over time and under varying circumstances. These signatures are used to develop

target classification profiles and discrimination and reporting algorithms for operational surveillance and weapon systems.

4. GEOINT. GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. GEOINT consists of imagery, imagery intelligence, and geospatial information. The DOD functional manager for GEOINT is the National Geospatial-Intelligence Agency (NGA).

a. GEOINT provides two irreplaceable components that contribute to the effectiveness of weapons and weapon systems: a framework that renders other intelligence actionable by virtue of referencing it to a four-dimensional space-time context; and, critical qualitative and quantitative information to describe the physical and functional characteristics of the political, economic, military, social, informational, and infrastructure components of an enemy's capabilities. The fusion of imagery-based intelligence (to include imagery-based MASINT) with geospatial information to create GEOINT conveys understanding of enemy assets and actions that play a dominant role in determining weapon and weapon system effectiveness. Early and concise identification of GEOINT shortfalls for planning and execution to optimize weapon and weapon system effectiveness is a matter of critical concern when NGA must justify requirements for resources and apportionment of those resources within the agency. An example of such GEOINT shortfalls would be the identification of routine data exploitation and production requirements for specific construction details of buildings that affect the performance of miniaturized munitions. Another example would be concise description of man-made features and demographic distributions in urban areas where planned operations must consider high-fidelity estimation of collateral damage risks.

b. To fulfill geospatial requirements for their capability solutions, Sponsors must comply with the processes and milestones identified in references nnnnn and ooooo to accommodate the planning, allocation, and de-confliction of geospatial information and services (GI&S)-related collection, analytic, and dissemination resources that are consistently in high demand. In accordance with reference nnnnn, all programs must use GEOINT data whose content, formats and standards conform to those established through the National System for Geospatial Intelligence governance processes. Systems which require unique GEOINT products and services must identify those requirements within capability requirement documents to ensure the products and services transition into the acquisition process. New or upgraded systems which require an increase in coverage or production capacity from the NGA baseline must also forecast the requirements within the JCIDS process. Because of the potential resource demands of these support requirements and

their resulting effect on the GEOINT community, requirements must be qualitatively and quantitatively identified at the earliest possible point in the JCIDS process and updated in accordance with reference nnnnn. Details include the required data, coverage, scale, timeliness, formats, numeric quantity of products, accuracy, resolution level (e.g., imagery and/or Digital Terrain Elevation Data (DTED) levels) and necessary update requirements (periodic versus as-needed).

(d) Address requirements for appropriate collection management resources, tools and infrastructure, and level of national/coalition interoperability to support the capability solution. Address types of intelligence information needed (form and substance), specific collection asset(s) or collection asset capabilities that will be needed to collect the requested information, and compliance with data and metadata standards. Address what intelligence information the capability solution will require during its life cycle.

(3) Processing and Exploitation

(a) Data initially received from the sensor arrives in various forms depending on the nature of the sensing device. Depending on the source, the raw input may be in the form of digitized data, unintelligible voice transmissions, or large digital files containing un-rectified images of the Earth. This collection output is converted by sensor-specific processing measures into visual, auditory, or textual information that is intelligible to humans, and which can then be used by intelligence analysts and other consumers. The data conversion may be automated using algorithmic fusion, cuing, data analytics and automated exploitation. Exploitation entails the further translation and contextualizing of information resulting from collection and initial processing into a product that the planner, decision maker, or intelligence analyst can cognitively assimilate. Exploitation efforts will vary greatly by specific products required; examples should include format specifications, accuracy requirements, and production timeline requirements.

(b) Address whether sufficient personnel and resources will be in place for effective processing and exploitation. Where possible, address required data, coverage, scale, timeliness, formats, accuracy, resolution level (e.g., imagery and/or DTED levels). Consider whether the intelligence architecture will support the volume of data requiring processing. Ensure data is in standard formats to support interoperability. Dependent upon the specific requirements of Sponsor's capability solution being supported, consider types of delivery/communications systems required and volume of information that will be delivered. In addition, see the section below on targeting support, for exploitation requirements supporting targeting and coordinate-seeking weapons.

(4) Analysis and Production

(a) During analysis and production, intelligence is produced from the information gathered by collection capabilities, and from the refinement and compilation of intelligence received from external organizations. All available processed information is integrated, evaluated, analyzed, and interpreted to create products that will satisfy users or requesters. Intelligence products can be presented in many forms; they may be oral presentations, hard copy publications, or electronic media accomplished by units and organizations at every echelon, and including reach back locations. Whereas collection, processing, and exploitation are primarily performed by specialists from one of the major intelligence disciplines, analysis and production is done primarily by all-source analysts that fuse together information from all intelligence disciplines.

(b) Intelligence products are generally placed in one of eight production categories: warning, current, general military, target, S&T, CI, identity intelligence, and estimative intelligence. The categories are distinguished from each other primarily by the purpose for which the intelligence was produced. The categories can and do overlap, and the same intelligence and information can be used in each of the categories.

(c) Address the necessary or desired product format (electronic versus paper), production timeline and necessary update requirements (periodic versus as-needed) will be available and have been requested to support their capability solutions. Consider whether sufficient personnel and resources will be in place for effective analysis and production.

(5) Dissemination and Integration

(a) The timely distribution of critical information and finished intelligence to appropriate consumers, readily accessible by the user. The movement toward a net-centric environment has reduced the technical challenges related to information dissemination. Nevertheless, intelligence infrastructure (such as intelligence networks, systems, and software) and intelligence resources (such as funded programs or manpower) remain critical (and necessary) components of information delivery. Another measure of dissemination support is compliance with IC and DOD data and metadata standards. Personal, networked, and database data transfers are all means of dissemination. The diversity of dissemination paths reinforces the need for communications and computer systems interoperability among joint and multinational forces, component commands, DOD organizations, and the interagency community.

(b) Address the specific requirements of the capability solution being supported, which may include: timeliness and means of delivery, interoperability of delivery/communications systems (to include requirements for interoperability with coalition and other organizations' systems), format of information delivered (to include compliance with data and metadata standards), and information/product storage location, capacity and accessibility.

(c) Identify all security requirements or considerations needed to support the capability solution, and address how those security considerations will be satisfied. Ensure classification levels; information sharing or releasability; certifications, and facility implications for receiving, using, and storing data; are addressed and are in compliance with references ppppp and qqqqq. If the capability solution will require or transmit Top Secret / Sensitive Compartmented Information, address appropriate physical security concerns (accreditation and use of a Sensitive Compartmented Information Facility) where required. For capability solutions using IS that have intelligence authorities as designated accrediting authorities, ensure interoperability test plans include security testing considerations.

(6) Evaluation and Feedback

(a) Evaluation and feedback occur continuously throughout the intelligence process, and as an assessment of the intelligence process as a whole. Intelligence personnel at all levels, as well as users of intelligence, should assess the execution of the intelligence tasks being performed to identify deficiencies within the intelligence process and determine if intelligence requirements are being satisfied. The goal of evaluation and feedback is to identify issues as early as possible to minimize information gaps and to mitigate capability shortfalls.

(b) When possible, address capability solution requirements for means, formats, information needs and periodicity of assessments to support decisions about reprioritization of intelligence requirements, shifts in collection emphasis, changes to analytic levels of effort, reallocation of available intelligence assets, training of intelligence personnel, and the development of new intelligence capabilities.

d. Targeting Support

(1) Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering commander's guidance and objectives, planning requirements at all warfare levels, and operational requirements and capabilities. See reference rrrrr.

(2) Targeting support refers to the intelligence information, infrastructure, or resources required:

(a) For target development, to include derivation of coordinates and target materials production, validation, nomination, and prioritization.

(b) To support capabilities analysis and force assignment.

(c) To support mission planning, to include support such as weaponeering, target imagery notation, collateral damage estimation, and coordinate verification.

(d) To support operational execution, to include time-sensitive targeting support such as target identification, coordinate derivation, and weaponeering.

(e) To support the combat assessment process, to include battle damage assessment (BDA), munitions effects assessment (MEA), and supporting re-attack recommendations.

(3) Sponsors must consider intelligence support to targeting if their capability solution will employ, or will rely upon the employment of, offensive kinetic and non-kinetic capabilities. Intelligence targeting support shortfalls may detrimentally affect the capability solution's successful development, on-time delivery schedule, and ultimately its operational status (i.e., intelligence support to targeting is a broad category that encompasses munitions and all associated capability solutions relying upon the munition).

(4) Intelligence support to targeting may also be required during munition and other non-kinetic offensive capability design, development, and testing to help ensure the anticipated performance. (MEA and BDA studies may help identify gaps in FA capabilities.) Sponsors with capability solutions that will employ or rely on the employment of munitions must also consider intelligence support to targeting, and identify and address intelligence support requirements and shortfalls, if any, regarding not only their capability solution, but the munitions it will employ or rely upon.

(5) Examples of targeting products include target lists, target folders, target materials, modeling and simulation products, and collection and exploitation requirements to support targeting and target briefs. Examples of targeting services include weaponeering, casualty and collateral damage estimation, point positioning/coordinate mensuration, and verification and tactical mission planning support.

(6) Targeting support may overlap with the GEOINT support category because many targeting services rely upon and/or incorporate geospatial products or information. Coordinate-seeking weapons, or weapons that can or will be able to operate in a coordinate-seeking mode, must declare required target location error -- expressed as circular and linear error in meters or feet -- with an associated confidence level reported at 90%.

(7) Address requirements for support to target development, mission planning, precise positioning, BDA, MEA, weaponeering, the anticipated volume of targets managed and numbers of target folders to be produced, and associated targets or aim points to plan for during mission planning. Also address capability targeting certification and accreditation requirements in accordance with reference sssss.

e. IMD Support

(1) DOD intelligence used for programming platform mission systems including, but not limited to, the functional areas of signatures, EWIR, OOB, C&P, and GEOINT.

(a) Signatures. Signatures are defined as the distinctive characteristics, or sets of characteristics, that consistently recur and identify a piece of equipment, materiel, activity, or event. Signature support is the provision of such data to capability solutions that use signatures in their design, development, testing, training, or operations of sensors, models, or algorithms for the purpose of: combat identification; blue force tracking; targeting; or, detecting or identifying activities, events, persons, materiel, or equipment. This data may be used by intelligence analysts, automated systems, and system design and development engineers to, among other things, analyze and identify threats or the patterns of use for an adversary system.

(b) EWIR. Assessed, all-source intelligence data on adversary and non-adversary commercial systems, to include technical parametric and performance data, observed electronic intelligence data on foreign emitters from the National Security Agency (NSA), and engineering-value/measured data on domestic emitters.

(c) OOB. The identification, command structure, strength, and disposition of personnel, equipment and units of an armed force.

(d) C&P. All-source derived assessments of foreign military system capabilities and physical attributes.

(e) GEOINT. GEOINT IMD provides programs with mapping, charting and geodesy, geospatial information, imagery intelligence, and other GEOINT data, data products and services to support operations, navigation, terrain visualization, targeting and characterization of the physical and manmade environments. It is important that GEOINT IMD requirements be addressed early in the JCIDS process and documented for the entire system life cycle.

(2) Capability requirement documents should state whether or not the capability solution requires IMD. If the capability solution is IMD dependent, include a list of the relevant IMD functional area(s), an assessment of the IC's ability to support those requirements, and a reference to the capability solution's Life cycle Mission Data Plan (LMDP). IMD production and collection requirements that can be met by an acquisition program and are validated by the capability requirements community are included in the capability solution's LMDP in accordance with reference ttttt.

(3) Among IMD requirements, address whether all signature support (to include coverage, timeliness, content, fidelity, security, and scalability), and denial and deception support been considered and addressed. In addition, address whether sufficient analytical support is available to provide EWIR and C&P data, and whether all categories of data can be collected (i.e., White, Red, Blue and Gray).

(4) For additional information on IMD, see references ttttt and uuuuu.

f. Warning Support

(1) Warning support usually involves the traditional intelligence mission of "Indications and Warning" – identifying and defining a potential threat, and monitoring the threat. However, as an intelligence support category, warning support should be thought of as information that enables that capability solution to remain scientifically and technologically superior relative to developing or projected adversary capabilities. This support depends upon direct involvement of the Sponsor or PM in identifying CIPs. CIPs refer to general or specific adversary capabilities that, if developed, procured, or implemented, could significantly influence the effective operation of the Sponsor's capability solution. CIPs therefore support the development of intelligence production requirements and associated intelligence collection requirements that support a Sponsor's capability solution.

(2) Address the accuracy and timeliness of information, format of information, frequency of collection and reporting, information updates, and means of communicating information and relevance to decision making. This type of support may be addressed in terms of high, medium, or low demand

levels. Depending on the technological complexity of the capability solution, the level of warning support that may be required could vary (although the numbers of CIPs developed may be a good indicator of the quantitative levels of support required).

g. Space Intelligence Support

(1) Space intelligence support refers to requirements for space-based capability solutions; other capability solutions relying upon space-derived capabilities; and, platforms that perform space control or space support. This category also includes intelligence information, infrastructure, or resources that provide space-specific intelligence analysis on foreign space capabilities. See reference vvvvv.

(2) Address requirements for space intelligence coverage, whether periodic or persistent, timeliness, security, form of support necessary, and accuracy.

h. CI Support

(1) CI refers to the process of gathering information on, and activities conducted to counter, adversary or other collection activities directed against U.S./allied forces, other intelligence activities, sabotage or terrorism conducted by, or on behalf of, foreign governments, foreign organizations, foreign persons or international terrorist entities. See reference wwwww.

(2) CI support can and should be applied throughout a capability solution's life cycle. In the context of this instruction, CI support refers to the intelligence information, infrastructure, or resources used to educate acquisition communities on those threats. CI support also helps acquisition communities establish plans, tools, or techniques to protect designated S&T information and critical program information from such threats in accordance with reference xxxxx.

(3) CI support may include a number of activities, from providing threat awareness education to scientists and engineers performing fundamental research, to the implementation of a program protection plan (PPP).

i. Intelligence Training Support

(1) Some capability solutions may require intelligence personnel to provide specialized training to support part or all of a given capability solution's life cycle.

(2) The training requirement may include training additional personnel in existing training programs and/or in a new, unique training program that will be developed to support the capability solution. In either case, the requirement for specific training to support part or all of a capability solution's life cycle must be identified, analyzed, and declared as soon as possible in the JCIDS process to permit sufficient lead time to develop personnel with the skills required to support sponsor's capability solution.

(3) Address the amount of manpower required to support the capability solution, expected certifications required, skill specialties required (e.g., Air Force Specialty Code, Military Occupational Specialty), schools/courses required, language skills, whether there will be a requirement for a new or unique training program for sponsor's capability solution.

3. Document Content Guidance

a. General. This section provides guidance on drafting intelligence supportability content in capability requirement documents, including analysis that Sponsors must consider and address when appropriate. This section also serves as a reference to reviewers during the intelligence certification review process.

(1) Each capability solution is different, and may have unique intelligence support requirements. While the Threat Summary paragraph in an ICD and the Threat Summary and Intelligence Supportability paragraphs in CDDs and CPDs are the primary intelligence-focused paragraphs in capability requirement documents, other paragraphs may need to consider intelligence support or integration concepts.

(a) Threat Summary. The intent of the Threat Summary paragraph is to ensure capability requirements and associated capability gaps are based upon a consistent and up to date DIA- or Service-approved threat products, and that threat summaries are updated as needed before validation of successor documents. For MDAPs and capability requirements likely to result in MDAPs, ensure compliance with references yyyyy and zzzzz.

(b) Intelligence Supportability. The intent of the intelligence supportability paragraph is to identify and assess all intelligence support requirements and anticipated shortfalls throughout the capability solution's life cycle in one, comprehensive section of the CDD or CPD.

(c) The intelligence supportability paragraph must be consistent with the Operational Context, Capability Discussion, Developmental KPPs, KSAs and APAs, and DOTmPLF-P sections of the capability requirement document. If threat or intelligence support issues are addressed in other

sections of a capability requirement document, then provide a reference to the applicable paragraph in these paragraphs, and do not replicate information unnecessarily.

(2) Intelligence support requirements and/or threats applicable to a capability solution may change over time. Understanding and specifying intelligence support requirements or shortfalls will become more refined as the capability requirement documents progress from ICD to CDD to CPD.

(3) Significant changes to current threats or the emergence of new threats associated with validated capability requirements and the development of related capability solutions may drive changes to the development of capability solutions. If updates to applicable threat products or other aspects of intelligence certification are required to react to unanticipated threat changes, see Enclosure E of this manual for details on updates to and revalidation of capability requirement documents.

b. CDD and CPD Content. The level of discussion and analysis in CDDs and CPDs is more refined than that contained in ICDs, and must address specific support requirements for the capability solution discussed in the CDD or CPD. As a capability solution progresses from CDD to CPD, Sponsors are responsible for increasing levels of refinement and analysis relating to intelligence supportability and shortfalls. In drafting the Intelligence Supportability paragraph of CDDs and CPDs, Sponsors must consider.

(1) Scope and Recommended Analytical Approaches

(a) Sponsors must identify, analyze, and discuss their capability solution's current and projected requirements for intelligence support (e.g., manpower, resources, and processes); its impact on joint intelligence strategy, policy, and architecture; and, intelligence support shortfalls, if any.

(b) Sponsors should consider whether each of the intelligence support categories discussed earlier in this section will be available, suitable, and sufficient throughout a given capability solution's life cycle, not just for a particular portion of the life cycle.

(c) Potential Intelligence Support Shortfalls. Consider and address known, projected, or potential intelligence support shortfalls that result from, or may result from, the development, testing, operation, and/or the sustainment of the capability solution (to include manpower, training, doctrine, processes, or systems). "Shortfalls" may include gaps related to the capability solution, those caused by the capability solution that affect other previously fielded or planned capability solutions, or which may exacerbate currently known shortfalls. Particular focus should be placed on shortfalls that could

affect or delay development, testing, or fielding the capability solution, or those shortfalls that may degrade the operational effectiveness or sustainment of the capability solution. Sponsor must also consider and address the cause of these shortfalls (such as technological capability shortfalls, undefined common intelligence data/metadata standards, scheduling problems, or funding issues) and, if possible, estimate the magnitude of the shortfall in terms of scheduling delays, vulnerability, materiel, resources, training, manpower, and any other relevant criteria. Note that information related to intelligence shortfalls may be, or may become, classified information when associated with a shortfall; therefore, sponsors must ensure that this section of the document is marked accordingly.

(d) Proposed Solutions. Identify, analyze, and discuss any and all possible solutions for shortfalls identified. Include key issues that must be resolved concerning each shortfall. Provide a plan to address such shortfalls, and a schedule or deadline to remedy each shortfall. If the solution lies outside the control of the program office, or is deemed to be unobtainable, provide a recommendation on how to address the shortfall, and identify the organization with the authority and responsibility to address the shortfall.

(e) DOTmLPF-P Considerations. If the capability solution is expected to require new, unique, and unplanned support, or will place additional burdens on the existing and projected intelligence architecture, consider and address what, if any, DOTmLPF-P changes are needed to address these requirements.

(f) Leverage related information contained in acquisition documents such as the ISP, LMDP, or PPP. Acquisition documents can greatly assist with information on intelligence support, such as IMD availability, life cycle cost estimates, CI support plans, etc.

(g) Review the architecture data and associated artifacts/views for intelligence requirements based on information and data flow plans that may impact the Intelligence Planning and Operations support category. For all intelligence requirements identified, address what intelligence infrastructure (e.g., platforms, systems, software, facilities, etc.) and resources will be required to collect, compile, store, analyze, and disseminate the intelligence required. Determine whether these information needs are addressed adequately to allow a thorough assessment of intelligence supportability.

(h) Include and address intelligence interoperability requirements in the Intelligence Supportability section wherever applicable. Address intelligence interoperability requirements at both the system level (the ability of the system to produce data and metadata standards-compliant information, and exchange data and products with similarly compatible systems) and the

operational level (within which the capability solution will function with operations and C2 systems and processes).

(2) Example Content and Format of Intelligence Supportability Paragraph. While the content and organization of this paragraph should be tailored to best fit the nature of the capability solution, this section provides a recommended general format for the intelligence supportability paragraph. The recommendations included should be answered in light of the considerations above, and should be supplemented with the Sponsor's unique knowledge and insight about the capability solution.

8. Intelligence Supportability. Introduce the paragraph with a general description of the types and level of intelligence support required to enable the program's intended capability, consistent with other document sections and considering factors in the Scope and Analytical Approaches, above.

a. Intelligence Support Category Requirements. Identify and address support requirements, potential shortfalls, and efforts to satisfy shortfalls for all applicable intelligence supportability categories below. (For category descriptions, see earlier sections of this Enclosure). Be as specific as possible, and include as many qualitative and quantitative attributes as possible. If attributes are unknown, state what is not known and why.

(1) Intelligence Manpower Support

(2) Intelligence Resource Support

(3) Intelligence Planning and Operations Support

(4) Targeting Support

(5) Intelligence Mission Data Support

(6) Warning Support

(7) Space Intelligence Support

(8) Counter Intelligence Support

(9) Intelligence Training Support

b. If requirements are discussed in other places within the document or in other documents (such as CI Support requirements addressed in a capability solution's PPP), provide cross-references to those paragraphs or documents.

c. Intelligence Security Requirements. Identify all security requirements or considerations that the capability solution will require, and address how those security considerations are satisfied (e.g., classification levels; information sharing or releasability; certifications, and facility implications for receiving, using, and storing SCI; and all other security considerations that the capability solution will require, such as compliance with references ppppp and qqqqq.

(INTENTIONALLY BLANK)

DRAFT

APPENDIX J TO ENCLOSURE D

CONTENT GUIDE FOR WEAPON SAFETY

1. Overview

a. Purpose. This guide provides document Sponsors with content related to the weapon safety assurance sections of CDDs and CPDs. Weapon safety assurance is also applicable to weapon related DCRs to ensure that non-materiel solutions using an existing system do not introduce new safety issues, hazards, or risk as a result of the proposed changes.

b. Designation of weapons as joint systems. Because all weapons/weapons systems have the potential of being deployed together or employed in joint environments, weapons and weapons systems will be considered joint systems within the JCIDS process and have a JSD of Joint Integration or higher. The term weapon in this context includes military munitions as defined in 10 USC 101. In addition, the weapon safety assurance is applicable to directed energy weapons (DEW), EM rail guns, and all firing, launching, safety critical software, and controlling systems as part of the definition. Exceptions include nuclear weapons and their components; small arms and associated ammunition not containing electronics or software; intercontinental ballistic missiles; and space launch vehicles.

c. Tailoring of Weapon Safety Requirements. The guide provides standardized requirements for weapon safety, which Sponsors may propose to tailor depending upon the specific operational context in question.

(1) In cases where a capability solution described in a CDD or CPD is intended to meet all baseline weapon safety requirements and criteria outlined above, and no tailoring of weapon safety requirements are needed to address unique aspects of the operational context, the weapon safety assurance section of the CDD or CPD may state that fact.

(2) In cases where tailoring of one or more of the baseline weapon safety requirements is proposed due to unique aspects of the operational context, the weapon safety assurance section of the CDD or CPD shall provide the specific weapon safety requirements which deviate from the standards. The Sponsor shall provide rationale for the deviations, traceable to the joint or multinational mission environment, and articulate the specific attributes and performance parameters that must be met as the basis for increased or decreased weapon safety requirements.

2. Baseline Weapon Safety Requirements

a. System Safety. Reference bb provides risk acceptance criteria for high, serious, medium, and low risks. Sponsors will identify the acceptable risk levels for weapon safety assurance. System safety and acceptable risk requirements informs the development of a System Safety Program (SSP) for the life cycle of the weapon system in accordance with references aa and aaaaaa.

b. Insensitive Munitions (IM). Standardized IM test protocols used in assessing a weapon's response to unplanned threats are established in references bbbbbb and cccccc.

c. Fuze Safety. Fuze safety requirements are established in references dddddd through ffffff.

d. Explosive Ordnance Disposal (EOD). Requirements for disposal of munitions containing or delivering energetic material must satisfy the EOD RDT&E authority in accordance with reference gggggg. Requirements for disposal will inform the development of a demilitarization and disposal plan IAW with treaties, international agreements, Federal and state regulations and laws, and reference bb.

e. Laser Safety. If the munitions contain lasers, to protect and mitigate the risk to personnel from laser radiation to an acceptable level, requirements for engineering design, protective equipment, administrative controls, or a combination thereof are established in reference ssss.

f. E3 Ordnance Safety. E3 ordnance safety requirements are established in references hhhhhh and iiiiii, including but not limited to hazards of electromagnetic radiation to ordnance, electrostatic discharge, EMP, electromagnetic interference, electromagnetic vulnerability, lightning, and precipitation-static.

g. Weapon Packing, Handling, Storage, and Transportation. Safety for packing, handling, storage, and transportation are established in reference jjjjjj.

h. Other Considerations. In addition to criteria in the categories above, Sponsors should consider criteria shown in Table D-I-1.

DRAFT

Additional Weapon Safety Criteria	
• Joint and Service unique safety requirements • Service and Joint Concepts and/or CONOPS • Assembly • Disassembly • Maintenance • Testing • Use	• Interoperability • Software safety • ESOH • Future CONOPS possibilities • HSI • Coalition factors • Cultural factors

Table D-I-1. Safety Review Criteria

3. Proponent. The WSE proponent is the Protection FCB. For questions, contact the Protection FCB at 703-693-7116. The JWSTAP also provides subject matter expertise to Sponsors for review during development of weapons program capability requirement documents prior to formal submission to the JCIDS process for review and validation.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

ENCLOSURE E

GATEKEEPING

1. Joint Staff Gatekeeper

a. Purpose. The primary function of the Joint Staff Gatekeeper is to manage the overall flow of capability requirement documents and other related issues into and out of the JCIDS process for staffing and validation, to ensure stakeholder visibility into documents and issues validated under independent validation authorities, and to support other activities of the JCIDS process.

(1) IC common gatekeeping. In accordance with reference xxx, the IC maintains a common Gatekeeper function with the Joint Staff Gatekeeper for the ICCR and JCIDS processes. Capability requirement documents for both processes are submitted to the Gatekeeper to initiate staffing and ensure appropriate visibility and participation across processes.

(2) DBS common gatekeeping. In support of reference zzz, the DCMO maintains a common Gatekeeper function with the Joint Staff Gatekeeper for the JCIDS process and the acquisition of DBS. DBS documents are submitted to the Gatekeeper to initiate staffing and ensure appropriate visibility and participation across processes.

(3) Sponsor organization gatekeepers. Sponsor organizations submitting and/or commenting upon capability requirement documents will have a Sponsor Gatekeeper function providing a single point of entry into the JCIDS process. If applicable, the Sponsor will also have Sponsor Gatekeepers for the ICCR process and acquisition of DBS, which may be the same as the Sponsor Gatekeeper for the JCIDS process. Sponsor Gatekeeper(s) will facilitate communications between the Joint Staff Gatekeeper and principals in Sponsor organizations.

b. Additional Activities

(1) Managing submissions with special protections. Coordinating with the J-8/SAPCOORD to ensure that appropriately cleared stakeholders have access to capability requirement documents or issues protected by SAP or SAR designation. Coordinating with the Sponsor to ensure that appropriate stakeholders have access to capability requirement documents or issues protected by ACCM designation.

(a) Typically, access will include the FCB Chair, and appropriate Action Officers (AOs) from the FCB, J-8/JRAD, J-8/CAD, and certifying or endorsing organizations as needed to complete the review.

(b) This ensures that decisions made regarding new capability requirements, and changes to previously validated capability requirements, are considered in the context of the entire capability requirement portfolio.

(2) Monitoring of validated JUONs and JEONs.

(a) The Joint Staff Gatekeeper monitors progress of efforts toward fielding capability solutions for JUONs and JEONs on a quarterly basis in accordance with Enclosure B of this manual. The Joint Staff Gatekeeper also initiates reviews of validated JUONs and JEONs which have been active for two years or more without receiving an assessment from the requirement sponsor indicating limited duration sustainment or proposal to validate enduring capability requirements to support transition of capability solutions to enduring PORs.

(b) The Joint Staff Gatekeeper does not monitor progress of efforts toward fielding capability solutions for DOD Component UONs. However, the validated DOD Component UONs contribute to the capability requirement portfolios managed by the FCBs, and stakeholders in the associated FCB may have interest in the progress of the capability solution.

(3) Managing the KM/DS system

(a) The Joint Staff Gatekeeper manages the organization of requirements data on the KM/DS system for data classified at or below the level of SECRET, and via other means for data classified above SECRET, and ensures that Sponsors provide studies or other data supporting their capability requirement documents prior to initiation of staffing.

(b) The Joint Staff Gatekeeper ensures that stakeholders are notified of new capability requirement documents or data which are applicable to their respective capability requirement portfolios.

(c) The Joint Staff Gatekeeper ensures any waivers to process and/or document formats are documented, and memos archived with the associated documents for future reference.

(4) Generating JCIDS process metrics. Specific process metrics tracked for JCIDS are outlined later in this enclosure.

2. Document Submission Guidance

a. Staffing process and validation authority determination. Regardless of potential ACAT or validation authority, Sponsors submit all ICDs, CDDs, CPDs, Joint DCRs, JUONs, and JEONs to the Joint Staff Gatekeeper for determination of the appropriate staffing process and validation authority.

(1) Capability requirement documents for capabilities funded by a combination of NIP and MIP funding are submitted to the Joint Staff Gatekeeper to enable a common gatekeeper function between JCIDS and ICCR processes.

(a) Documents for capability requirements that are funded primarily or wholly with NIP funding, will be developed, reviewed, and validated in accordance with the ICCR process outlined in reference yyy.

(b) Documents for capability requirements that are funded primarily or wholly with MIP funding will be developed, reviewed, and validated under the JCIDS process outlined in this manual and in reference b.

(2) Documents related to DBS are submitted to the Joint Staff Gatekeeper to enable a common gatekeeper function between the JCIDS process and the acquisition of DBS.

(3) DOD Component UONs are not submitted to the Joint Staff Gatekeeper for determination of the appropriate staffing process and validation authority, but are submitted for visibility and archiving after validation.

b. Use of DOD Component Gatekeepers

(1) Sponsors submit all capability requirement documents via their DOD Component gatekeeper to the Joint Staff Gatekeeper to facilitate single point of entry into the JCIDS process. Submissions received from other entities will be referred back to the DOD Component gatekeeper prior to staffing.

(2) DOD Component gatekeepers, together with the DOD Component representatives to the FCB, will assess documents assigned a JSD of Joint Information by the Joint Staff Gatekeeper to determine which documents impact DOD Component equities and require review and commenting.

c. Recommendation for parallel staffing. In cases where minimizing the overall staffing timeline is a priority, Sponsors are encouraged to submit documents for joint staffing of applicable certifications/endorsements or validation in parallel with any Sponsor approval processes. This ensures that issues from lower level reviews can be addressed between the Sponsor and the Joint Staff before receiving higher level Sponsor approval, and minimizes the need for Sponsor re-approval when addressing joint equities.

d. Document and Data Submission

(1) For capability requirement documents and related data classified at or below the level of SECRET, and not protected by ACCM or SAP/SAR designation:

(a) ICDs, CDDs, CPDs, and Joint DCRs. Sponsors submit capability requirement documents and related data via the KM/DS system located at the URL in reference h. If a Sponsor wishes to submit a physical signature page, the Sponsor may submit that one page in pdf format as an attachment.

(b) JUONs and JEONs. Sponsors submit JUONs and JEONs via SIPRNET email or memo to the Joint Staff Gatekeeper without using the KM/DS System.

(c) DOD Component UONs. After DOD Component validation, Sponsors submit validated DOD Component UONs via SIPRNET email or memo to the Joint Staff Gatekeeper without using the KM/DS System.

(2) For capability requirement documents and related data classified above the level of SECRET, and not protected by ACCM or SAP/SAR designation:

(a) ICDs, CDDs, CPDs, and Joint DCRs. Sponsors enter placeholder records in the KM/DS system and then provide the capability requirement documents to the Joint Staff Gatekeeper via the Joint Worldwide Intelligence Communications System (JWICS) or hard copy. The placeholder record will include instructions on document location and how to access.

(b) JUONs and JEONs. Sponsors submit JUONs and JEONs via JWICS to the Joint Staff Gatekeeper without using the KM/DS System.

(c) DOD Component UONs. After DOD Component validation, Sponsors submit validated DOD Component UONs via JWICS to the Joint Staff Gatekeeper without using the KM/DS System.

(3) For capability requirement documents and related data protected by SAP/SAR designation:

(a) Sponsors or the J-8/SAPCOORD enter a placeholder record in KM/DS only when the presence of the capability requirements protected by SAP/SAR designation can be disclosed at or below the classification level of SECRET. Note that a reference number or other substitute for the actual title may be used when the presence can be disclosed but the classification of the title is such that it cannot be stored in KM/DS.

(b) Capability requirement documents and related data are provided through the Sponsor Special Access Program Control Office (SAPCO) to the J-8/SAPCOORD, who will coordinate with the Joint Staff Gatekeeper for review by appropriately cleared reviewers. As there is typically a time lag involved with considering specific personnel for SAP/SAR access the J-8/SAPCOORD and Joint Staff Gatekeeper will:

1. Maintain a roster of personnel, appropriately cleared to one or more of the capability requirement portfolios, who can facilitate the review of submitted documents while minimizing the number of additional accesses granted.

2. Identify essential JCB or JROC participants who may not already have appropriate access, and facilitate initial vetting to provide timely access when/if appropriate.

(c) The J-8/SAPCOORD will retain validated documents and associated validation memos in accordance with SAP/SAR policy outlined in references kkkkkk and llllll, and storage and handling procedures for each program.

(4) For capability requirement documents protected by ACCM designation:

(a) Sponsors enter a placeholder record in the KM/DS system only when the presence of the capability requirements protected by ACCM designation can be disclosed at or below the classification level of SECRET. Note that a reference number or other substitute for the actual title may be used when the presence can be disclosed but the classification of the title is such that it cannot be stored in KM/DS.

(b) Sponsors coordinate with the Joint Staff Gatekeeper to ensure appropriate personnel are accessed to the ACCM for the review, and that documents are handled in accordance with the ACCM protections.

(c) The Joint Staff Gatekeeper will retain validated documents and associated validation memos in a manner such that only those accessed to the applicable ACCM may review the documents.

e. Sequence for Document Submissions

(1) Concurrent staffing of ICDs, CDDs, and CPDs for the same capability requirement/solution is not allowed.

(2) Submission of a CDD or CPD for validation prior to, or in parallel with, the associated post-AoA (or similar study) review is not allowed. A draft

CDD, prepared to support MS A and not submitted for validation at that time, will be provided to support the post-AoA (or similar study) review.

(3) Concurrent staffing of waiver requests for predecessor documents is allowed. The staffing of a successor document will be immediately terminated if the waiver request for its predecessor is denied.

f. ICD or CDD Waiver Requests. ICDs and/or CDDs may be waived by the Joint Staff Gatekeeper, in coordination with the validation authority and MDA, approves in cases where potential programs are best served by proceeding directly to MS B or MS C, such as for GOTS/COTS solutions, transitioning JUONs, JEONs, and DOD Component UONs, successful JCTDs, etc.

(1) The Sponsor will submit the waiver request in memo form into the KM/DS system as the document type that is being waived (e.g., ICD waiver request will be submitted as an ICD document type), and must be endorsed by the Sponsor J8-equivalent or higher. The waiver request must include the rationale/justification for why an ICD and/or CDD is not appropriate, the source(s) of equivalent information, and the proposed path forward. In cases where the MDA recommends proceeding directly to a CPD and MS C decision, the post-AoA (or similar study) review by the validation authority and the resulting JROCM satisfies the intent of the CDD waiver.

(2) The Joint Staff Gatekeeper assigns the waiver request to the appropriate FCBs and a J-8/CAD AO for evaluation within 4 calendar days of receiving the waiver request.

(3) The lead FCB, in coordination with the J-8/CAD AO, will develop a recommendation for approval/disapproval of the waiver within 13 calendar days.

(4) After receiving the recommendation from the Lead FCB, the Joint Staff Gatekeeper will approve or disapprove the request within 4 calendar days.

(5) Approval or denial of the request is documented in memo format from the Joint Staff Gatekeeper and is posted as an attachment to the request in the KM/DS system. The waiver memo will identify the traceability to any appropriate predecessor documents that provide justification for the waiving of the ICD and/or CDD.

g. Other format or process waiver requests. Requests for exceptions or variances to reference b or the document formats and processes described in this manual must be directed to the Joint Staff Gatekeeper.

(1) The Joint Staff Gatekeeper will work in coordination with the document Sponsor and the appropriate FCB to ensure any exceptions or

variances meet the needs of the validation authority while allowing for appropriate flexibility in the capability requirements process.

(2) Waivers granted by the Joint Staff Gatekeeper shall be documented in memo format to provide traceability in future staffing and validation activities.

3. Joint Staff Gatekeeper Activities

a. Initial Review. The Joint Staff Gatekeeper provides initial review of all incoming documents and performs several activities prior to documents entering staffing:

(1) Reviews each document submitted, regardless of actual/potential ACAT designation or previous JSD or independent validation authority decisions, to confirm that the document is complete and ready for staffing.

(2) Confirms that results of CBAs, studies, and other applicable supporting data for the document have been uploaded to the KM/DS Studies repository, or if not appropriate for the KM/DS studies repository, have been provided to the Joint Staff Gatekeeper via alternate means so that they can be made available to applicable reviewers.

(3) Returns documents to Sponsors for further development prior to staffing when they are not compliant with the JCIDS process as outlined in this manual.

(a) The intent is to address fundamental deficiencies which will delay or complicate review of the document. This allows staffing and senior leader discussions to focus on the substantive nature of the proposed capability requirements and the associated life cycle cost, schedule, performance, and quantity tradeoff decisions in the best interest of the overall joint force. Some examples include, but are not limited to:

1. Incorrect document type being submitted. E.g. – IS-ICD for efforts including hardware development (should be a regular ICD), CDD for purely DOTmLPF-P efforts (should be a Joint DCR), etc.

2. Lack of predecessor documents or supporting studies. E.g. – a CDD being submitted prior to having a validated ICD or post-AoA (or similar study) review, or an ICD being submitted without the supporting CBA or other analysis provided to the studies repository in the KM/DS system.

3. Incomplete, omitted, or inappropriate operational attributes (in ICDs) or KPPs/KSAs/APAs (in CDDs/CPDs), such as, but not limited to:

a. ICD attributes / metrics that are written with the specificity of KPPs/KSAs/APAs. (ICD attributes/metrics should describe solution agnostic capability requirements rather than system or solution specific performance parameters)

b. Values specified as "TBD" or unquantified descriptions in the definition of operational attributes or KPPs/KSAs/APAs.

c. Omission of any of the mandatory KPPs without appropriate justification.

4. Incomplete or unclear representation of capability gaps with respect to the capability solutions currently available to the joint force or in development. Except in rare cases, the capability requirement is not the same as the capability gap. In most cases, there is some level of legacy capability, and the gap must be presented as the difference between the legacy capabilities and the capability requirements articulated in the document, and the operational impact or risk due to that difference.

5. Incomplete or omitted life cycle cost data associated with the proposed capability, refined appropriately to the stage of the requirements process – ICD, post-AoA (or similar study) review, CDD, or CPD.

6. Unclear or omitted discussion of interdependencies between the proposed capability and enabling capabilities, or other capabilities within an SoS approach.

(b) Documents with minor formatting errors that can be easily corrected during post-staffing comment resolution may be allowed to enter staffing. Joint Staff Gatekeeper noted discrepancies will be documented via Comment Resolution Matrix (CRM) in the normal staffing process.

(c) Document rejection prevents initiation of the staffing process until corrective actions are taken, and the revised document is accepted by the Joint Staff Gatekeeper.

b. Actions for ICDs, CDDs, CPDs, and Joint DCRs. The Joint Staff Gatekeeper:

(1) FCB Assignment. Identifies lead FCB and supporting FCBs as needed.

(2) JSD Assignment. Assigns one of the four possible JSDs outlined below, based on actual/potential ACAT and Joint Staff equities (necessity of specific certifications and endorsements, leadership guidance, predecessor document JSD, etc.).

(a) The JSD sets the staffing path and timeline for the document, and identifies the validation authority.

(b) To maximize speed and flexibility in the JCIDS process, JSDs will be set at the lowest level which ensures that joint equities are addressed. In cases where a Sponsor believes the JSD should be set at a different level than that assigned by the Joint Staff Gatekeeper, Joint Staff J-8, Deputy Director for Requirements (J-8/DDR) will provide timely review and adjudication of the assigned JSD.

(c) JSDs may be changed during active staffing, but will not be revisited for a subsequent submission of the same document unless the lead FCB submits a request for JSD change to the Joint Staff Gatekeeper.

(d) There are three categories of JSDs:

1. JROC or JCB Interest. Applied to capability requirement documents which have a potentially significant impact to the joint force or otherwise require high-level oversight and coordination, including interoperability (other US government agency/department, allied/partner nation, coalition, etc.), and other aspects such as transportability and other joint force enablers not otherwise covered by joint certifications and endorsements.

a. JROC Interest is used for these documents associated with, or with the potential to drive, ACAT I/IA programs, or where the intended level of joint oversight cannot be satisfied by assignment of a lower level JSD. The JROC is the validation authority for JROC Interest documents.

b. JCB Interest is used for these documents associated with, or with the potential to drive, ACAT II and below programs where the intended level of joint oversight cannot be satisfied by assignment of a lower level JSD. The JCB has independent validation authority for JCB Interest documents, except for USSOCOM capability requirement documents for which the Special Operations Command Requirements Evaluation Board has independent validation authority.

c. JCB Interest is the minimum JSD for Joint DCRs and for any documents where the Sponsor is a CCMD, with the exception of USSOCOM when sponsoring internal capability solution development.

2. Joint Integration. Applied to all capability requirement documents associated with, or with the potential to drive, ACAT II and below programs, which require one or more Joint Staff certifications or endorsements, but are below the level of JCB Interest. Joint Integration is the minimum JSD

for weapons and munitions meeting the definitions outlined in Appendix J to Enclosure D of this manual. The Sponsor organization has independent validation authority for Joint Integration documents, once applicable Joint Staff certifications and endorsements are received.

3. Joint Information. Applied to all capability requirement documents associated with, or with the potential to drive, ACAT II and below programs, which do not need Joint Staff certifications or endorsements, and are below the level of JCB Interest. The Sponsor organization has independent validation authority for Joint Information documents and responsibility for applicable certifications and endorsements. Staffing comments provided by stakeholders are incorporated at Sponsor discretion.

(e) Subsequent review of capability requirement documents previously assigned a JSD of Independent, or JSD assignment to successor documents, will be assigned a JSD of Joint Information unless a higher JSD is applicable.

(f) With the exception of majority NIP-funded IC capability requirements and requirements managed by the Nuclear Weapons Council, the JROC may exert validation authority over any capability requirement by changing the JSD to JROC Interest or JCB Interest.

(3) Determine Certification/Endorsement Authority. Determines responsibility for certifications or endorsements which may be necessary during staffing for capability requirement documents. Unless otherwise tailored by the Joint Staff Gatekeeper, in coordination with the certifying or endorsing organization, the responsibilities are assigned based upon assigned JSDs as shown in Table E-1.

DRAFT

Certifications and Endorsements	**JROC or JCB Interest**	**Joint Integration**	**Joint Information**
Threat Assessment / Intelligence Certification	Joint Staff	Joint Staff	Sponsor
Weapon Safety Endorsement	Joint Staff	Joint Staff	
FP KPP Endorsement	Joint Staff	Sponsor	Sponsor
SS KPP Endorsement	Joint Staff	Sponsor	Sponsor
Sustainment KPP Endorsement	Joint Staff	Sponsor	Sponsor
NR KPP Certification	Joint Staff	Joint Staff	Sponsor
Energy KPP Endorsement	Joint Staff	Joint Staff	Sponsor
DOTmLPF-P Endorsement	Joint Staff	Sponsor	Sponsor

Table E-1. Certification and Endorsement Responsibilities

(a) In cases where the Sponsor has responsibility for certifications and endorsements, and has independent validation authority, the Sponsor organizations will certify, endorse, or waive each item as they deem appropriate.

(b) In cases where the Sponsor has responsibility for certifications and endorsements, and the JCB or JROC has validation authority, the Sponsor organizations will certify, endorse, or waive each item, and provide an associated memo to the Joint Staff Gatekeeper to support staffing and validation. If the Sponsor prepares a certification or endorsement ahead of, rather than in parallel with, joint staffing and validation of the document, the certification or endorsement may require updates based upon changes made during staffing. (Note that this case is not reflected in Table E-1, but may result from tailoring of certification or endorsement responsibilities on a case-by-case basis.)

(c) In cases where the Joint Staff has responsibility for certifications and endorsements, and the Sponsor has validation authority, the Joint Staff organizations will certify, endorse, or waive each item, and provide an associated memo to the Sponsor to support staffing and validation. The Sponsor is encouraged to initiate joint staffing for certification or endorsement as early as practical within the Sponsor staffing and validation process to ensure, if required, any associated changes to the capability requirement document can be made in a timely manner to support certification and/or endorsement.

DRAFT

(d) In cases where the Joint Staff has responsibility for certifications and endorsements, and the JCB or JROC has validation authority, the Joint Staff organizations will certify, endorse, or waive each item, and provide an associated memo to the Joint Staff Gatekeeper to support staffing and validation.

(e) The following organizations provide Joint Staff certifications or endorsements when indicated in Table E-1. Note that for USSOCOM capability requirement documents assigned a JSD of JCB Interest or Joint Integration, where Table E-1 indicates Joint Staff responsibility, certifications or endorsements will be performed by USSOCOM, with participation in reviews by representatives from Joint Staff certifying or endorsing organizations.

1. Threat Assessment and Intelligence Certification. The Joint Staff J-283 / Intelligence Requirements Certification Office (J283/IRCO) provides intelligence certification in accordance with Appendix I to Enclosure F of this manual, including threat assessment provided by DIA/TLA. Threat assessment and intelligence certifications is applicable to ICDs (including IS variants), CDDs (including IS variants), and CPDs, and to Joint DCRs with intelligence supportability impacts or affecting capability solutions which previously received threat assessment and intelligence certification.

2. WSE. The Chair of the Protection FCB provides the WSE in accordance with Appendix A to Enclosure F of this manual and reference jjjj. The WSE is applicable to CDDs and CPDs addressing munitions and Joint DCRs with potential impact to weapon safety.

3. FP KPP Endorsement. The Chair of the Protection FCB provides endorsement of the FP KPP in accordance with Appendix B to Enclosure F of this manual. The FP KPP is applicable to all CDDs and CPDs addressing manned systems, or systems designed to enhance personnel survivability.

4. SS KPP Endorsement. The Chair of the Protection FCB provides endorsement of the SS KPP in accordance with Appendix C to Enclosure F of this manual. The SS KPP is applicable to all CDDs and CPDs.

5. Sustainment KPP Endorsement. The Chair of the Logistics FCB, in coordination with the J-4/MXD, provides endorsement of the Sustainment KPP in accordance with Appendix D to Enclosure F of this manual. The Sustainment KPP is applicable to all CDDs and CPDs.

6. NR KPP Certification. The Chair of the C4/Cyber FCB provides certification of the NR KPP in accordance with Appendix E to Enclosure F of this manual and reference iiii. The NR KPP is applicable to IS-

ICDs, and all CDDs and CPDs addressing IS, regardless of classification or sensitivity of the data handled by the IS, unless defined as non-DODIN IT by reference qqqq.

7. Energy KPP Endorsement. The Chair of the Logistics FCB, in coordination with the J-4/ED, and with advice from the office of the ASD(OEPP) as appropriate, provides endorsement of the Energy KPP in accordance with Appendix F to Enclosure F of this manual. The Energy KPP is applicable to all capability requirement documents addressing systems where the provision of energy, including both fuel and electric power, to the system impacts operational reach, or requires protection of energy infrastructure or energy resources in the logistics supply chain.

8. Training KPP Endorsement. The J-7/DDI, with advice from the office of the OSD(P&R) as appropriate, provides endorsement of the Training KPP as part of the training considerations in the DOTmLPF-P endorsement in accordance with Appendix H to Enclosure F of this manual. A separate endorsement of the Training KPP is not required. The Training KPP is applicable to CDDs and CPDs that have system performance requirements necessary to enable training associated with the materiel capability solution.

9. DOTmLPF-P Endorsement. The J-7/DDI, in coordination with DOTmLPF-P stakeholder organizations, provides endorsement of DOTmLPF-P considerations and non-materiel capability solutions in accordance with Appendix H to Enclosure F of this manual. This endorsement includes endorsement of Training KPP content together with the non-materiel aspects of training addressed in the DOTmLPF-P section. The DOTmLPF-P endorsement is applicable to both ICDs and Joint DCRs recommending non-materiel capability solutions, and CDDs and CPDs that advocate for DOTmLPF-P changes associated with materiel capability solutions.

(4) Other pre-staffing activities

(a) For revisions to previously validated documents, determines if staffing will be conducted only upon the proposed changes and impacts thereof or if revalidation of the overall document is warranted.

(b) In coordination with J-8/JRAD, J-8/CAD, and J-8/PBAD, the Joint Staff Gatekeeper assigns POCs, as required, to participate in the FCB review.

(c) Initiates staffing of the document by sending the document to the lead FCB, and ensures notifications generated by the KM/DS system are sent to all affected stakeholders, including the Sponsor, FCBs, validation authorities, Joint Staff certifying or endorsing organizations, and JROC advisors. Staffing calendars in the KM/DS system are tentatively set based

upon nominal process timelines, and are updated automatically as process activities are completed.

1. For IC capability requirements assigned to the ICCR process for review and validation, the Joint Staff Gatekeeper will notify the Chair of the BA FCB to enable proper coordination with and participation in the ICCR process.

2. For IC capability requirements assigned to the JCIDS process for review and validation, the Joint Staff Gatekeeper will notify the Associate Director of National Intelligence for Systems and Resource Analysis (ADNI/SRA) to enable proper coordination with and participation in the JCIDS process.

3. For DBS capability requirements, the Joint Staff Gatekeeper will assess if there are equities requiring JCIDS staffing and validation of requirements, and notify the applicable FCB(s) and DCMO of the decision related to staffing in JCIDS.

(7) Pre-validation activities. Ensures comment adjudication is complete prior to validation of documents for documents with JSDs of Joint Integration, JCB Interest, or JROC Interest.

(a) Comment adjudication for comments unrelated to joint certifications or endorsements must be completed to the satisfaction of the validation authority.

(b) Comment adjudication related to joint certifications or endorsements must be completed to the satisfaction of the certifying or endorsing organization. Completion will be documented via a certification or endorsement memo, or waiver memo, from the certifying or endorsing organization.

c. Actions for JUONs, JEONs, and DOD Component UONs.

(1) DOD Component UONs. DOD Component UONs are validated by DOD Component validation authorities using staffing detailed in references hh through oo.

(a) Upon completion of Sponsor staffing and validation, copies of the DOD Component UON and validation decision are submitted to the KM/DS system for information purposes and visibility in the capability requirement portfolios.

(b) If a Sponsor also uses processes in reference hh through oo to manage actions unrelated to documenting urgent or emergent capability

requirements and associated capability gaps, they will filter documents accordingly, and upload to the KM/DS system only those documents which reflect new or modified capability requirements and capability gaps.

(2) JUONs. Upon receiving a JUON document, the Joint Staff Gatekeeper verifies that the submission meets the JUON criteria as defined in Enclosure D of this manual, and is not better addressed through other departmental processes.

(a) In cases where the submission does not meet the JUON criteria, the Joint Staff Gatekeeper will issue a memo to the Sponsor and appropriate stakeholders with the rationale for rejection, and if applicable, suggestion(s) for alternate approaches to satisfy the capability requirement. Disposition will be archived on the KM/DS system for visibility and reference purposes.

(b) In cases where a submission does not meet the criteria for a JUON, but J-8/DDR anticipates that VCJCS may approve handling the capability requirement as a JEON, the Joint Staff Gatekeeper will notify the Sponsor of the designation change and, unless withdrawn by the Sponsor, will continue processing the submission as a JEON.

(c) Documents meeting the JUON criteria are assigned to the appropriate Lead FCB for collaborative review with the JRAC in accordance with Enclosure G of this manual.

(3) JEONs. JEONs require expedited handling in a similar manner to JUONs, but with several distinct differences:

(a) Upon receiving a JEON document, the Joint Staff Gatekeeper will coordinate through the Director, Joint Staff J-8 (DJ-8) to the VCJCS to confirm the request justifies expedited handling, even if the anticipated contingency operations are not known to the Joint Staff Gatekeeper.

(b) In cases where the JEON is not approved by the VCJCS, the Joint Staff Gatekeeper will issue a memo to the Sponsor with the rationale for rejection, and if applicable, suggestion(s) for alternate approaches to satisfy the capability requirement. Disposition will be archived on the KM/DS system for visibility and reference purposes.

(c) Following VCJCS confirmation, JEONs are assigned to the appropriate Lead FCB for collaborative review with the JRAC in accordance with Enclosure G of this manual.

d. <u>Actions for Other Submissions</u>

(1) Study notices and reports

(a) Identify lead FCB and supporting FCBs as needed to align the study with the appropriate capability requirement portfolios.

(b) Ensure the purpose and description of the study are clearly articulated in the meta-data and the supporting documentation is included as part of the KM/DS record.

(c) Archive the notice/study in KM/DS and ensure notifications generated by the KM/DS system are sent to process participants including the sponsor, lead and supporting FCBs, Service and CCMD representatives.

(d) Note that while AoAs are a form of study, AoAs with approved CAPE AoA Study guidance do not require separate notice to be sent to the Joint Staff Gatekeeper. Visibility into CAPE approval of AoA Study Guidance serves to inform JCIDS stakeholders that an AoA is underway. AoAs or similar studies executed without CAPE AoA Study guidance will provide notice to the Joint Staff Gatekeeper.

(2) Post-AoA (or similar study) reviews, JROC/JCB Tripwire reviews, Nunn-McCurdy Unit Cost Breach reviews, and MAIS Critical Change reviews.

(a) Identify lead FCB and supporting FCBs as needed.

(b) In coordination with J-8/JRAD, J-8/CAD, and J-8/PBAD, the Joint Staff Gatekeeper assigns POCs, as required, to participate in the FCB review.

(c) Send the documentation to the lead FCB via KM/DS. The lead FCB will review the documentation, ensure the brief contains appropriate content, and schedule the follow-on activities (FCB WGs, FCB, JCB, JROC etc.) through the KM/DS calendar function.

(d) After the briefing cycle is complete, ensure the final briefing, appropriate notes, minutes and any associated JROCMs are attached to the record and archived in KM/DS.

(3) Updates to Sponsor validated capability requirement documents, and non-KPP changes to JCB or JROC validated capability requirement documents where non-KPP change authority has been delegated to the Sponsor.

(a) For changes to validated ICDs, CDDs, or CPDs:

1. Following Sponsor approval of the change in accordance with references hh through oo, the Sponsor submits the updated document to the Joint Staff Gatekeeper for assessment.

2. In coordination with J-8/JRAD, J-8/CAD, and J-8/PBAD, the Joint Staff Gatekeeper assigns POCs, as required, to participate in the FCB review.

3. The Joint Staff Gatekeeper forwards the revised document to the appropriate FCB(s) for assessment.

4. The Lead FCB and assigned AOs will evaluate the changes and determine if staffing is required. Changes that exceed the validation authorities' purview such as those affecting a non-delegated KPP, one or more certifications or endorsements, or other provision either implicit or explicit in a JROCM or other directive will require additional staffing.

5. If additional staffing is required, the Joint Staff Gatekeeper will provide initial review of the document as described in this enclosure, and will staff the document to the appropriate stakeholders in KM/DS.

6. If the lead FCB Chair determines the revision affects one or more certifications or endorsements, staffing is conducted through the appropriate stakeholders and certification or endorsement authorities to secure updated certifications or endorsements.

7. If staffing is not required, a description of the changes, rationale for the changes, and the revised document and its updated DOD Component validation memorandum will be posted in KM/DS and archived for future reference.

(b) For changes to DOD Component UONs: Following Sponsor approval of the change in accordance with references hh through oo, the Sponsor submits the updated and validated DOD Component UON to the Joint Staff Gatekeeper for archiving.

(4) Processing Sponsor requests for changes to previous validation, where the Sponsor is not the validation authority. Proposed updates/revisions to previously validated capability requirement documents shall be resubmitted by the Sponsor to the Joint Staff Gatekeeper for appropriate action. The staffing path will be determined by the type of document, the scope of the change, and the previously assigned JSD.

(a) For changes to validated ICDs, CDDs, CPDs, or Joint DCRs:

1. The Sponsor submits the updated document to the Joint Staff Gatekeeper for assessment.

2. The Joint Staff Gatekeeper assigns POCs from J-8/JRAD, J-8/CAD, and J-8/PBAD, as required, to participate in the FCB review.

3. The Joint Staff Gatekeeper forwards the revised document to the appropriate lead FCBs and certification/endorsement authorities for assessment.

4. The Lead FCB and assigned AOs will evaluate the change and determine if staffing is required.

5. If additional staffing is required, the change will go through the normal staffing process based upon its latest JSD.

6. If the lead FCB Chair determines the revision affects one or more certifications or endorsements, staffing is conducted through the appropriate stakeholders and certification or endorsement authorities to secure updated certifications or endorsements.

7. If additional staffing is not required, the lead FCB will work with the Sponsor to prepare a briefing for the JROC/JCB to obtain approval.

8. The lead FCB will schedule the briefing on the JCB and JROC calendars as required.

9. A revised validation memorandum is returned to the Sponsor once the revalidation has been completed or the original validation reconfirmed.

(b) For changes to validated JUONs or JEONs:

1. The Sponsor submits the updated document to the Joint Staff Gatekeeper, consistent with the classification level of the JUON or JEON and the guidelines outlined earlier in this enclosure.

2. The Joint Staff Gatekeeper forwards the updated document to the Lead FCB and JRAC for review.

3. The Lead FCB and JRAC will evaluate the change and determine if revalidation is required.

4. If required, the Lead FCB, in coordination with JRAC, will assess the proposed changes and make a validation recommendation to the validation authority.

5. A revised validation memorandum is returned to the Sponsor once the revalidation has been completed.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX A TO ENCLOSURE E

GATEKEEPING AND STAFFING METRICS

1. Overview. The Joint Staff Gatekeeper generates metrics related to the JCIDS Processes and posts to the KM/DS system for visibility and potential process improvement action. To the maximum extent practical, metrics are intended to be automated from data available within the KM/DS system – i.e. dates/times of document submittals and approvals, number of iterations, etc.

2. Gatekeeping Metrics

a. Percent of documents initially accepted/rejected by the Joint Staff Gatekeeper. Measure of quality of Sponsor document submissions.

b. Percent of documents, based upon CBAs or other studies, which had a study initiation notice posted to the KM/DS studies repository prior to study initiation and had study results posted to the KM/DS study repository prior to submitting document. Measure of Sponsor compliance with policy to facilitate collaboration on studies, reduce redundant study efforts, and enable leverage of historical studies.

c. Elapsed time from Sponsor document submission to the Joint Staff Gatekeeper assignment for staffing. Measure of Joint Staff Gatekeeper compliance with staffing timelines, and measure of contribution to overall staffing time metrics.

3. Deliberate Staffing/Validation Metrics

a. Elapsed time for FCB WG review. Measure of FCB WG compliance with staffing timelines, and measure of contribution to overall staffing time metrics.

b. Elapsed time for Sponsor comment adjudication. Measure of Sponsor compliance with staffing timelines, and measure of contribution to overall staffing time metrics.

c. Elapsed time for FCB Chair Review and validation recommendation. Measure of FCB compliance with staffing timelines, and measure of contribution to overall staffing time metrics.

d. Percent of documents receiving positive/negative FCB validation recommendations. Indirect measure of quality of Sponsor comment adjudication and/or indirect measure of significance of Sponsor proposed capability requirements to the capability requirement portfolio.

e. Elapsed time from FCB validation recommendation to validation by JCB or JROC. Measure of JCB/JROC compliance with staffing timelines, and measure of contribution to overall staffing time metrics.

f. Percent of documents validated/non-validated by validation authority. Indirect measure of FCB and validation authority alignment on intended direction for capability requirement portfolios.

g. Elapsed time from validation authority decision to signed JROCM being available in the KM/DS system. Measure of contribution to overall staffing time.

4. Urgent/Emergent Staffing/Validation Metrics. Note that the Joint Staff Gatekeeper maintains metrics on JUONs and JEONs. Generation of metrics for DOD Component UONs are at the discretion of the DOD Components.

a. Elapsed time for FCB WG and JRAC review. Measure of FCB WG and JRAC compliance with staffing timelines, and measure of contribution to overall staffing time metrics.

b. Percent of JUONs and JEONs receiving positive/negative FCB/JRAC validation recommendations. Indirect measure of significance of Sponsor proposed capability requirements to the capability requirement portfolio.

c. Elapsed time from FCB/JRAC validation recommendation to validation by the validation authority. Measure of validation authority compliance with staffing timelines, and measure of contribution to overall staffing time metrics.

d. Percent of JUONs and JEONs validated/non-validated by the validation authority. Indirect measure of FCB and validation authority alignment on intended direction for capability requirement portfolios and/or indirect measure of significance of Sponsor proposed capability requirements to the capability requirement portfolio.

5. Post Validation Metrics

a. Elapsed time from document validation to submission of successor document or fielding of capability solution(s). Measure of acquisition contribution to elapsed time.

b. Percentage of validated documents returning for revalidation due to JROC/JCB Tripwire review or Nunn-McCurdy breach review. Measure of Sponsor ability to meet validated capability requirements as proposed/validated.

c. Percentage of validated documents returning for revalidation due to Sponsor proposed changes to requirements. Measure of requirement stability.

d. For JUONs and JEONs, elapsed time from fielded solution to CCMD submission of an assessment of operational utility of the fielded capability solution. Measure of CCMD compliance with policy to facilitate feedback and facilitate assessment of merits (or lack thereof) of validation as enduring capability requirements.

e. For JUONs and JEONs, percent of rapidly fielded capability solutions receiving each of the assessment categories – success/enduring requirement, success/limited sustainment, or failed/develop alternate capability solution.

f. For JUONs and JEONs with assessments proposing enduring capability requirements, elapsed time from assessment to submission of CDD or CPD for validation of enduring capability requirements. Measure of transition percentage.

g. For DOD Component UONs, number of DOD Component UONs submitted to the Joint Staff Gatekeeper for visibility.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

ENCLOSURE F

DELIBERATE STAFFING PROCESS

1. Overview

a. Purpose. This enclosure provides the overview of the deliberate staffing process for capability requirement documents, as required by the Joint Staff Gatekeeper assigned JSD. The staffing process allows for robust review and validation of proposed capability requirements and other information relevant to development of capability solutions, ensuring that new or altered capability requirements are compatible with and collectively provide the best value to the joint force.

(1) ICDs, CDDs, CPDs, and related reviews, with Joint Staff Gatekeeper assigned JSDs of Joint Integration or Joint Information are reviewed and validated by a DOD Component validation authority, in accordance with references hh through oo.

(a) Sponsor processes must accommodate the time required to obtain applicable Joint Staff certifications or endorsements in accordance with Enclosure E of this manual.

(b) After validation, final versions of all Sponsor validated documents and their associated validation memoranda, including those for updated or changed requirements after initial validation, are submitted to the KM/DS system for information purposes and for visibility in the capability requirement portfolios.

(2) ICDs, Joint DCRs, CDDs, CPDs, and related reviews, with Joint Staff Gatekeeper assigned JSDs of JROC Interest or JCB Interest, other than Special Operations Peculiar (SO-P) documents assigned a JSD of JCB Interest, are reviewed and validated in accordance with this enclosure. See Figure F-1. SO-P documents assigned a JSD of JCB Interest are reviewed and validated in accordance with reference oo.

DRAFT

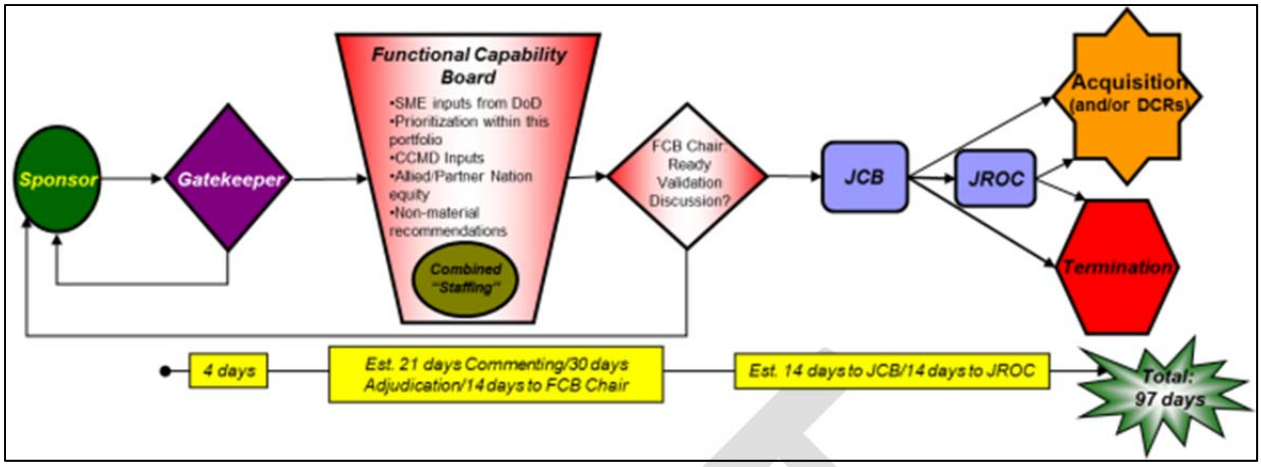

Figure F-1. Deliberate Staffing Overview

b. Staffing Timelines. The deliberate staffing process for a properly prepared capability requirement document takes no more than 97 calendar days.

(1) Requests for extensions to staffing timelines may be submitted to the Joint Staff Gatekeeper on a case-by-case basis.

(2) A document Sponsor may withdraw a document from staffing at any time during the staffing process, with notification to the Joint Staff Gatekeeper.

(3) While timely review and validation of capability requirement documents is a goal, the best measure of success for the staffing process is when the FCB Chairs, certification and endorsement organizations, and other stakeholders, have a clear understanding of and can recommend to leadership how a new or modified capability requirement and supporting data within the document represents the best tradeoff in performance, cost, schedule, and quantity to minimize unnecessary redundancy and meet the needs of the joint force.

c. Draft documents. All documents undergoing staffing are considered "draft" until validated by the validating authority, and the associated validation memorandum attached to the document as a validation page.

d. Tailored staffing. Staffing processes for post-AoA (or similar study) reviews, certifications and endorsements of documents with JSDs of Joint Integration, and review of other requirements related issues follow a similar staffing process, but may omit or tailor various steps as applicable.

e. JCB and JROC procedures. Once documents or issues are recommended by the FCB Chair for presentation to the JCB or JROC, specific

preparation and formatting procedures are required. See reference mmmmmm.

2. Pre-Staffing

a. Initiation. The deliberate staffing process begins when the Joint Staff Gatekeeper completes preliminary activities described in Enclosure E, and initiates staffing of the document or issue. Pre-staffing review of documents is conducted for four calendar days.

b. Initial review. Selected stakeholders may be asked by the Joint Staff Gatekeeper to provide an initial review of a document or issue as part of activities described in Enclosure E, but such actions do not initiate formal staffing in accordance with this enclosure.

c. Early engagement with stakeholders. Sponsors are encouraged to engage with any of the stakeholders of the JCIDS process at any time prior to staffing to help ensure that capability requirement documents are developed in a way that will not require significant rework during staffing. This is particularly important in cases where the Sponsor intends to request waivers of any certifications or endorsements, or other deviations from the process as allowed by reference b.

3. Staffing of Draft/Initial ICDs, Joint DCRs, CDDs, and CPDs

a. Document Review and Commenting Stage. 21 Days.

(1) Initial staffing of documents is conducted with documents available to Services, CCMDs, and other DOD Components, as well as certifying/endorsing organizations and other stakeholders, for review and commenting. For SAP/SAR or ACCM protected documents, the J-8/SAPCOORD and Joint Staff Gatekeeper will ensure appropriately cleared AOs and FCB Chairs with equity in the document are read-in to the program and related program(s) in the capability requirement portfolio(s) as needed to review and comment on the document.

(2) Primary Stakeholders in Document Review

(a) Capability requirement documents contain content which is of interest to, or may have impact upon, many different stakeholders across the joint force in addition to the Services and CCMDs, including but not limited to those shown in Table F-1.

(b) It is critical that stakeholders review and comment upon capability requirement documents to ensure that proposed new capability requirements or changes to previously validated capability requirements are

aligned with the needs of the joint force. As capability requirement documents are intended to address operational needs, comments from stakeholders should be only those required to ensure alignment with the overall needs, priorities, and policies of the joint force, and not unduly replicate content which exists, or should exist, in other documents or policies.

Capability Requirement Documents			**Section Primary Equities**	
ICD	**Joint DCR**	**CDD/CPD**	**Joint Staff**	**Other/Advisors**
Operational Context	Operational Context	Operational Context	J3/J5	CAPE (for ISCs)
Threat Summary	Threat Summary	Threat Summary	J-2/IRCO	USD(I)
Capability Requirements / Capability Gaps	Capability Discussion	Capability Discussion	FCBs, J-8/JRAD, J-8/CAD, J-8/PBAD	MDA, ASD(A), ASD(R&E), ASD(L&MR), USD(I), DOD CIO, DASD(T&E), DOT&E
		Program Summary		
		KPPs/KSAs/APAs Other Attributes		
		Mandatory KPPs	J8/FPD, J4/MXD, J6/C4CD, J4/ED	DASD(MR), DOD CIO, ASD(OEPP)
		Spectrum Requirements	J-6/C4CD	DOD CIO, USD(AT&L) – C3 & Cyber
		Intelligence Supportability	J-2/IRCO	USD(I)
		Weapon Safety Assurance	JWSTAP	ASD(L&MR)
		Technology / Manufacturing Readiness	FCBs, J-8/JRAD, J-8/CAD, J-8/PBAD	ASD(R&E)
Non-materiel Approaches	Change Recommendations	DOTmLPF-P Considerations	J-1, J-4, J-5, J-7, J-8/FD	USD(P), USD(P&R), ASD(L&MR)
Recommendations	Resource Summary	Program Affordability	Validation Authority	MDA, CAPE

Table F-1. Primary Equities in Capability Requirement Documents

(c) The review by stakeholders should not be a cursory evaluation of content and formatting, but rather inform both:

1. A robust understanding of implications to the warfighter and the capability requirement portfolios, to inform comments to the Sponsor and discussion with the FCB and FCB WG during staffing.

2. A robust understanding of how validation of the capability requirements may impact stakeholder processes and other equities.

(d) Key points for stakeholders to understand include, but are not limited to:

1. What problem are we trying to solve and for whom? What CCMDs are impacted, and are they supportive of the proposed changes? What is the timing of the capability requirements and why?

2. What operational risks, and for what missions/tasks, is the joint force buying down with a proposed capability solution to identified capability requirements and associated capability gaps? For CDDs and CPDs, are the KPPs, KSAs, and APAs traceable to the operational tasks and capability requirements they support, and do the KPPs reflect the parameters most critical to mission effectiveness, in accordance with Appendix A to Enclosure D of this manual?

3. What joint alternatives could be pursued in lieu of developing a new capability solution? What missions/tasks cannot be completed by any alternatives across the joint force while a capability solution is developed?

4. Where is the "knee in the curve" for cost/performance tradeoffs? Who has conducted independent review or analysis, and do we understand the reasons for any differences in results?

5. Where is the money coming from? Unless sustained budgetary increases will fund the capability solution over its life cycle, what other capabilities will be reduced or eliminated to provide resources for a new capability solution? What are the operational risks, or missions/tasks that cannot be performed, that result from these choices?

6. If the capability requirements are validated in the JCIDS process, what implications result for stakeholder processes and other equities?

(3) Joint Staff certifying and endorsing organizations. Each of the organizations responsible for certifications or endorsements, as identified in Enclosure E to this manual, reviews documents and provides comments if changes to the document are required prior to providing the certification or endorsement.

(a) In cases where a certification or endorsement is not applicable to a specific document, these organizations will provide a waiver stating that their certification or endorsement is not required.

(b) Comments from the certifying or endorsing organization are authoritative with respect to their certification or endorsement. Other stakeholders should submit comments related to the certification or endorsement via the certifying or endorsing organization for potential inclusion in the authoritative direction.

(4) Comment Submission. All comments are due by the end of the initial staffing period.

(a) Substantive or Critical comments submitted in response to staffing are expected to be signed out at the GO/FO or SES, level. Administrative comments may be signed out at the O-6 or GS-15 level.

(b) Organizations/agencies making comments as part of staffing will coordinate comments through a single organizational gatekeeper.

(c) Comment Submission. Comments are submitted in a manner dependent upon their classification level and ACCM or SAP/SAR protections, as outlined in Enclosure E of this manual.

b. Comment Adjudication Stage. 30 Days.

(1) Following initial review and commenting, the Sponsor adjudicates comments.

(a) Comments against documents with JSDs of JROC interest or JCB Interest must be adjudicated to the satisfaction of the FCB Chair (on behalf of the JCB/JROC) and the Joint Staff certifying or endorsing organizations.

(b) Comments against documents with JSDs of Joint Integration must be adjudicated to the satisfaction of the DOD Component validation authority and the Joint Staff certifying or endorsing organizations.

(c) Comments against documents with JSDs of Joint Information must be adjudicated to the satisfaction of the DOD Component validation authority. It is at the discretion of the DOD Component validation authority whether documents with JSD of Joint Information will be:

1. Validated prior to receiving comments, and then revalidation considered if any comments are to be incorporated.

2. Validation withheld during the comment and adjudication periods to allow any applicable comments to be incorporated before final validation decision.

(2) Sponsors are to work with stakeholders to adjudicate comments to the greatest extent possible during the comment adjudication stage. Comments which remain unadjudicated to the satisfaction of the stakeholder will require attention later in the staffing process, and may delay or stop staffing of the document.

(3) Upon completion of comment adjudication, the Sponsor submits the revised document, along with disposition of all comments and status of any unresolved comments. The revised document does not require re-staffing

unless the lead FCB Chair deems the updated document not ready for validation and recommends that the Joint Staff Gatekeeper restart the staffing process.

c. FCB WG and FCB Review Stage. 14 Days.

(1) General

(a) The most critical aspect of the FCB review stage is for the FCB Chair to ensure that proposed new capability requirements, changes to previously validated capability requirements, or adjudication of other issues, provide best value to the warfighter without unnecessary redundancy in the capability requirement portfolio, and align with the priorities of the joint force.

(b) Following Sponsor comment adjudication, the FCB reviews the revised document, ensure certifying or endorsing organizations concur with Sponsor adjudication of comments, and assists the FCB Chair in reaching a recommendation for the JCB or JROC. Specifically, the FCB WG and FCB are forums for identifying and discussing divergent stakeholder views. While consensus is not required to move an issue forward to the next level of review, all dissenting views will be captured and briefed to inform decision makers.

1. For capability requirement documents falling primarily within a single FCB, the FCB Chair makes the recommendation to the JCB or JROC. For capability requirement documents protected by ACCM or SAP/SAR designation, the FCB Chair makes the recommendation based upon review and assessment by a subset of appropriately cleared AOs.

2. For capability requirement documents not protected by ACCM or SAP/SAR designation, with equity spread across multiple FCBs, the lead FCB Chair will either coordinate efforts directly with the supporting FCB Chair(s) or utilize the O6 and GO/FO Integration Groups to coordinate interdependent efforts before making the recommendation to the JCB or JROC.

3. For capability requirement documents protected by ACCM or SAP/SAR designation, with equity spread across multiple FCBs, the J-8/DDR will consolidate inputs from individual FCB Chairs and their AOs, and any other participating reviewers, and makes the recommendation to the JCB or JROC.

(c) Certifying and endorsing organizations use the same time period to review the revised document, and provide a memorandum which either: certifies or endorses the document; withholds certification or endorsement of the document, with identification of specific unadjudicated issues which must be resolved to gain certification or endorsement; or waives the need for the certification or endorsement.

(2) The lead FCB forms a FCB WG from lead and supporting FCBs, as well as applicable subject matter experts from across DOD, to review each document in staffing. Assessing a capability requirement document may include, but is not limited to:

(a) Comparison of proposed capability requirements within the document against previously validated capability requirements, development programs, and fielded capability solutions within their capability requirement portfolio(s). For CDDs and CPDs, verification that the KPPs, KSAs, and APAs are traceable to the operational tasks and capability requirements they support, and that the KPPs reflect the parameters most critical to mission effectiveness in accordance with Appendix A to Enclosure D of this manual.

(b) Consideration of how the proposed capability requirements align with any EAs associated with the capability requirement portfolio(s), closing associated capability gaps without introducing unnecessary redundancy in capability or capacity.

(c) Consideration of how the proposed capability requirements address issues identified in the most recent CRA or output of the most recent CGA.

(d) Consideration of how the proposed capability requirements may impact previously fielded systems or developmental efforts, and whether or not those impacts have been coordinated with the affected organizations and associated costs accounted for in the affordability portion of the document. E.g. – a new munition program may not provide the intended capability if the integration efforts and associated costs have not been coordinated with the intended threshold delivery system.

(e) Evaluation of the potential for the capability requirements or resulting capability solutions to support the joint warfighter, including roles and missions of other DOD Components not necessarily identified by the Sponsor – either by leveraging the same capability solution or by realigning organizational roles and missions.

(f) Reviewing all critical comments not adjudicated to the satisfaction of commenter.

1. For critical comments submitted by FCB members or certifying and endorsing organizations, lack of suitable adjudication may be grounds for the FCB to withhold recommendation for validation of the document.

2. For critical comments submitted by any stakeholders, those not adjudicated to the satisfaction of the commenter will be summarized for review by the validation authority prior to a validation decision.

(g) In cases where a submitted ICD, CDD, or CPD represents an unnecessary redundancy to previously fielded capability solutions in the joint force, the FCB review may include:

1. Recommending that no action be taken on the capability requirements in cases where the likely costs associated with providing a capability solution outweigh the operational risk of leaving the capability gap unmitigated.

2. Recommending non-materiel changes to partially or wholly address the capability requirements and associated capability gaps. To facilitate review of DOTmLPF-P considerations and interaction with other stakeholders, a J-7/DDI representative will participate as a member of the Lead FCB WG, and will raise issues for discussion, as necessary, related to the DOTmLPF-P endorsement.

3. Recommending other US government agency/department or allied/partner nation collaboration to partially or wholly address the capability requirements and associated capability gaps. To facilitate review of other US government agency/department or allied/partner nation collaboration opportunities, the Lead FCB will work with representatives from J-5 and the USD(AT&L) International Cooperation (IC).

(3) The FCB Chair is ultimately responsible for providing a positive or negative validation recommendation to the validation authority.

(a) When submitting a positive validation recommendation to the JCB or JROC, the FCB Chair is certifying that the capability requirements, and proposed capability solutions if applicable, articulated in the document are not unnecessarily redundant to previously fielded capability solutions in the joint force and provide best value to the warfighter. Positive validation recommendations will also summarize life cycle cost, schedule, and quantity parameters, as appropriate for the document.

(b) When submitting a negative validation recommendation to the JCB or JROC, the FCB Chair will provide the associated justification such as non-alignment with the needs of the capability requirement portfolio, lack of one or more certifications or endorsements, unresolved critical comments, etc. Unless the document is withdrawn by the Sponsor, the FCB Chair will ensure that the JCB Chair is made aware of any ongoing efforts to reach a positive validation recommendation.

d. Validation Stage. 14 Days for JCB Interest. 28 Days for JROC Interest.

(1) The validation stage begins when the FCB Chair provides a positive validation recommendation.

(2) The FCB Chair or Lead briefs the validation authority with any related s for discussion, along with the recommendation for or against validation. Sponsors/SMEs may be present to answer questions of a technical nature but are not to brief FCB assessments, issues, or recommendations on behalf of the FCB Chair.

(a) In cases where there are critical comments from staffing or the FCB WG and FCB deliberations which are not adjudicated to the satisfaction of the commenting organization, or where any of the required certifications or endorsements have not been obtained, the FCB Chair or Lead shall present the dissenting comments or issues for discussion. An appropriate level GO/FO or SES representative from the dissenting organization should be present at the JCB and JROC to engage in the discussion.

(b) In cases where there are no issues for discussion, and the recommendation is for validation, the FCB chair may recommend a "paper" JCB and/or JROC in lieu of a physical meeting of the validation authority.

(3) In support of reference cc, the validation authorities identified in this section provide validation that:

(a) The capability requirements and proposed IOC/FOC for capability solutions meet the national military strategy and the needs of the CCMDs.

(b) The capability requirements address the priorities of the joint force and do not represent unnecessary redundancy in capabilities.

(c) Capability solutions have had appropriate consideration of tradeoffs between life cycle cost, schedule, performance, and quantity.

(d) Estimated total cost of resources required to satisfy the capability requirement are consistent with the priority of the capability requirement.

(e) In accordance with reference nnnnnn, validation includes agreement that the identified Service(s) will support implementation action and/or funding in related processes. In cases where changes to operations, threats, priorities, or fiscal environment may impact prior agreement to support implementation and/or funding, the Sponsor may return to the

validation authority for review and potential adjustment of capability requirements before POM decisions are finalized.

(4) The JROC is the validation authority for all documents that have a JSD of JROC Interest.

(a) The JROC may assert itself as the validation authority for any document of any assigned JSD at any time by directing the Joint Staff Gatekeeper to set the JSD to JROC Interest.

(b) As an advocate for DOTmLPF-P considerations during validation discussions, Director J-7 (DJ-7) or designee will be present for JROC discussions.

(c) The JROC may elect to validate a document through a "Paper JROC" without physically convening, when the FCB and JCB Chairs recommend validation and there are no issues for JROC discussion.

(5) The JCB is the validation authority for all documents that have a JSD of JCB Interest.

(a) The JCB may assert itself as the validation authority for any document with a JSD other than JROC Interest at any time by directing the Joint Staff Gatekeeper to set the JSD to JCB Interest.

(b) As an advocate for DOTmLPF-P considerations during validation discussions, Vice Director J-7 or designee will be present for JCB discussions.

(c) The JCB may elect to validate a document through a "Paper JCB" without physically convening, when the FCB Chair recommends validation and there are no issues for JCB discussion.

(6) The Sponsor is the validation authority for all documents given a JSD other than JROC Interest or JCB Interest.

(7) In validating an ICD, the validation authority:

(a) Validates the document, including the capability requirements and initial objective values, associated capability gaps, and supporting data in the capability requirement document.

(b) Supports the recommended approach(es) to meet the validated capability requirements and close or mitigate the capability gaps.

(c) Includes, where applicable, recommendations for development of the AoA guidance, in support of reference bb.

(8) In validating a CDD or CPD, the validation authority:

(a) Validates the document, including the KPPs, KSAs, and APAs, their associated threshold and objective values, and supporting data in the capability requirement document.

1. For JROC Interest or JCB Interest CDDs and CPDs, the JROC or JCB generally delegates non-KPP change authority to the Sponsor validation authority, with the provision that any subsequent changes be provided to the Joint Staff Gatekeeper for visibility.

2. The JROC or JCB may also retain change authority for all changes, or delegate a different set of change authorities, at their discretion.

(b) Ensures that the capability solution being developed (in accordance with the CDD) or produced (in accordance with the CPD) contributes toward satisfying or satisfies the validated capability requirements and closes or mitigates associated capability gaps.

(b) Assesses the risks in meeting those performance attributes in terms of life cycle cost, schedule, and technological maturity.

(c) Assesses the affordability of the system as compared to the capability solution being delivered, and may consider other alternatives to the proposed capability solution. For CPDs, and changes to previously validated CDDs, significant changes from previous resource projections will warrant extra scrutiny by the validation authority.

(d) Sets parameters on PAUC or APUC, IOC and FOC dates, and procurement quantities. If the resulting program deviates from the specified parameters the requirements may be subject to JROC/JCB Tripwire review procedures, outlined in this enclosure and Enclosure B of this manual, to ensure that the program is still in the best interest of the joint force to satisfy the validated capability requirements, and that the impact – in terms of extended sustainment of legacy systems and/or reduced funding for other programs – represents reasonable risk.

e. Post-Validation Documentation

(1) Validation decisions by the JROC or JCB are documented via JROCM and are signed by the JROC Chairman or designee. Validation decisions by Sponsors and final versions of all validated requirement documents are uploaded to the KM/DS system for information purposes and visibility in the capability requirement portfolios.

(a) The final version of the validated document will incorporate changes to the capability requirements and/or supporting information as directed or agreed to during staffing.

(b) In cases where validation of new or modified capability requirements impose changes to other previously validated capability requirements, the JROCM may document changes for the other system(s) which have been agreed upon during staffing. This negates the need for separate rounds of staffing and separate JROCMs for each affected system.

(c) For Joint DCRs, the validation memorandum will also formalize the assignment of OPRs as agreed to during staffing.

(d) The validation decision memorandum will be inserted behind the cover page of the capability requirement document itself, replacing the validation page placeholder if one was part of the draft document. A capability requirement document without the associated validation memorandum attached shall be considered draft and not yet usable for follow-on activities.

(e) For recordkeeping, updated documents and associated validation memoranda classified at or below the level of SECRET are uploaded to the KM/DS system. Documents and associated validation memoranda classified at a level higher than SECRET are provided to the Joint Staff Gatekeeper via JWICS or via the J-8/SAPCOORD, depending upon classification.

(2) Consistent with the type of document being validated, positive validation decisions will:

(a) Summarize the PAUC and APUC, IOC/FOC schedule, and quantity.

(b) Identify any applicable changes to capability requirements associated with other capability solutions which are a result of the validation of the new or updated capability requirements.

(3) Sponsorship of a document may change as a result of staffing, upon the recommendation of the lead FCB and positive validation decision.

(4) Any changes made which relate directly to the substance of the document or certifications/endorsements – including KPPs, life cycle cost, schedule, and/or quantity – render the document invalid for the purpose of any follow-on processes until revalidated by the validation authority.

(5) The validation authority may rescind a previous validation and/or direct changes to or re-staffing of a validated document at any time. The

validation authority will notify the document Sponsor in writing, with rationale for the rescission.

4. Staffing of Changes to Previously Validated Documents. The scope of staffing required for changes to previously validated documents is determined by initial Joint Staff Gatekeeper review as outlined in Enclosure E.

a. Abbreviated staffing. For changes not requiring full staffing, document review/commenting and comment adjudication stages may be omitted. The updated document will be provided at least 7 days ahead of the scheduled FCB WG meeting, and stakeholders may discuss issues/comments at the FCB WG meeting.

b. Staffing for certifications or endorsements. For changes that affect one or more certifications or endorsements, document review/commenting and comment adjudication is required but may be expedited. The updated document will be provided at least 21 days ahead of the scheduled FCB WG meeting.

(1) Certifying or endorsing organizations have 7 days to assess the impact of changes to previously provided certifications and endorsements. If changes are required, they will provide comments to the Sponsor within 7 days.

(2) The Sponsor has 14 days to adjudicate comments to the satisfaction of the certifying or endorsing organizations. The resulting updated document will be provided to the Joint Staff Gatekeeper prior to the FCB WG meeting.

c. Full staffing. For changes deemed to require robust review, full staffing will be conducted as if the document were an initial/draft document.

d. Focus of staffing for proposed changes. When changes to previously validated documents are in staffing, comments will be made only upon the alterations or impacts thereof (such as to certifications or endorsements), unless the Joint Staff Gatekeeper has determined that revalidation of the entire document is appropriate, such as for changes in strategic guidance, operational context or other factors which suggest a more comprehensive review is appropriate.

5. Staffing of Post-AoA (or Similar Study) Reviews

a. Abbreviated staffing. For post-AoA (or similar study) reviews, the document review/commenting and comment adjudication stages applicable to review of capability requirement documents may be omitted. The final AoA report and any supporting data/analyses will be provided to the Joint Staff Gatekeeper at least 7 days ahead of the scheduled FCB WG meeting, and stakeholders may discuss issues/comments at the FCB WG meeting.

b. Focus of a post-AoA (or similar study) review. Following an AoA which addresses validated capability requirements in JROC or JCB Interest ICDs, the appropriate FCB(s) and other stakeholders will review the AoA and Sponsor's preferred alternative(s), and other applicable analyses completed during the MSA phase of acquisition. Assessments may include, but are not limited to:

(1) Assessment of how each alternative would or wouldn't contribute to satisfying the validated capability requirements and associated operational context, and whether or not any changes to assumptions or discriminators would be appropriate and provide better value to the joint force.

(2) Assessment of how mandatory KPPs and/or Intelligence Supportability concerns, critical dependencies/enablers, and other DOTmLPF-P impacts were considered as potential discriminators between alternatives, and how they affected the cost of pursuing each alternative.

(3) For the alternative recommended by the Sponsor, the degree to which the KPPs, KSAs, and APAs proposed by the Sponsor contribute to satisfying the validated capability requirements and associated operational context. The KPPs, KSAs, and APAs presented in the post-AoA (or similar study) review will also be consistent with and used to derive:

(a) The RFP for the TMRR phase of acquisition.

(b) Other documentation required at MS A, including the updated CONOPS and/or OMS/MP documentation containing operational tasks, events, durations, frequency, operating conditions and environment in which the recommended materiel capability solution is to perform each mission.

(c) The KPPs, KSAs, APAs, and other associated information shall be captured in a Sponsor developed and approved draft CDD, not submitted to the Joint Staff Gatekeeper for staffing and validation at this time, to inform the discussion and decision making at MS A. Data provided by the solution Sponsor must include, but is not limited to:

1. Any applicable updates to the operational context (CDD Section 1), with focus on the summary of the Service and joint concepts and/or CONOPS.

2. Notional program summary (CDD Section 4), with focus on the synchronization of SoS efforts across other CDDs, CPDs, and DCRs, and identification of dependencies on any legacy or future enabling capabilities.

3. Development KPPs, KSAs, and APAs (CDD Section 5), with focus on the initial/draft performance attributes resulting from the AoA or

similar studies. Initial/draft performance attributes for the five mandatory KPPs, or justification for why they are not applicable, must also be provided.

4. Other System Attributes (CDD Section 6), with focus on attributes which require significant efforts during the TMRR phase of acquisition.

5. Technology Readiness Assessment (CDD Section 10), with focus on the critical technology elements (CTEs) which need to be matured during the TMRR phase of acquisition.

(4) Assessments in the post-AoA (or similar study) review are facilitated in part by comparing draft DODAF SV-3 and SV-8 views, generated for the recommended alternative coming out of the AoA, with the DODAF OVs and CVs associated with the validated ICD.

(5) Following the assessment, the FCB Chair prepares to brief the JCB and/or JROC, with the solution Sponsor available as a Subject Matter Expert (SME), on the Sponsor's AoA (or similar study) results and preferred alternative(s) as well as the FCB assessment, including any alternative recommendations or trade-offs deemed appropriate by the FCB. This facilitates the JCB or JROC providing informed advice to the MDA on the best approach to satisfy the capability requirement(s).

6. Staffing of JROC/JCB Tripwire and CIP Breach Reviews. See Enclosure B of this manual for additional considerations related to Tripwire reviews.

a. Overview. The JROC/JCB Tripwire review process is illustrated in Figure F-2 and is initiated when one or more cost, schedule, or quantity parameters set in the validation JROCM are exceeded. Note that CIP Breach reviews follow this same general process when evaluating impacts of CIP changes, but are initiated under different conditions and by different organizations.

DRAFT

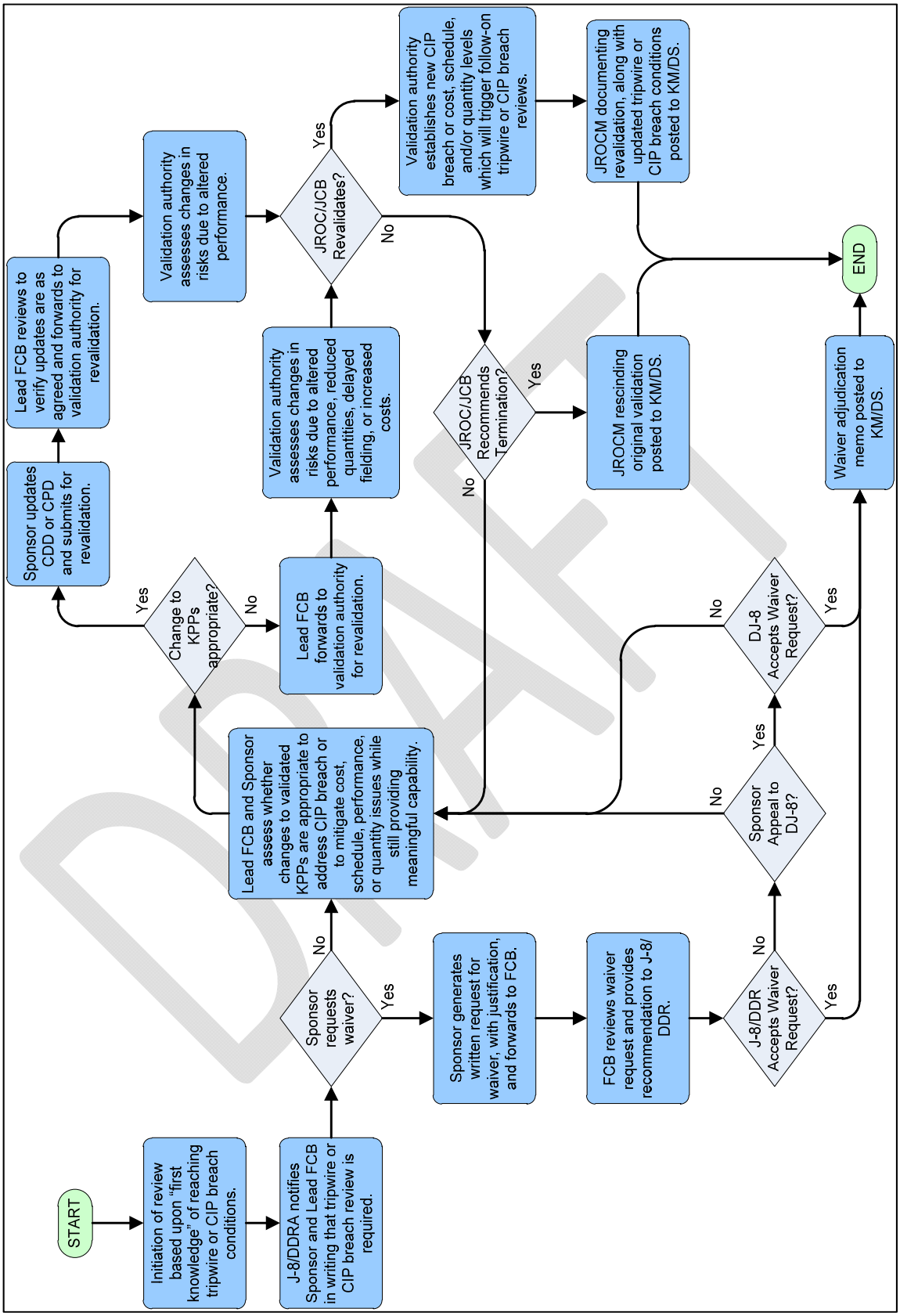

Figure F-2. JROC/JCB Tripwire and CIP Breach Review Process.

b. Initiation

(1) JROC or JCB Tripwire Reviews. The J-8/CAD or J-8/PBAD initiates a JROC/JCB Tripwire review based upon "first knowledge" of PAUC and APUC, schedule, and/or quantity changes reaching the trigger values outlined in the validation JROCM, and providing notification to the Joint Staff J-8, Deputy Director for Resources and Acquisition (J-8/DDRA). The J-8/DDRA will notify the Sponsor and the Lead FCB in writing that trigger conditions have been met and that a JROC/JCB Tripwire review is required. First knowledge of a trigger condition is usually determined by, but not limited to, one of the following events:

(a) POM or Budget Reviews.

(b) Program restructures.

(c) JCIDS Reviews.

(d) Defense Acquisition Executive Summary (DAES) Reviews.

(e) Overarching Integrated Process Teams (OIPTs).

(f) Selected Acquisition Reports (SARs).

(g) Program Deviation Reports or changes to APBs.

(h) MAIS Quarterly Reports.

(2) CIP Breach Reviews. The IC initiates a CIP Breach review when the supporting military Service Intelligence center determines a CIP has been breached, and notifies the appropriate offices in DoD, and the program office(s) and FCB(s) impacted by the breach.

c. Review

(1) The lead FCB, together with other stakeholders involved in the review and validation of the capability requirements, will work with the Sponsor to assess whether an adjustment to validated KPPs is appropriate to mitigate the tripwire or breach conditions, while still providing meaningful capability for the warfighter.

(a) A key aspect of this review is a robust understanding of the impact to UJTs enabled by the capability solution and impact to critical enablers/dependencies. Discussions and briefings related to the review will

include impacts to both the program under review as well as other impacted programs within and across the portfolios.

(b) This understanding of impacts is facilitated by review of the applicable DODAF OVs, CVs, and SVs, in particular the OV-5a (UJTs), CV-3 (time sequenced capability requirements), SV-3 (KPPs), and SV-8 (time sequenced dependencies/enablers).

(2) In cases where adjustment of KPPs is appropriate, the Sponsor will generate an updated CDD or CPD and submit for revalidation. The Lead FCB will forward the updated document to the validation authority for review and revalidation.

(3) In cases where adjustment of KPPs cannot mitigate the tripwire or breach conditions, the validation authority will re-evaluate the operational risks associated with the delayed and/or decreased capabilities offered by the program, and consider whether any alternatives are more appropriate to satisfy the original capability requirements.

(4) The validation authority will assess the potential impact to other capability solutions which are dependent on or enablers for the capability solution under JROC/JCB Tripwire review, and resulting changes to operational risk.

(a) If revalidated, the validation authority will also establish:

1. For JROC or JCB tripwire reviews, new PAUC and APUC, schedule, and/or quantity levels which will trigger follow-on JROC/JCB Tripwire reviews if the program experiences further changes.

2. For CIP breach reviews, new CIP breach levels which will trigger follow-on CIP breach reviews if the adversary further advances their capabilities relevant to the CIP.

(b) If not revalidated, the validation authority will either recommend the Sponsor and Lead FCB consider alternate approaches to mitigation, or will rescind the original validation.

(5) Elapsed time between written notice and final adjudication by the validation authority will not exceed 75 calendar days.

d. Waiver. In cases where a Sponsor receives notice from the FCB but does not believe a JROC/JCB Tripwire or CIP breach review is necessary, the Sponsor may submit a written request, with justification, to the FCB for relief.

(1) The FCB will review the Sponsor's justification and provide a recommended disposition to the J-8/DDR.

(2) The J-8/DDR is the approval authority for JROC/JCB Tripwire or CIP breach review relief. If J-8/DDR does not approve the request, the Sponsor may appeal to DJ-8 for final decision.

(3) If approved, a waiver memo is retained in the KM/DS system, and if applicable, establishes new PAUC and APUC, schedule, and/or quantity levels for follow-on JROC/JCB Tripwire reviews or new CIP breach levels for follow-on CIB Breach reviews. If not approved, the FCB review begins within 30 calendar days.

e. Other review authority. JROC/JCB Tripwire and CIP breach reviews do not preclude a validation authority from, at any time, requiring a review of previously validated requirements or programs by directly communicating to the applicable Sponsor, outlining the review requirements, timeline, and other details.

(1) The JROC and JCB issue review notification via JROCM.

(2) The J-8/DDR issues review notification via memorandum.

(3) Other independent validation authorities are not required to have similar review procedures, but may issue similar review notifications in accordance with their internal processes.

7. Staffing of Nunn-McCurdy Unit Cost Breach and MAIS Critical Change Reviews

a. Statutory basis. These reviews of acquisition programs are required by statute, as outlined in references dd and ee.

b. Initiation. Nunn-McCurdy Unit Cost Breach reviews are initiated when:

(1) When MDAPs experience cost growth of 15 percent from their current baseline or 30 percent from their original baseline, they are in a "significant" Nunn-McCurdy Unit Cost Breach. Sponsors must notify Congress within 45 calendar days after the report (normally program deviation report) upon which the determination is based. Sponsors must also submit a SAR with the required additional unit cost breach information.

(2) When MDAPs experience cost growth of 25 percent from their current baseline or 50 percent from their original baseline, they are in a "critical" Nunn-McCurdy Unit Cost Breach. Programs in "critical" breach status are subject to detailed review for potential termination.

c. Criteria. MAIS Critical Change reviews are initiated when:

(1) When MAIS programs experience cost growth of 15-25 percent in program development cost or total life cycle cost; experience a 6-12 month delay in schedule; or are expected to have a significant adverse change in performance, they are in a "significant change" status. Sponsors must notify Congress within 45 calendar days after receiving the PM's MAIS Quarterly Report (MQR) upon which the determination is based.

(2) When MAIS programs experience cost growth of more than 25 percent in program development cost or total life cycle cost; experience greater than a 12 month delay in schedule; are expected to be unable to meet a KPP or otherwise be unable to perform the intended mission; or will not achieve Full Deployment Decision (FDD) within five years of when funds were first obligated for the program, they are in a "critical change" status. Programs in "critical change" status are subject to detailed review for potential termination. Sponsors must notify Congress within 45 calendar days after receiving the PM's MQR upon which the determination is based.

d. Review teams. USD(AT&L) organizes integrated process teams (IPTs) to assess national security impact, analyze alternatives, estimate life cycle costs and review management structure. More detail on Nunn-McCurdy Unit Cost Breach and MAIS Critical Change review procedures are in references aa, bb, and ff.

e. JROC participation. The JROC and its subordinate boards participate in these reviews in order to review the relevant capability requirements and associated capability gaps and operational risks, and provide recommendations with respect to the essentiality of the program to satisfying capability requirements which are critical to national security.

(1) Upon notification by the Joint Staff Gatekeeper of a Nunn-McCurdy Unit Cost Breach or MAIS Critical Change review, the lead (and supporting, if necessary) FCB, together with other stakeholders involved in the review and validation of the capability requirements, will initiate a review of their capability requirement portfolios to assess the impact of the program in question upon capability requirement(s) in their capability requirement portfolio.

(2) Focus of the reviews must be on the essentiality of the program to satisfying capability requirements which are critical to national security. This part of the review should begin with examination of the DODAF OV-5a (UJTs) and CV-3 (time sequenced capability requirements) associated with the program and comparison to similar capabilities within the capability requirements portfolio. Alternative CONOPS or alternative capability solutions should also be considered.

(3) As time will have passed since the validation of the original capability requirements upon which the program was established, review of strategic guidance, DIA- or Service-approved threat products, and/or other aspects of operational context may be necessary before evaluating the essentiality of the program.

8. Staffing of Other Reviews or Issues

a. Tailored staffing. Any other requirements related reviews or issues to be considered by the JROC or any of its subordinate boards may use variations of the basic staffing process. Tailoring of the staffing process or adaptation of alternative staffing processes for issues or reviews not specifically outlined above are at the discretion of the Joint Staff Gatekeeper.

b. Examples. Assessing other issues submitted for staffing may include, but is not limited to:

(1) Assessment of how an issue and associated COAs may affect previously validated capability requirements, development programs, and fielded capability solutions within their capability requirement portfolio(s).

(2) Consideration of how an issue may impact any operational architectures associated with the capability requirement portfolio(s).

DRAFT

APPENDIX A TO ENCLOSURE F

ENDORSEMENT GUIDE FOR WEAPON SAFETY

1. Purpose

a. This guide provides the policies and procedures for the weapon safety review and endorsement of weapons-related capability requirement documents. The endorsement ensures that capability requirement documents adequately address the weapon safety requirements necessary for munition life cycle management, including the safe use in the joint operating environment (JOE), as well as packing, handling, storage, transportation, and destruction/de-mil.

b. This guide provides procedures to engage the JWSTAP, established in accordance with reference jjjj, as a source of expert consultation regarding weapon safety within the JOE for document Sponsors and the Joint Staff J-8, Deputy Director for Force Protection (J-8/DDFP). The JWSTAP will collaborate with program sponsors and the J-8/DDFP to develop possible solutions to weapon safety issues. Consultation in the development and review of capability requirement documents may be both prior to formal submittal into the JCIDS process and during the staffing process.

c. ORDs for previously fielded weapons that are being converted to CDDs or CPDs, with no change in capability, in support of MS B or MS C decisions, are exempt from the JWSTAP review process.

d. Any substantive changes to this guide will be coordinated with and approved by the DJ-8 or designee.

2. Weapon Safety Review

a. These reviews will focus on identifying potential safety issues resulting from munition life cycle management, including interactions between the proposed weapon and the JOE, handling, packaging, transportation, destruction/de-mil, assembly, disassembly, maintenance, testing, storage, and use of the weapon system.

b. The JWSTAP, on behalf of the J-8/DDFP and based on the information provided in the capability requirement document under review, accomplishes the following:

(1) Identifies potential safety issues associated with the proposed capability requirements in joint warfighting environments.

(2) Coordinates with the DOD Explosives Safety Board to coordinate with reviews conduced in accordance with reference kkkk.

(3) Develops recommended revisions to the document language to reduce or eliminate the identified safety concerns while maintaining the desired operational effectiveness.

(4) Advises the J-8/DDFP and FCBs in support of a JROC review of the capability requirement document.

c. The JWSTAP provides to the J-8/DDFP a WSE recommendation for each reviewed program. A WSE is the means for documenting that weapons-related capability requirement documents provides for safe munition life cycle management, including integration into the JOE, identification of potential operational limits due to potential hazards when the weapon is handled, stored, transported, assembled, disassembled, maintained, tested, destroyed/demilled, or used in the JOE.

3. JWSTAP Review Process

a. The JWSTAP safety review is a "top down" review that is primarily focused on the safety of a weapon used in the JOE. The output of this review is a WSE recommendation memorandum deliverable to the J-8/DDFP.

(1) The JWSTAP will meet at the request of the JWSTAP Chair to conduct technical safety reviews of weapons related JCIDS documents, discuss items of mutual interest, develop WSE recommendations, and recommend policies and priorities to the J-8/DDFP related to the WSE process.

(a) Travel to accomplish routine review actions shall be minimized to the extent feasible. Deliberations of the JWSTAP will be accomplished by electronic means to the maximum extent possible.

(b) Funding to support JWSTAP activities, including travel and per diem costs, will be provided by the participating agencies.

(2) JWSTAP members may also consult with SMEs within their respective Services or organizations to develop safety comments which represent a Service/organization-wide, technically sound, well-reasoned position.

(3) The JWSTAP Chair shall serve as the primary point of contact for coordination with external agencies. The Chair will notify members when formal document reviews are required, and will assign suspense dates to ensure JWSTAP recommendations are provided to the DDFP within established timeframes.

(4) Comments are normally staffed via the KM/DS system and require that JWSTAP members have access to SIPRNET resources and email. JWSTAP members shall establish a SIPRNET account for email and to access the KM/DS system to facilitate reviews and comment submission as part of the JCIDS document review process. See reference h for access to the KM/DS system.

b. In order to review documents from a joint warfighting perspective, reviewers must understand the applicable Service and joint concepts and/or CONOPS. This can be accomplished by reviewing the DODAF architecture views referenced in the capability requirement document. Reviewers can also gain greater understanding of the Service and joint concepts and/or CONOPS by referring to the ISP associated with the program, which defines the system operation, the interfaces, the environment, and the support required.

c. The JWSTAP safety review considers compliance with established standards, or the justification for deviations based upon unique operational context for the weapon:

(1) System Safety. Is the Sponsor proposing compliance with system safety standards identified in Appendix J to Enclosure D of this manual, or are proposed deviations justified in light of the operational context?

(2) IM. Is the Sponsor proposing capability to resist unplanned threats per established standardized IM test protocols identified in Appendix J to Enclosure D of this manual? If munitions are proposed to not meet all IM passing criteria, are proposed deviations justified in light of the operational context? Has the Sponsor provided details of and a proposed path forward for improving IM response, for consideration during review for the WSE? Status and plans for improving IM response are to be submitted for JROC approval using the IM strategic planning process in accordance with references oooooo and pppppp.

(3) Fuze Safety. Is the Sponsor proposing compliance with fuze safety standards identified in Appendix J to Enclosure D of this manual, or are proposed deviations justified in light of the operational context?

(4) EOD. Is the Sponsor proposing compliance with EOD standards identified in Appendix J to Enclosure D of this manual, or are proposed deviations justified in light of the operational context?

(5) Demilitarization and Disposal. If the munitions contain or deliver energetic material, is the Sponsor proposing compliance with treaties, international agreements, Federal and state regulations and laws, and reference bb in a demilitarization and disposal plan, or are proposed deviations justified in light of the operational context?

(6) Laser Safety. Is the Sponsor proposing compliance with laser safety standards identified in Appendix J to Enclosure D of this manual, or are proposed deviations justified in light of the operational context?

(7) E3 Ordnance Safety. Is the Sponsor proposing compliance with E3 ordnance safety standards identified in Appendix J to Enclosure D of this manual, or are proposed deviations justified in light of the operational context?

(8) Weapon Packing, Handling, Storage, and Transportation. Is the Sponsor proposing compliance with packing, handling, storage, and transportation standards identified in Appendix J to Enclosure D of this manual, or are proposed deviations justified in light of the operational context?

(9) Other. Are other criteria specified by the Sponsor, or lacking thereof, appropriate to weapon safety in the operational context?

d. Each JWSTAP member will submit to the JWSTAP Chair, via the SIPRNET and using a standard CRM, the suggested changes to be incorporated in the JCIDS document that will eliminate or mitigate the safety concerns. In accordance with the CRM, the JWSTAP members shall identify the comment type (critical, substantive, or administrative) and rationale for each suggested change to the JCIDS document. Comments will be submitted by the suspense date specified by the JWSTAP Chair.

e. The JWSTAP shall strive for a unanimous position on formal JCIDS document reviews. In the event the JWSTAP cannot achieve agreement, the Chair may request a vote in order to resolve the matter. Each JWSTAP member shall have one vote. In the case of a tie, the JWSTAP Chair shall cast the deciding vote. If a JWSTAP position is established by majority vote, the minority opinion and rationale will be documented in the WSE recommendation memorandum submitted to the J-8/DDFP.

f. To document the results of the JWSTAP safety review, the JWSTAP Chair or Deputy provides a WSE recommendation memorandum to the J-8/DDFP, through the Chief, Joint Staff J-8 Force Protection Division (J-8/FPD). The memorandum will recommend one of the following:

(1) WSE should be granted.

(2) WSE, with limitations, should be granted.

(3) WSE should be withheld.

g. In cases where the recommendation for a WSE is withheld or granted with limitations, the JWSTAP Chair will consolidate the suggested changes and the rationale and provide as two enclosures:

(1) Enclosure (1) to the WSE recommendation memorandum identifies concerns with the JCIDS document under review in narrative format with supporting rationale.

(2) Enclosure (2) to the WSE recommendation memorandum provides, in CRM format, the specific language to be incorporated in the document under review to eliminate the safety concerns. The J-8/DDFP will enter the recommendations and the supporting rationale into the KM/DS system for staffing.

h. WSE related comments will be returned to the Sponsor for adjudication along with other comments from the JCIDS staffing process. During the comment adjudication period, the Sponsor may consult with the JWSTAP to ensure that safety concerns are adequately addressed.

i. Following Sponsor comment adjudication, the J-8/DDFP will review the revised document, generate the WSE, and inform the lead FCB that the WSE has been provided. If comments have not been adequately adjudicated, the J-8/DDFP will identify remaining issues for the Sponsor and notify the lead FCB that the WSE will not be granted on the nominal timeline and recommend that the document not be forwarded for validation until issues have been resolved.

j. Safety Review Guidelines and Timelines. The JWSTAP safe weapons review will be conducted within the 21 day staffing timeline for JCIDS document reviews as outlined in this manual. Following Sponsor comment adjudication, the WSE will be provided within seven days unless there are outstanding issues which the Sponsor did not address during comment adjudication. See Figure F-A-1.

4. Proponent. The WSE proponent is the Protection FCB. For questions, contact the Protection FCB at 703-693-7116.

DRAFT

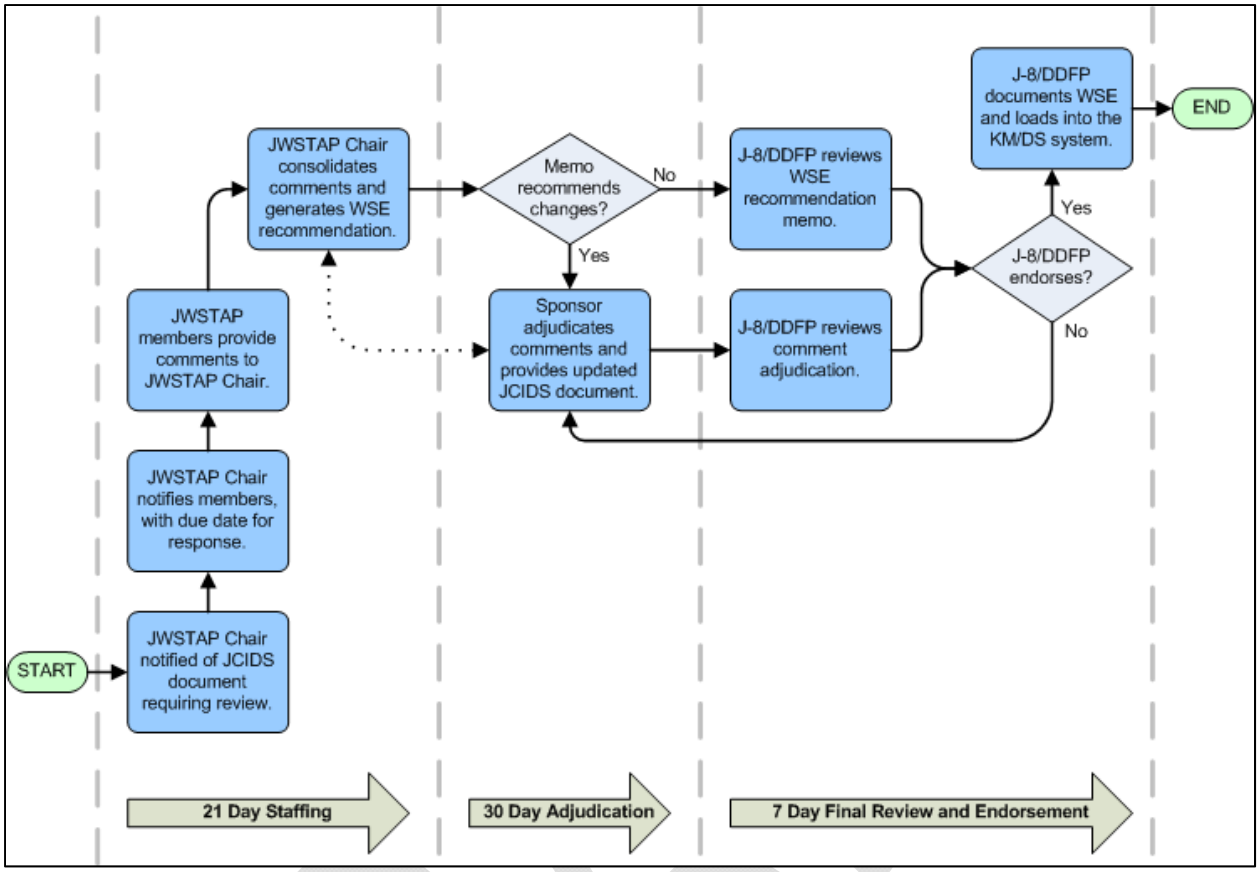

Figure F-A-1. JWSTAP WSE Process and Timeline

ATTACHMENT A TO APPENDIX A TO ENCLOSURE F

EXAMPLE WSE RECOMMENDATION MEMORANDUM

8020
Ser N3/XXX
<Date>

MEMORANDUM FOR RECORD

From: Chair, Joint Weapon Safety Technical Advisory Panel

To: Deputy Director, Force Protection, J-8

Subj: WEAPON SAFETY ENDORSEMENT RECOMMENDATION: JOINT AIR-TO-AIR KINETIC KILL WEAPON (JAAKKW) CPD Review

Ref: (a) JROCM 102-05 of 20 May 05, Safe Weapons in Joint Warfighting Environments
(b) Capability Production Document for the Joint Air-To-Air Kinetic Kill Weapon (JAAKKW) Version 1.0, Dated 4 Aug 08

Encl: (1) Joint Weapon Safety Technical Advisory Panel Concerns with the Capability
Production Document for the Joint Air-To-Air Kinetic Kill Weapon (JAAKKW) Version 1.0, dated 4 Aug 08
(2) JWSTAP Concerns with the Capability Production Document for the Joint Air-To-Air Kinetic Kill Weapon (JAAKKW) Version 1.0, dated 4 Aug 08
(3) Comment Resolution Matrix for the JWSTAP_JAAKKW CPD Version 1.0 Review

1. In accordance with reference (a), the Joint Weapon Safety Technical Advisory Panel (JWSTAP) conducted a safety review of reference (b) which is the Capability Production Document (CPD) for the Joint Air-To-Air Kinetic Kill Weapon (JAAKKW) Version 1.0 dated 4 Aug 08. Based on this review, the JWSTAP recommends that a Weapon Safety Endorsement (WSE) for the JAAKKW be withheld until the JWSTAP concerns discussed in enclosure (1) have been resolved. Enclosure (2) - *not included in this JCIDS Manual example* - is a Comment Resolution Matrix that provides the specific wording to address the enclosure (1) concerns. Enclosure (2) also addresses administrative concerns.

Subj: WEAPON SAFETY ENDORSEMENT: JOINT AIR-TO-AIR KINETIC KILL WEAPON (JAAKKW) CPD Ph1 Review

2. Upon resolution of the JWSTAP concerns, the JWSTAP will provide a recommendation for a WSE. The JWSTAP point of contact is <name> at comm. <(123) 456-7891>; DSN <555-7891>; or email <email address>.

<Signature>
<Name of JWSTAP Chair>

Copy to:
FA FCB (Code/Name)
Sponsor (Code/Name)
Joint Staff (J8/FPD; <name>)
JWSTAP Members

DRAFT

JWSTAP Concerns with the Joint Air-To-Air Kinetic Kill Weapon (JAAKKW) CPD Ph1

1. Confusion in the platforms that will carry the JAAKKW. The Revision History section, page 6, of the CPD states that the XYZ Aircraft is to be an objective platform, but there is no mention of that as an objective in the document. Specifically, paragraph 1.5, titled "Capability Delivered," lists the ABC Aircraft as an objective aircraft but does not list the XYZ Aircraft as a follow-on objective. The ABC aircraft would carry and launch this weapon on an external weapon station, while the XYZ aircraft would carry and launch this weapon from a station that is internal to the aircraft. CPD clarity is required since the System Safety Program (SSP) needs to address the potential safety issues associated with JAAKKW and the launch aircraft as a unified system. The SSP will fail to address the JAAKKW and the XYZ Aircraft as a system if the XYZ Aircraft is not included as an objective. Failure to include the XYZ Aircraft as an objective aircraft may result in safety issues unique to the JAAKKW and XYZ Aircraft going undetected and may require corrective actions at a later time.

2. The failure to address requirements for Organizational-Level (O-Level) maintenance. Although O-Level is addressed there is no mention of the support that is necessary such as inspection lists, safeguards, and training. Support needs to be addressed to ensure that O-Level maintenance can be effectively conducted.

3. Lack of an SSP. Safety is discussed in paragraph 15.1, but system safety is not discussed. There is no evidence that a comprehensive SSP has been conducted and no evidence that one is planned. DOD Directive 5000.1 requires that safety be addressed throughout the acquisition process. USD(AT&L) Memo Subj: Defense Acquisition System Safety – Environment, Safety, and Occupational Health (ESOH) Risk Acceptance of 7 Mar 07 requires programs, developing solutions to this CPD, to establish an SSP in accordance with MIL-STD-882D.

4. Failure to address the need for Explosives Ordnance Disposal (EOD). The CPD does not address the need for EOD. EOD needs to be addressed in accordance with DOD Directive 5160.62 to ensure EOD plans are in place when the need arises to dispose of dudded rounds.

Enclosure (1)

(INTENTIONALLY BLANK)

DRAFT

APPENDIX B TO ENCLOSURE F

ENDORSEMENT GUIDE FOR THE FORCE PROTECTION KPP

1. Purpose

a. This guide provides procedures for the Chair of the Protection FCB to review the FP KPP during the staffing of capability requirement documents.

b. When responsibility to review and endorse the FP KPP is assigned to the Sponsor in accordance with Enclosure E of this manual, the Sponsor may deviate from this endorsement guide.

c. Any substantive changes to this guide will be coordinated with and approved by the DJ-8 or designee.

2. Review Process

a. The Protection FCB receives, via the KM/DS system, all JROC Interest or JCB Interest documents.

b. The Protection FCB reviews and assesses the FP KPP, with advisory support from the Office of the USD(P&R), and determines if requirements for protecting system operator and other personnel under applicable threat environments are adequately described.

c. The Protection FCB reaches out to the Sponsor for further clarification, if needed.

d. The Protection FCB endorses the FP KPP, documents rejection of the FP KPP, or provides waiver thereof.

3. Review Criteria

a. Is there evidence of a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, threat, vulnerability assessment, and solutions leading to the determination of the KPP value? Are the analyses of these assumptions supporting the FP KPP documented?

b. Are the FP KPP attributes and associated values consistent with the intended operational use of the system (i.e., the CONOPs)? Relative to the FP areas identified in Appendix B to Enclosure D of this manual:

DRAFT

(1) Are the occupants adequately protected from kinetic fires, and are the identified attributes and associated values appropriate given the operational context?

(2) Are the occupants adequately protected from non-kinetic fires (other than CBRN), given the operational context? Are the attributes and associated values in compliance with the standards identified in Appendix B to Enclosure D of this manual, or are deviations justified in light of the operational context?

(3) Are the occupants adequately protected from CBRN effects, given the operational context? Are the attributes and associated values in compliance with the standards identified in Appendix B to Enclosure D of this manual, or are deviations justified in light of the operational context?

(4) Are the occupants adequately protected from environmental effects, given the operational context? Are the attributes and associated values in compliance with the standards identified in Appendix B to Enclosure D of this manual, or are deviations justified in light of the operational context?

(5) Are the occupants adequately protected from crash events, given the operational context? Are the attributes and associated values in compliance with the standards identified in Appendix B to Enclosure D of this manual, or are deviations justified in light of the operational context?

4. Proponent. The FP KPP proponent is the Protection FCB, with advisory support from the Office of the USD(P&R). For questions, please contact the Protection FCB at 703-693-7116.

DRAFT

APPENDIX C TO ENCLOSURE F

ENDORSEMENT GUIDE FOR THE SYSTEM SURVIVABILITY KPP

1. Purpose

a. This guide provides procedures for the Joint Staff J-8/DDFP to review the SS KPP during the staffing of JCIDS documents.

b. When responsibility to review and endorse the SS KPP is assigned to the Sponsor in accordance with Enclosure E of this manual, the Sponsor may deviate from this endorsement guide.

c. Any substantive changes to this guide will be coordinated with and approved by the DJ-8 or designee.

2. Review Process

a. The Protection FCB receives, via the KM/DS system, all JROC Interest or JCB Interest documents.

b. The Protection FCB reviews and assesses the SS KPP and determines if requirements for the system to maintain its capabilities under applicable threat environments are adequately described.

c. The Protection FCB reaches out to the Sponsor for further clarification, if needed.

d. The Protection FCB endorses the SS KPP, documents rejection of the SS KPP, or provides waiver thereof.

3. Review Criteria

a. Is there evidence of a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, threat, vulnerability assessment, and solutions leading to the determination of the KPP value? Are the analyses of these assumptions supporting the FP KPP documented?

b. Are the SS KPP values consistent with the intended operational use of the system (i.e., the CONOPs)? Relative to the SS areas identified in Appendix C to Enclosure D of this manual:

(1) Is the system adequately protected from being hit by kinetic or non-kinetic fires, and are the identified attributes and associated values appropriate given the operational context?

(2) Is the system adequately robust to maintain its mission capabilities after being hit by kinetic or non-kinetic fires (other than CBRN), and are the identified attributes and associated values appropriate given the operational context?

(3) Is the system adequately protected from CBRN effects to maintain its mission capabilities, given the operational context? Are the attributes and associated values in compliance with the standards identified in Appendix C to Enclosure D of this manual, or are deviations justified in light of the operational context?

(4) Is the system and its broader architecture adequately resilient to maintain its mission capabilities after losses of individual systems or enabling capabilities, and are the identified attributes and associated values appropriate given the operational context?

4. Proponent. The SS KPP proponent is the Protection FCB. For questions, please contact the Protection FCB at 703-693-7116.

DRAFT

APPENDIX D TO ENCLOSURE F

ENDORSEMENT GUIDE FOR THE SUSTAINMENT KPP

1. Purpose

a. This guide provides procedures for the Joint Staff J-4/MXD to review the Sustainment KPP during the staffing of capability requirement documents.

b. When responsibility to review and endorse the Sustainment KPP is assigned to the Sponsor in accordance with Enclosure E of this manual, the Sponsor may deviate from this endorsement guide.

c. Any substantive changes to this guide will be coordinated with and approved by the Director, Joint Staff J-4 Directorate for Logistics (DJ-4)or designee.

2. Review Process

a. J-4/MXD receives notification of all capability requirement documents via the KM/DS system.

b. J-4/MXD reviews and coordinates with the Office of the DASD(MR) for Sustainment KPP analysis.

c. J-4/MXD consolidates and enters comments into the KM/DS system.

d. Program Sponsors will contact J-4/MXD for comment adjudication.

e. J-4/MXD and the Office of the DASD(MR) will provide representation to JROC and subordinate boards for unresolved critical comments.

3. Review Criteria

a. Sustainment KPP

(1) Materiel Availability metric

(a) Is there evidence of a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, reliability alternatives, maintenance approaches, and supply chain solutions leading to the determination of the materiel availability value? Are the analysis assumptions documented?

(b) Is the total population of systems being acquired for operational use documented, including those in storage or used for training?

DRAFT

(c) Are specific definitions provided for failures, mission-critical systems, and criteria for counting assets as "up" or "down"? Are the failure rate values supported by analysis?

(d) Does the metric clearly define and account for the intended service life of the total inventory, from initial placement into service through the planned removal from service? A graphic representation, such as a timeline or sand chart, of the life cycle profile is an effective way to present the data.

(e) What is the overall sustainment CONOPS? Is it consistent with SSA products, including Service and joint concepts, CONOPS, design reference missions, etc. being supported? Is it traceable to the original capability requirements, or agreement with the warfighting community? What alternatives were considered? Have surge/deployment acceleration requirements been identified and are they factors in development of the Materiel Availability metric?

(f) Is failure/down-time defined? Is planned downtime (all causes) identified and included? Does analysis data support the downtime? Are data sources cited? How does the downtime value compare with downtimes for analogous systems?

(2) Operational Availability metric

(a) Is there evidence of a comprehensive analysis of the system and its planned use, including the planned operating environment, operating tempo, reliability and maintenance concepts, and supply chain solutions leading to the determination of the value? Are the analyses documented?

(b) Are specific definitions provided for failures, mission-critical systems, and criteria for counting assets as "up" or "down"? Are the values for failure rates supported by analysis?

(c) Is scheduled downtime which affects the CONOPS identified and included? Does the analysis package support the downtime? Are data sources cited? How does the downtime value compare with that experienced by analogous systems?

(d) Is downtime caused by failure addressed? Are the values used for failure rates supported by the analysis? Is there a specific definition established for failure?

(e) Is the administrative and logistics downtime associated with failures addressed (e.g. - recovery time, diagnostics time, movement of maintenance teams to the work site, etc.)?

(f) For complex systems and systems of systems, is the operational availability defined at the appropriate system level? Is it consistent with Operational Availability and Reliability requirements?

b. Reliability KSA

(1) Has the reliability metric been established at the system level? Is it traceable to the original capability requirements, or other performance agreement?

(2) Does the analysis clearly provide criteria for defining relevant failure?

(3) Does the analysis clearly define how time intervals will be measured?

(4) Does the analysis identify sources of baseline reliability data and any models being used? Is the proposed value consistent with comparable systems? Are sources of data and processes to track reliability across the life cycle identified?

(5) Is the reliability value consistent with the intended operational use of the system (i.e., the CONOPs)?

(6) Is the reliability value consistent with the sustainment approach as presented in the operational availability metric?

(7) Is the reliability value improved relative to previously fielded or analogous systems? If lower reliability is proposed, what improvements are gained in other areas to make the trade-off valuable to the warfighter?

(8) For single-shot systems and systems for which units of measure other than time are used as the basis for measuring reliability, does the package clearly define the units, method of measuring or counting, and the associated rationale?

c. O&S Cost KSA

(1) Has the O&S cost goal been defined for the system?

(2) Does the analysis utilize the CAPE O&S cost element structure? Are there costs included in the O&S Cost KSA that fall outside of the CAPE O&S cost element structure? If so, have those costs been explained in sufficient detail?

(3) Is the documentation for the O&S cost estimate of the objective value supplied and available in the KM/DS system? If so, is it to an appropriate level of detail to adequately explain the estimate values?

(4) Is the cost model consistent with the assumptions and conditions being used for materiel availability and materiel reliability?

(5) Is the cost metric traceable to the original capability requirements, or agreement with the warfighter?

(6) Are all required costs included, regardless of funding source or management control?

(7) Were applicable environmental issues considered in the development of the O&S cost estimate?

(8) Is the O&S Cost KSA data consistent with the capability solution's life cycle cost estimate (LCCE), Cost Analysis Requirements Data (CARD) and/or the CAPE independent cost estimate (ICE) if available for comparison?

(9) Is the threshold value for the O&S Cost KSA calculated as 10% higher than the objective value?

(10) Has the annual cost of a system (or systems for munitions and networks) been provided as part of the rationale?

d. Are sources of data, information systems, and processes identified to track the Sustainment KPP and its supporting KSAs across the life cycle? What models are used to establish and track the Sustainment KPP and its supporting KSAs?

e. Other logistics attributes

(1) Is there evidence of analysis of the system and its planned use, including the operating environment, operating tempo, reliability, maintenance concepts, and supply chain solutions (logistics and administrative downtime) leading to the determination of each attribute's value? Are the analyses documented?

(2) Are specific definitions for each attribute's value provided? Are they supported by analysis and are they testable?

(3) Are information systems for sources of data and processes to track each attribute's metric or value across the life cycle identified? Are there models or simulations available that establish or track each attribute?

(4) Does the attribute require discrete funding and is that requirement included in the O&S Cost KSA, LCCE, CARD and/or CAPE ICE?

f. Other KPP, KSA, or APAs

(1) Do any of the other KPPs, KSAs, or APAs require specific or discrete logistics support or affect the Sustainment KPP or its supporting KSAs?

(2) Are there logistics information systems for sources of data and processes to track the KPPs, KSAs, or APAs that impact logistics support?

4. Proponent. The Sustainment KPP proponent is the Joint Staff J-4 / Maintenance Division (J-4/MXD), with analytical support from the Office of the DASD(MR). For questions regarding the Sustainment KPP, contact J-4/MXD at 703-614-0161.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX E TO ENCLOSURE F

CERTIFICATION GUIDE FOR THE NR KPP

1. Overview

a. This enclosure provides an NR KPP certification process overview within the DOD IT life cycle. NR KPP assessments are conducted throughout the IT life cycle to identify and resolve potential interoperability and/or emerging net-centricity challenges and mitigate the risk of delivering non-interoperable capabilities to the Warfighter.

b. When responsibility to review and endorse the NR KPP is assigned to the Sponsor in accordance with Enclosure E of this manual, the Sponsor may deviate from this endorsement guide.

c. Any substantive changes to this guide will be coordinated with and approved by the DJ-6 or designee.

2. Types of NR KPP Certifications. NR KPP certification is provided via a Joint Staff J-6 signed memo. The four NR KPP certifications are:

a. Certified. The IT has completed all NR KPP requirements and/or stages and all comments were successfully adjudicated.

b. Not Certified. The IT has completed all NR KPP requirements and/or the stages, but has unresolved critical comments that deny certification.

c. Not Applicable. Consistent with Joint Staff Gatekeeper assigned JSD and guidance in Enclosure E of this manual, the NR KPP does not require joint certification because it lacks joint interface or doesn't exchange joint information. The DOD Component will provide Component NR KPP certification as required.

(1) To facilitate this determination, the sponsor/program will provide Joint Staff J6 with the DODAF OV-2, OV-4, OV-5, and SV-2 views.

(2) The component will then certify that the IT has met all of the NR KPP and integration requirements specified by the component.

d. Not Required. The NR KPP certification is not required for this stage or type of document in accordance with this manual.

3. Process Relationships. Figure F-E-1 depicts the DOD acquisition, JCIDS, NR KPP certification, and spectrum requirement compliance process relationships. The Joint Interoperability Test Command (JITC) provides

interoperability test certification prior to the full rate production decisions in accordance with reference cccc.

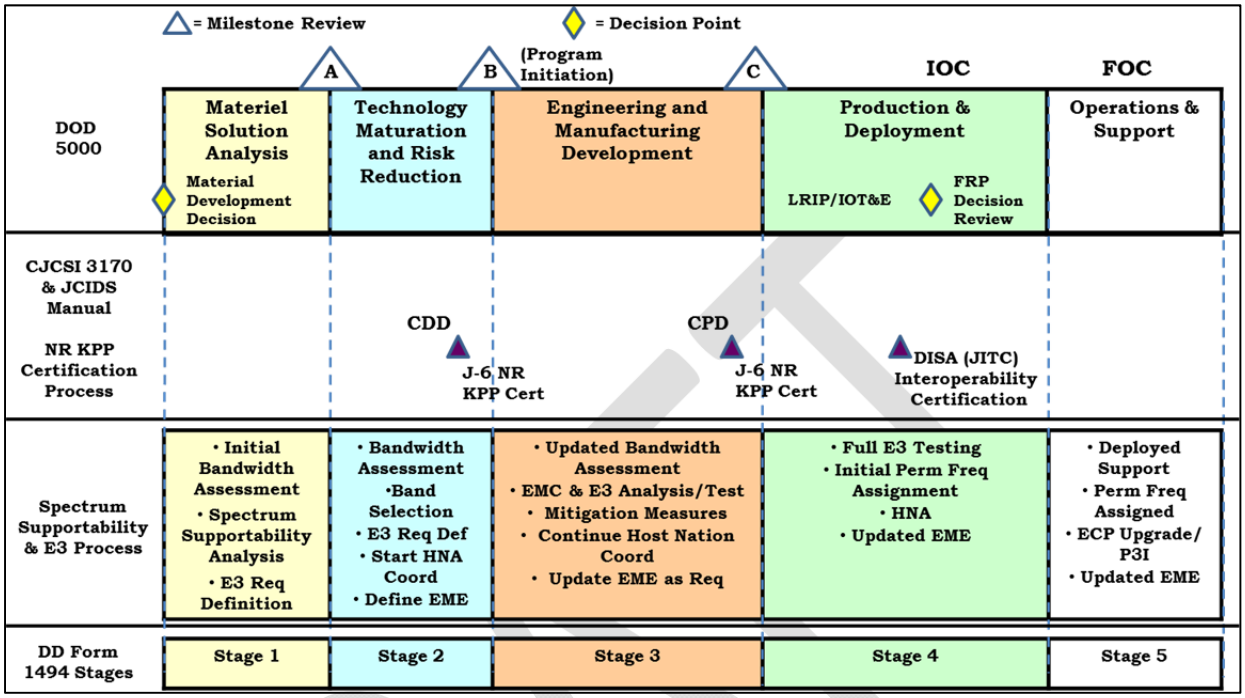

Figure F-E-1. DAS, JCIDS, and NR KPP Certification Relationship Overview

4. NR KPP Certification Process. The Joint Staff certifies the NR KPP and spectrum requirements compliance. The Joint Staff reviews and comments on the ISP, including content of the NR KPP, DODAF architecture data, associated artifacts/views, and spectrum requirements compliance. DBS documents comply with the Business EA.

a. Pre-DOD Acquisition System MS A Documents. Prior to MS A, ICDs, DCRs, and CONOPS are reviewed to determine which JCA, JMT, associated mission areas, and UJTs are identified; to determine if interoperability with other developing capabilities is considered; to determine if DODIN goals and characteristics and NetOps for the DODIN direction in reference eeeee are addressed, and to ensure spectrum requirements are identified in accordance with references bb, kkkkk, and qqqqqq.

b. Post-DOD Acquisition System MS A Documents

(1) CDDs and CPDs are reviewed and the NR KPP certified via KM/DS, using DODAF architecture data, associated artifacts/views, and spectrum requirement compliance. The post MS-A document certification evaluates compliance with NR KPP attributes, DODIN goals and characteristics, capability requirement portfolio management recommendations, and alignment

to the current DODAF. Certification occurs prior to acquisition MS B and MS C and when capability changes result in updates to the NR KPP. Architecture data and associated artifacts/views is provided via a URL where the architecture is registered or repository access versus incorporating the architecture products in the document.

(2) NR KPP certification also applies to IS-ICD and IS-CDD variants outlined in this manual. Initial NR KPP certification will occur during the IS-ICD or IS-CDD review process. Final NR KPP certification must be completed prior to MS C.

(3) The NR KPP contained in the ISP is reviewed for recommendation to DOD CIO, including current DODAF architecture data, associated artifacts/views, and spectrum requirements compliance.

c. DBS Document Reviews and NR KPP Certification. DBS documents are reviewed to determine if JROC interest exists, in accordance with this manual and reference lll, and to provide comments.

5. NR KPP Staffing

a. JCIDS Document Review and Certification. Pre-MS A JCIDS document reviews, CDD and CPD certification of the NR KPP, using the DODAF architecture data, associated artifacts/views, and spectrum compliance is accomplished in concert with JCIDS document staffing. Interoperability issues may be identified by DOD Component via KM/DS.

b. C4/CYBER FCB Adjudication. Unresolved NR KPP, DODAF architecture data, associated artifacts/views, and spectrum compliance issues are forwarded to the C4/CYBER FCB or Military Intelligence Board (MIB) for resolution and their decisions provided to the lead DOD Component to complete the JROC approval process. The C4/CYBER FCB and MIB ensure unresolved issues are presented to the JROC for resolution via the appropriate FCB. Unresolved issues will prevent JCIDS document NR KPP certification.

6. Failure to Meet NR KPP Certification Requirements. Failure to meet or maintain NR KPP certification or joint interoperability certification may result in:

a. No JROC validation of the program CDD, CPD, or DOD CIO approval of the ISP.

b. Recommendation that the IT not proceed to the next acquisition MS.

c. Recommendation that funding be withheld until compliance is achieved and the program and/or system is validated.

d. Withholding of NR KPP certification and recommend revoking any existing Interim Certificate to Operate (ICTO) until the issue is corrected.

7. Recommendations. Failed NR KPP certification recommendations are provided to USD(AT&L); USD(P); USD(C); the Under Secretary of Defense for Intelligence (USD(I)); Director, CAPE; DOD CIO; DOD EA for Space; and the JROC. Recommendations are also posted to the KM/DS system for visibility and access to other stakeholders.

8. Resources. NR KPP internet resources are located at the URL in reference iiii. This page will be kept up-to-date as Web sites change. Contact the Joint Staff lead if unable to access the resource page.

9. Spectrum Requirements Compliance. To obtain an I&S NR KPP certification, all spectrum dependent devices must comply and be developed with the spectrum management and E3 direction in references bb, cccc, and rrrrrr through tttttt. The assessment of equipment or systems needing spectrum is the receipt of equipment spectrum certification, availability of frequencies for operation, and consideration of EMC. The spectrum process includes joint, DOD, national, and international policies and procedures for the management and use of the EM spectrum. The spectrum process is detailed in Appendix E to Enclosure D of this manual and at the URL in reference iiii.

DRAFT

APPENDIX F TO ENCLOSURE F

ENDORSEMENT GUIDE FOR THE ENERGY KPP

1. Purpose

a. This guide provides procedures for the Logistics FCB Chair to review the Energy KPP during the staffing of JCIDS documents. On behalf of the Logistics FCB Chair, the Joint Staff J-4/ED evaluates and endorses the Energy KPP in capability requirement documents, with analytical support from the office of the ASD(OEPP).

b. When responsibility to review and endorse the Energy KPP is assigned to the Sponsor in accordance with Enclosure E of this manual, the Sponsor may deviate from this endorsement guide.

c. Any substantive changes to this guide will be coordinated with and approved by the DJ-4 or designee.

2. Review Process. The J-4/ED, with support from the office of the ASD(OEPP) , will review energy performance metrics for alignment with Energy KPP guidance provided in Appendix F to Enclosure D of this manual.

a. J-4/ED receives notification of new capability requirement documents in the KM/DS system.

b. J-4/ED reviews and coordinates with the office of the ASD(OEPP) for Energy KPP analysis.

c. J-4/ED consolidates and enters comments into the KM/DS system.

d. Document Sponsors will adjudicate comments as part of document staffing outlined in Enclosure F of this manual, including coordination with J-4/ED and the office of the ASD(OEPP).

e. J-4/ED and the office of the ASD(OEPP) will provide representation to the JROC and subordinate boards for unresolved critical comments.

3. Review Criteria

a. Energy Supportability Analysis

(1) Is there evidence of a comprehensive analysis of the system and its planned use, including the intended operating environment, operating tempo, and supply chain solutions/constraints leading to the determination of the Energy KPP attribute values?

(2) Does the analysis present energy performance and mission effectiveness relationships?

(3) Does the analysis identify the most critical attributes associated with the use, delivery, storage or protection of energy that impact mission success?

(4) Did the Sponsor provide the assumptions on which the analysis is based?

(5) Does the analysis present energy supply/demand relationships?

b. Scope

(1) Are the CONOPS and/or OMS/MPs based on relevant situations derived from the approved scenario?

(2) Do the energy performance attributes encompass critical energy-demanding activities the system must perform within the mission profile?

(3) Do the threshold and objective values of the energy performance attributes enable operations at the required tempo and CONOPS given constraints on the energy supply in the operational area?

c. Relevance

(1) Do the energy performance attributes relate energy demand directly to a relevant combat performance issue?

(2) Is there evidence of due diligence to determine threshold and objective values for energy performance attributes relevant to the state of technology?

d. Clarity

(1) Do the energy performance attributes directly relate to mission effectiveness by improving the system's energy performance?

(2) Are the energy performance attributes expressed in commonly used terms and/or metrics?

e. Measurability

(1) Are the energy performance attributes quantified in metrics commonly tested in similar systems?

(2) Can compliance with the energy performance attribute be demonstrated by a combination of test results and modeling acceptable to the DOT&E community?

4. Waiver Process

a. Sponsors requesting relief from the Energy KPP must seek approval for a waiver through the J-4/ED. Together with the waiver request, the Sponsor will provide the analysis supporting the assessment that the Energy KPP is not applicable.

b. J-4/ED, with assistance from the office of the ASD(OEPP), will review the request and the supporting documentation. J-4/ED will either approve the waiver or inform the Sponsor why the waiver was not approved.

c. Because the acquisition process deals with trade space and balancing cost, schedule, and performance, waivers must be carefully weighed. "The new platform doesn't use more energy than the old platform" is not a sufficient justification for a waiver. Without an Energy KPP, that energy limit could be "traded" for some other attribute. In this example, the threshold value of an Energy KPP attribute could be the same as the previous platform; the Sponsor is not spending money to be more energy efficient but the current energy efficiency cannot be traded away to improve some other performance attribute.

5. Proponent. The Energy KPP proponent is the J-4/ED, with analytical support from the office of the ASD(OEPP). For questions regarding the Energy KPP, contact J-4/ED at 703-697-4445.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX G TO ENCLOSURE F

ENDORSEMENT GUIDE FOR THE TRAINING KPP

1. The content of the Training KPP, if applicable, and the training content within the DOTmLPF-P section are reviewed together as part of the DOTmLPF-P endorsement to ensure that the Sponsor has a robust approach to ensuring training equities are addressed. A separate endorsement of the training KPP is not required. See Appendix H to Enclosure F of this manual for detail of the DOTmLPF-P endorsement which incorporates Training KPP equities.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX H TO ENCLOSURE F

ENDORSEMENT GUIDE FOR DOTmLPF-P

1. Purpose

a. This guide provides procedures for the Joint Staff J-7 and DOTmLPF-P stakeholder organizations to review issues, ensure all appropriate DOTmLPF-P considerations are addressed in capability requirement documents, and develop the DOTmLPF-P endorsement as part of document staffing.

(1) The DOTmLPF-P endorsement ensures that Sponsors adequately consider potential non-materiel capability solutions to identified capability requirements, and adequately address DOTmLPF-P issues associated with materiel capability solutions.

(2) Inadequate DOTmLPF-P content in capability requirement documents must be addressed to the satisfaction of the appropriate stakeholder organization prior to granting the DOTmLPF-P endorsement.

b. When responsibility to review and endorse DOTmLPF-P is assigned to the Sponsor in accordance with Enclosure E of this manual, the Sponsor may deviate from this endorsement guide.

c. Any substantive changes to this guide will be coordinated with and approved by the DJ-7 or designee.

2. Review Process

a. J-7/JIB reviews JCIDS documents for DOTmLPF-P issues with JSDs of JROC Interest, JCB Interest, and Joint Integration. J-7/JIB may also review other JCIDS documents when requested by J-8/DDR or the Sponsor. As DOTmLPF-P covers a broad range of topics, J-7/JIB coordinates with the following DOTmLPF-P stakeholder organizations:

(1) J-7, and the processes established in reference ww, for doctrine issues.

(2) J-8 (with support from J-1 and J-5), and the processes established in reference xx, for organization issues.

(3) The Office of the USD(P&R), and the processes established in reference yy, for training issues. Note that the content of the Training KPP, if applicable, and the training content within the DOTmLPF-P section are reviewed together as part of the DOTmLPF-P endorsement to ensure that the

Sponsor has a robust approach to ensuring training equities are addressed. A separate endorsement of the training KPP is not required.

(4) J-8 and affected Sponsors of existing materiel for materiel issues.

(5) J-1 and the Office of the USD(P&R), and the processes established in references zz through bbb, for leadership and education, and personnel issues.

(6) J-4, and the processes established in references ccc and ddd, for facilities issues.

(7) J-5 and the Office of the USD(P), and the process established in reference eee, for policy issues.

b. Organizations coordinating with J-7/JIB for the DOTmLPF-P endorsement will ensure up-to-date POC information is provided to J-7/JIB.

c. These reviews focus on:

(1) Non-materiel approaches that address capability requirements identified in ICDs or DCRs, and partially or wholly mitigate associated capability gaps.

(2) Non-materiel enablers identified in CDDs and CPDs that are associated with materiel capability solutions, without which the materiel capability solution cannot be successfully fielded.

d. The DOTmLPF-P endorsement is based on review of the information provided in the JCIDS document and accomplishes the following:

(1) Ensures non-materiel solutions are fully considered and documented or that justification regarding recommendation for their exclusion is provided.

(2) Develops recommended revisions to the document language to reduce or eliminate identified concerns.

(3) Informs the lead FCB that the required DOTmLPF-P review has been completed.

e. An endorsement memorandum will be signed by the DJ-7 or designee and provided to the lead FCB.

3. <u>Review Criteria and Endorsement Memorandum</u>

a. J-7/JIB will use Appendix H to Enclosure D of this manual as the basis for the DOTmLPF-P review. DOTmLPF-P content not in compliance with this guidance shall be updated to the satisfaction of the stakeholder organizations identified above before the DOTmLPF-P Endorsement will be issued.

b. J-7/DDI will submit to the DJ-7 or designee a recommendation to grant or withhold the endorsement. Once determination is made, a signed endorsement letter will be uploaded to the KM/DS system.

c. If the DOTmLPF-P endorsement is withheld, suggested changes and/or rationale will be included with the memorandum.

4. Proponent. The DOTmLPF-P proponent is the Joint Staff J-7, Joint Integration Branch (J-7/JIB), on behalf of the Joint Staff J-7 Deputy Director for Integration (J-7/DDI). For questions, please contact the J-7/JIB at 703-692-0785.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

APPENDIX I TO ENCLOSURE F

CERTIFICATION GUIDE FOR INTELLIGENCE SUPPORTABILITY

1. Overview. The objective of intelligence certification is to ensure intelligence requirements have been identified at the earliest possible point, and that all likely intelligence support requirements and shortfalls (if applicable) have been documented. Threat assessment accomplished as part of intelligence certification further ensures that continuous system and protection threat analysis of applicable adversary threat capabilities is complete and incorporated into capability requirement documents.

a. The scope of intelligence certification shall include the entire program or capability solution's life cycle. Intelligence certification shall seek to:

(1) Preclude fielding capabilities, systems, or programs that are unsupportable by the national and defense intelligence communities.

(2) Prevent scientific and technological surprise by ensuring Sponsors consider and incorporate the most current, applicable intelligence information, analysis, and findings into their capability development efforts.

(3) Ensure that national and defense intelligence architectures remain capable of, and agile enough, to support future warfighting by identifying and assessing possible intelligence support requirement shortfalls created by, or existing shortfalls aggravated by, programs and capabilities being reviewed.

b. When responsibility to review and certify intelligence supportability is assigned to the Sponsor in accordance with Enclosure E of this manual, the Sponsor may deviate from this endorsement guide to the extent that the Sponsor remains consistent with IC policies and procedures.

c. Collaboration. The intelligence review process is based on a collaborative, analytical process that evaluates what is required from, or contributes to, the IC throughout the capability solution's life cycle. Extensive cooperation, coordination, collaboration and analysis are critical to ensure the full range of potential intelligence supportability issues is addressed.

(1) Intelligence certification is the result of collaboration and analysis that leverages the expertise and unique perspectives of all applicable offices within DIA, NGA, NRO, NSA, CCMDs, Service Intelligence, and the Joint Staff Directorate for Intelligence (J-2).

(2) J283/IRCO shall lead this collaborative intelligence certification process for the Joint Staff on behalf of the J-2 directorate.

d. Intelligence Certification

(1) The intelligence certification is a statement of adequacy based on previously completed reviews and IMD derived requirements. It assesses whether the projected intelligence architecture, infrastructure, collection, production and exploitation data, and priorities will provide necessary and expected support to the acquisition and operational communities.

(2) J283/IRCO review and intelligence certification will be conducted as part of validation of each capability requirement document, in support of each acquisition decision point – i.e. the ICD for MS A, the CDD for the developmental RFP release decision point before MS B, and the CPD for MS C. As programs proceed through acquisition milestones, information regarding intelligence supportability within capability requirement documents is expected to increase in refinement and specificity. In addition, J283/IRCO review and intelligence certification will be conducted as part of validation of Joint DCRs which have intelligence supportability impacts or affect capability solutions which previously received threat assessment and intelligence certification.

(3) The intelligence certification process evaluates and analyzes a program's intelligence support requirements for completeness, supportability, and impact on joint intelligence strategy, policy, and architectural planning. Sponsors shall be responsible for identifying and explaining each proposed or affected capability, and any and all associated intelligence support requirements and shortfalls related to such capabilities, to enable a complete analysis of the program in anticipation of intelligence certification. The intelligence certification will analyze programs for applicable system and protection threats, and assess a program document's threat information. Descriptions of completeness, supportability, and impact on intelligence architecture, strategy, and policy are explained below.

(a) Completeness. Completeness refers to whether a Sponsor's document adequately addresses the applicable intelligence requirements and the associated intelligence supportability requirements related to the proposed capability requirements. Additionally, completeness requires the capability to comply with requirements by intelligence.

1. Requirements by Intelligence. Sponsors must address how their capabilities comply with requirements imposed by intelligence, such as security considerations, classification levels of information and systems, procedures or authority to release or handle classified or sensitive information, and interoperability with operations, C2, and supporting intelligence systems; as well as their responsibilities as they relate to the handling, processing, dissemination, consumption and production of intelligence data or information.

2. Requirements for Intelligence Support. Sponsors must, as specifically as possible and at the earliest possible stage of review, identify and explain known or anticipated intelligence support requirements and shortfalls that are expected to be necessary or result from the program -- the scope of this analysis includes the capability solution's entire projected life cycle. This includes projected requirements for all intelligence data or information (collection requirements/ parameters, analytical products, etc.), infrastructure (intelligence systems, processes, etc.), and/or resources (intelligence funding, personnel, etc.). Sponsors must include qualitative and quantitative attributes for each intelligence support requirement.

(b) Supportability. Supportability refers to the availability, suitability, and sufficiency of intelligence support required by a capability. Assessing supportability requires a comparison of the Sponsor's stated operational/capability requirements with the expected intelligence support capabilities, throughout a capability solution's projected life cycle. The ability to adequately assess supportability depends upon the completeness of the sponsor's declaration of the intelligence requirements and resulting intelligence support required by the capability, and must also be evaluated within the context of any shortfall mitigation strategies identified. Although availability, suitability, and sufficiency are discussed separately below, these criteria often overlap and do not necessarily represent discrete assessments.

1. Availability: whether the intelligence data, information, infrastructure, or resources are, or are expected to be, available throughout the capability solution's projected life cycle.

2. Suitability: whether the required intelligence data, information, infrastructure, or resources are, or are expected to be, appropriate to support the capability.

3. Sufficiency: whether the intelligence data, information, infrastructure, or resources are, or are expected to be, adequate to support Sponsor's capability. Sufficiency may apply to quantitative as well as qualitative (i.e., specificity of information, types or forms of information, amount of analytical refinement, etc.) aspects of intelligence support.

(c) Impact on intelligence strategy, policy, and architecture planning. Impact refers to the identification and analysis of additional inputs to, or outputs from, the IC/infrastructure as a result of the Sponsor's capability.

1. Requirements for intelligence support may not be a concern with regard to the intelligence support infrastructure if planned products, data,

information, or services are, or are projected to be, available, suitable, and sufficient throughout a capability solution's life cycle.

2. In other cases, capabilities may require new types of support or a more demanding standard of support that differs from current intelligence support. These additional inputs or outputs may also require changes across the DOTmLPF-P spectrum. These potential changes may have an impact on intelligence strategy, policy, and architecture that may require planning to support.

3. This impact assessment provides a mechanism to provide critical feedback to the defense and national intelligence communities to identify actual or potential shortfalls in current and/or planned intelligence support, and provides a means to address these shortfalls at the earliest possible point in the development of a capability solution.

e. Threat Assessment. All acquisition programs or capabilities that are expected to operate in a threat environment (lethal or non-lethal) must be developed in accordance with the most current DIA- or Service-approved threat products. The applicable system and protection threat information must be continually updated to account for threats throughout the capability solution's projected life cycle, in accordance with DIA- and Service-approved threat products. Sponsors shall also account for protection threats to research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts.

(1) Threat assessment shall begin with identifying all anticipated capabilities that adversaries might employ against the capability being reviewed, and including these threats as inputs to the Sponsor's CBA or other studies and analyses. Operational tasks, conditions, and standards identified should then be submitted to DIA to enable production of an ITEA. The ITEA will identify projected adversary threat capabilities which are a factor in setting the capability requirements and initial objective values, to include scientific and technological developments as well as reverse-engineering capabilities, which may affect a program or capability's design or implementation. DIA/TLA will assist Sponsors with incorporating adversary capabilities in the development of initial and successor capability requirement documents.

(2) DIA will assess Sponsor's threat information and threat analysis by evaluating Sponsor's capability requirement documents for appropriateness of judgments concerning the extent and scope of threats, ensuring consistency with DIA- or Service-approved threat products, and by ensuring that the sponsor has included current threat references, information, and findings.

f. Intelligence Certification of capability requirement documents protected by ACCM or SAP/SAR designation. Documents protected by ACCM or SAP/SAR designation must also be reviewed and certified for intelligence supportability. Once notified by the Joint Staff Gatekeeper or J-8/SAPCOORD that a capability requirement document requires review, J283/IRCO will coordinate with Sponsor or J-8/SAPCOORD for appropriate access to conduct the review. While ACCM and SAP/SAR security restrictions preclude normal collaboration and coordination, J283/IRCO will endeavor to represent IC supportability capabilities and concerns to the greatest extent possible. When intelligence support requirements and issues exceed the expertise of J283/IRCO personnel, a recommendation will be made to grant access to applicable SME(s) for a more comprehensive document review, as program security regulations allow. Document review coordination and discussions, and transmittal of intelligence certification letters will be conducted via appropriate communications means.

2. Intelligence Certification Procedures

a. Intelligence certification, including DIA/TLA threat assessment and, when applicable, DIA Office of Counterintelligence (D/OCI) protection threat review, is required for all capability requirement documents assigned a JSD of JROC Interest, JCB Interest, or Joint Integration.

b. Intelligence supportability reviews and certifications are performed during the normal staffing of capability requirement documents as described in Enclosure F.

(1) Document Review and Commenting Stage. During this 21 day stage, threat assessment and intelligence supportability content of the capability requirement document will be reviewed, including development and/or updating of appropriate CIPs associated with KPPs. Any issues which impact the ability to issue the intelligence certification will be documented and submitted for Sponsor adjudication.

(2) Comment Adjudication Stage. During this 30 day stage, Sponsors adjudicate each comment submitted to the satisfaction of the reviewer. Active coordination between the Sponsor and J283/IRCO personnel is expected to facilitate comment adjudication.

(3) FCB and FCB WG Review Stage. During this 14 day stage, J283/IRCO shall review the final CRM and draft capability requirement document to ensure that all intelligence-related comments, with particular focus on critical comments, have been appropriately adjudicated and incorporated.

(a) J283/IRCO will coordinate with the assigned FCB when intelligence-related comments arise during the review and adjudication process, or when a program or capability is facing a recommendation of non-certification, to ensure the FCB is made aware of potential intelligence-related issues that must be addressed and resolved prior to intelligence certification approval.

(b) If comments have been adequately addressed, an intelligence certification memorandum will be generated prior to the end of this stage.

(c) If comments have not been adequately addressed, a memorandum stating that the intelligence certification is being withheld will be generated. The memorandum will state specifically which issues remain unresolved for review by the validation authority.

(4) Validation Stage. During this 14 or 28 day stage, any issues which remain unresolved and contribute to the withholding of the intelligence certification can be reviewed by the validation authority. The validation authority will determine how the issue(s) will be resolved, and whether or not validation of the capability requirement document should be withheld pending resolution of the issues.

c. Intelligence Certification

(1) Intelligence certification is effective for only a specific capability requirement document and its associated acquisition milestone (e.g., an intelligence certification letter issued for a CDD will be effective only for MS B). Intelligence Certification letters will be provided to the Joint Staff Gatekeeper for distribution to DJ-8, the Sponsor, and Lead and Supporting FCBs.

(a) For intelligence certifications that identify CIPs associated with applicable KPPs, the certification is valid until the next acquisition milestone, with a new intelligence certification to be generated during the validation of the successor capability requirement document.

(b) For previous intelligence certifications that do not identify CIPs associated with applicable KPPs, an end-to-end review by J283/IRCO is required every two years to ensure the system and protection threats remain valid and changes within the IC will still support program development. A new intelligence certification will be issued for the next two-year period. Once CIPs are identified for applicable KPPs, the intelligence certification will remain valid until the next acquisition milestone.

(b) In the event that the Sponsor initiates a change to the subject document, and the periodicity for the most recent threat assessment falls

beyond the year of the last threat assessment period, the Sponsor is required to request an updated threat assessment be conducted by DIA or the Service in accordance with reference zzzzz.

(c) Upon first notification of either a threat change which impacts one or more of the program's CIPs or a change to an intelligence program supporting or enabling the capability solution, via J283/IRCO or other source, the Joint Staff Gatekeeper may recommend to the validation authority that a program's intelligence certification be reevaluated.

1. In cases of CIP changes or changes to intelligence supporting or enabling capabilities, staffing procedures similar to JCB/JROC Tripwire reviews will be used.

2. As multiple capability requirements and their associated capability solutions could be affected by the same CIP changes or changes to intelligence supporting or enabling capabilities, the FCBs and other stakeholders in the review process will consider impacts within and across the capability requirement portfolios.

3. Not every CIP change will necessarily drive a change to capability requirements, but the validation authority and other stakeholders must balance the potential increase to operational risk from not making a change to the capability requirements with the potential impacts to cost and schedule from making changes to capability requirements being addressed by an ongoing acquisition program.

(2) Intelligence certification shall affirm that:

(a) The program or capability meets minimal requirements for intelligence support needs related to completeness and supportability, and that an assessment concerning the program's impact on intelligence strategy, policy, and architecture has identified no significant shortfalls in current or planned intelligence support.

(b) Any critical intelligence-related comments or critical threat-related comments relating to the program or capability have been appropriately adjudicated to the satisfaction of the entity submitting the comment, or otherwise resolved by the appropriate FCB WG, FCB, JCB, or JROC.

(c) DIA/TLA has reviewed threat information, including DIA- or Service-approved threat products used in the capability requirement document, and concurs with the threat section content pursuant to references yyyyy and zzzzz.

(d) DIA D/OCI, when applicable, has validated the currency and relevancy of intelligence and CI analytical products used to assess the foreign collection threat and referenced in a PPP prior to major milestone decisions; conducted threat analysis of supply chain risk focusing on identifying foreign-affiliated capabilities that would enable an adversary to exploit vulnerabilities, maliciously modify a provided product or service, sabotage system function, or clandestinely extract data or information; and verifies that applicable DIA- or Service-approved threat products are current.

(e) Any projected shortcomings in joint intelligence support will be included in BA FCB analysis efforts as part of the CGA, to identify and prioritize capability gaps within the BA functional area.

(3) Intelligence certification memoranda will document specific areas of risk, as opposed to failure, in relation to the intelligence supportability categories. Areas cited for potential or actual risk must be addressed by the Sponsor.

(4) Certification letters issued following review of an ICD, or following the initial Intelligence Sensitivity Systems Assessment (ISSA) for subsequent capability requirement documents, will document the results of an ISSA and serve to inform the Sponsor and MDA that an Intelligence Supportability Analysis (ISA) should be conducted for solutions identified during the AoA.

d. Conditional Intelligence Certification

(1) When capability documentation does not adequately identify support requirements in one or more categories, but otherwise meets minimum standards, J238/IRCO may issue a Conditional Intelligence Certification, allowing the capability to continue development while shortfalls are addressed. These shortfalls can normally be resolved through review of other capability documentation, such as a PPP, evidence of vulnerability assessments, or documentation of intelligence supportability assessments.

(2) J238/IRCO will coordinate with Joint Staff Gatekeeper and the Sponsor to determine if the capability can meet minimum standards in a reasonable period of time. Conditional Certification will be valid for a specified period of time, not to exceed 180 days, and may include periodic reviews with the Sponsor.

(3) Conditional Intelligence Certification letters will be provided to the Joint Staff Gatekeeper for distribution to DJ-8, the Sponsor, and Lead and Supporting FCBs, and will specify shortfalls and conditions required to be met for final certification. Once conditions have been satisfied, J238/IRCO will issue a final Intelligence Certification; otherwise, J238/IRCO will revoke the

Conditional Certification in a memoranda provided to the Joint Staff Gatekeeper for distribution to DJ-8, the Sponsor, and Lead and Supporting FCBs.

e. Certification Failure

(1) If J283/IRCO determines that there are critical intelligence-related comments that remain unsatisfactorily adjudicated upon its review, then J283/IRCO will recommend withholding intelligence certification for the capability requirement document, or granting intelligence certification with documented risk.

(2) If there is concurrence in J283/IRCO's assessment by the certifying authority, then an intelligence certification failure will result and Sponsor's intelligence certification letter shall be withheld. Intelligence certification shall be withheld until all critical intelligence-related comments have been adjudicated to the satisfaction of the commenter.

f. Revocation of Certification. In instances when an organization or agency submits critical comments after the review period, or other circumstance arises that necessitate further review, J283/IRCO will issue a letter revoking the current certification and provide to the Joint Staff Gatekeeper for distribution to DJ-8, the Sponsor, and Lead and Supporting FCBs. Once the review of comments or circumstance is complete, J283/IRCO will reissue the intelligence certification.

g. Intelligence Supportability Shortfalls. It is possible that the IC cannot support a capability solution's intelligence support requirements (i.e., a shortfall may result from developing a capability). The likelihood that a capability solution may create an intelligence shortfall equates to a risk; it is this risk of an intelligence shortfall that is of central concern in the intelligence certification process. It is acknowledged that each capability has unique attributes that require differing levels and forms of intelligence support. Assessing a capability's risk of creating an intelligence shortfall is, therefore, many times imprecise due to the wide range of variables that affect a capability solution's intelligence support determination (e.g., types of collection assets required, allocation and prioritization of funds or collection time to fulfill intelligence support requirements, complexity of the support necessary, quantity of support necessary, etc.). As a result, a capability's likely effect on the IC and its risk of creating an intelligence shortfall will need to be determined on a case-by-case basis using available information related to intelligence support. Sponsors are required to provide sufficient information, and to perform adequate analysis, to enable reviewers to assess and identify intelligence support requirements and shortfalls, if any.

3. ISSA

a. Regardless of the type of capability requirement document used to initially propose new capability requirements, an ISSA will be conducted to determine whether the program contains potential intelligence support requirements.

(1) The ISSA is a critical element of J283/IRCO's evaluation of a program and was developed to assist in reaching an initial determination whether a program is Intelligence-sensitive. Intelligence sensitivity is determined through the application of the assessment questions shown below, which are administered by J283/IRCO in consultation with the capability Sponsor/PM. A "Yes" answer to any of the ISSA questions indicates the capability has intelligence support requirements and will be designated Intelligence-sensitive.

(2) ISSA Questions:

(a) Does this capability initiative require access to data and/or information produced by the IC to support the research, design, development, manufacturing, testing and evaluation and operations effort?

(b) Will this capability initiative require data and/or information to flow from the IC to support full scale development, operations, or sustainment?

(c) Will this capability produce data and/or information that will flow to the IC for processing, exploitation and dissemination (PED) during full scale development, operations, or sustainment?

(3) If the ISSA indicates the capability is intelligence-sensitive, it should then undergo a more thorough ISA. Certification letters for intelligence-sensitive programs will include appropriate statements informing the Sponsor and MDA that an ISA should be conducted for solutions identified during the AoA.

(4) If the ISSA indicates the capability has no intelligence support requirements, and is not intelligence-sensitive as a result, the requirement for intelligence certification cannot be waived, as capability documents must still receive a DIA threat assessment.

b. The goal of the ISA is to effectively identify and document intelligence support requirements, primarily those requirements associated with the intelligence supportability categories described in Appendix I to Enclosure D of this manual. The results of the ISA should be included in the AoA Report to inform the JCIDS post-AoA review and the MS A acquisition decision, and

provided prior to MS B and MS C decision for capability solutions further along in development.

(1) The ISA results in the identification of derived intelligence support requirements and deficiencies, along with associated impacts to both acquisition and operational capability if the required intelligence support is not provided. Sponsors/PMs and the IC can then develop plans and strategies to support these derived intelligence requirements, and ensure the requisite supporting intelligence infrastructure needed to successfully acquire and employ future joint capabilities is available. The ISA should begin as early as possible and continue throughout the life cycle for capability solutions deemed intelligence-sensitive.

(2) At a minimum, the ISA assists the evaluation and analysis of a capability's intelligence certification by identifying projected requirements for intelligence products, information, or services to include required performance, descriptive, or qualitative and quantitative attributes, as well as any resulting intelligence support requirements for completeness, supportability and impact on joint intelligence strategy, policy, and architectural planning.

(3) From the initial derived intelligence support requirements, more detailed requirements in terms of timeliness, accuracy, volume, etc., can be defined. Sponsors should then determine if the requirements can be satisfied by existing IC capabilities and architectures; requirements that can be supported by the IC should be documented and traced for continuity or changes as they occur.

(4) Any shortfalls identified in IC support should be considered intelligence deficiencies and documented as well, along with proposed solutions and/or risk mitigation plans.

(5) J283/IRCO personnel will support Sponsors in ISA execution, to include intelligence support requirements identification and analysis, IC supportability evaluation, process and documentation support, and developing potential shortfall resolution and risk mitigation strategies. J283/IRCO can also convene an intelligence certification working group for program support and deficiency resolution coordination, as needed or desired.

DRAFT

(INTENTIONALLY BLANK)

DRAFT

ATTACHMENT A TO APPENDIX I TO ENCLOSURE F

INTELLIGENCE CERTIFICATION SUMMARY AND LETTER

THE JOINTSTAFF
WASHINGTON,DC

Reply ZIP Code: U-12345/J28
20318-2000 (DATE)

MEMORANDUM FOR DJ-8, BATTLESPACE AWARENESS FCB, AND U.S. ARMY

Subject: Intelligence Certification of the [Name of program and type of document]
(KM/DS Control Number: XX-XXXXXXXX-XX)

1. Intelligence certification is granted for [Name of program and type of document with acronym] and is written in preparation for a Milestone [__] decision, as required by CJCSI 3170.01J, *Joint Capabilities Integration and Development System (JCIDS)*, and the JCIDS Manual.

2. This certification states that, as of the date of this letter, [program acronym] meets minimal requirements for intelligence completeness and supportability, and that an assessment concerning [program acronym]'s impact on intelligence strategy, policy, and architecture has identified no significant shortfalls in current or planned intelligence support. It is affirmed that all critical intelligence-related comments submitted during the intelligence certification process have been satisfactorily adjudicated.

3. DIA/TLA has reviewed this document and concurs with the threat section and Intelligence Mission Data (IMD) requirements for [program acronym] pursuant to DODD 5000.01 and DODI 5000.02, Operation of the Defense Acquisition System, and DODD 5250.01, Management of Intelligence Mission Data (IMD) in DOD Acquisition. Programs should refer to the latest applicable DIA- or Service-approved threat products, including but not limited to the System Threat Assessment Report (STAR), if available, for threat information specific to [program acronym]. Programs should endeavor to ensure the most current and relevant threat information and IMD requirements are considered prior to and during production.

4. The Joint Staff J-2 point of contact is [J283/IRCO POC Info].

F. M. LASTNAME
Deputy Director for Battlespace
Awareness (J28)

(INTENTIONALLY BLANK)

DRAFT

ENCLOSURE G

URGENT/EMERGENT STAFFING PROCESSES

1. Overview

a. Purpose. The urgent/emergent staffing process allows for timely review and validation of proposed capability requirements related to ongoing or anticipated contingency operations, which if not satisfied in an expedited manner, would result in unacceptable loss of life or critical mission failure.

(1) This enclosure provides the overview of the urgent/emergent staffing processes for JUONs and JEONs in support of rapid acquisition of capability solutions, including those potentially addressed by non-materiel solutions and service contracting efforts.

(2) DOD Component UONs are reviewed and validated by a DOD Component validation authority, in accordance with references hh through oo. After DOD Component validation, copies of the Sponsor validated DOD Component UONs are submitted to the Joint Staff Gatekeeper for information and visibility into capability requirement portfolios managed in accordance with Enclosure B of this manual.

(3) Warfighter issues, including the acquisition of materiel capability solutions in response to validated capability requirements, are addressed in accordance with reference gg.

b. Compromises to facilitate timeliness. By design, the review and validation of JUONs, JEONs, and DOD Component UONs emphasizes speed in both the review and validation process as well as the adjustment of capability requirements to enable approaches which rapidly deliver capability solutions to the warfighter for an ongoing or anticipated contingency operation. As such two areas of compromises are made:

(1) The review of the capability requirements prior to validation may not be as robust as that performed during deliberate staffing, and adjustments to requirements made to enable rapid delivery of capability solutions may result in validation of a sub-optimal set of requirements. In cases where urgent/emergent capability requirements are proposed for extension or validation as enduring capability requirements, the capability requirements will be reassessed to ensure the enduring capability requirements, and associated capability solutions, best meet the needs of the joint force.

(2) A capability solution fielded in response to a JUON, JEON, or DOD Component UON, may not fully satisfy the validated requirements, and may make compromises in areas such as, but not limited to: price, interoperability,

sustainability, training, etc. In cases where urgent/emergent requirements are proposed for extension or validation as enduring capability requirements, the enduring capability solution will not necessarily be the same as the rapidly fielded capability solution. If a rapidly fielded capability solution does become the enduring capability solution, changes or updates may be required to address compromises that were made for timeliness in rapid acquisition.

c. Staffing Timelines for JUONs and JEONs. See Figure G-1.

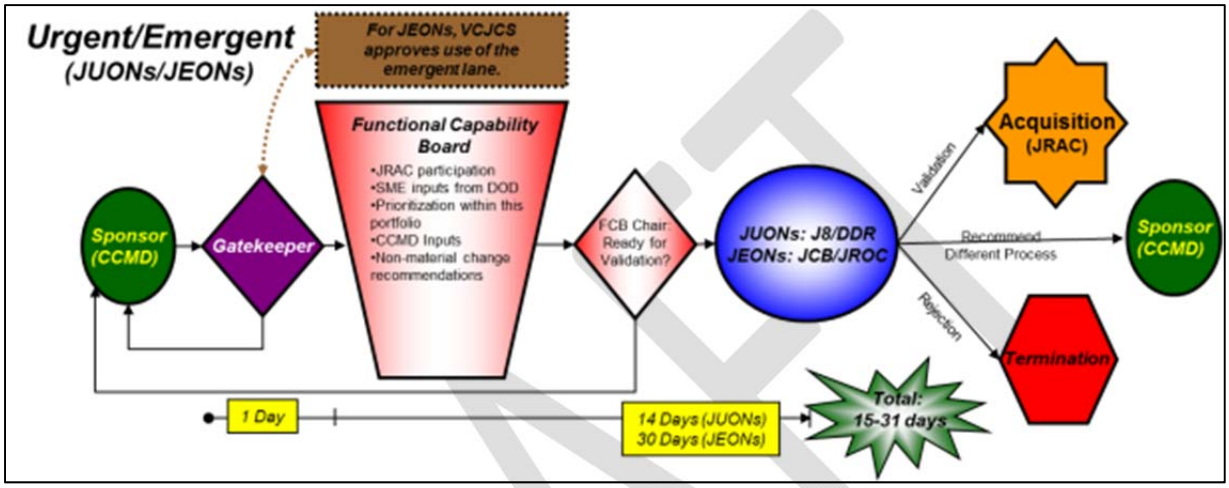

Figure G-1. Urgent/Emergent Staffing Overview

(1) JUON staffing takes no more than 15 days; 1 day for the Joint Staff Gatekeeper to assign a lead FCB for triage, and 14 days for the FCB to conduct triage and present a validation recommendation to the validating authority.

(2) JEON staffing takes no longer than 31 days upon receipt of VCJCS approval to enter the emergent lane of JCIDS; 1 day for the Joint Staff Gatekeeper to assign a lead FCB for review, and 30 days for the FCB to conduct review, prepare a recommendation and schedule the JCB.

(3) Requests for acceleration or extension to staffing timelines may be submitted to the Joint Staff Gatekeeper on a case-by-case basis.

(4) A document Sponsor may withdraw a document from staffing at any time during the staffing process, with notification to the Joint Staff Gatekeeper.

d. Follow-on Activities. Once validated, JUONs, JEONs, and DOD Component UONs allow initiation of rapid acquisition activities to develop and implement capability solutions in a shorter timeframe than typical of deliberate DAS processes. These rapid acquisition activities may also include expedited procurement of COTS/GOTS/NDI solutions, or modification/acceleration of ongoing development programs initiated under the deliberate process. Rapid acquisition in response to validated JUONs, JEONs, and DOD Component

UONs will be accomplished in accordance with references bb, and gg through oo.

2. Staffing of JUONs and JEONs

a. Initiation. JUON and JEON staffing begins when the Joint Staff Gatekeeper receives the document from the Sponsor. All documents undergoing staffing are considered "draft" until validated by the appropriate validating authority.

b. Joint Staff Gatekeeper Review. The Joint Staff Gatekeeper has one day to perform initial review.

(1) Following confirmation that the JUON meets the appropriate entry criteria, JUONs are assigned directly to a Lead FCB and JRAC for collaborative review.

(2) JEONs are first confirmed by the VCJCS, via the Joint Staff Gatekeeper and DJ-8, due to the unique nature of capability requirements associated with anticipated contingency operations. Once the VCJCS provides confirmation that the JEON may use the emergent process, JEONs are assigned to a Lead FCB and JRAC for collaborative review.

c. FCB Review. The Lead FCB, in collaboration with the JRAC, will assess the validity of the JUON or JEON and identify potential solution approaches which could satisfy the capability requirement in the requested timeframe.

(1) The first assessment for JUONs and JEONs is the identification of the driver of the change which necessitates the urgent or emergent need. I.e. – what has changed in strategic guidance, the global context, threats, and/or ongoing or anticipated contingency operations, which now require different action than approved in the Service POMs, previous requirements and acquisition decisions, etc.

(2) As JUONs and JEONs are used ONLY when other means of addressing the requirement such as the GFM process, JMVP, etc., are not practical for satisfying the capability requirement in the operational timelines, the lead FCB will first assess whether there are any more timely approaches to address the urgent or emergent need in place of pursuing a new capability solution. While fielding a capability solution in less than two years is a typical goal, JUONs and JEONs may also be validated to support near-term resourcing and initiation of efforts to field capability solutions in greater than two years.

(3) In addition to considering off-the-shelf COTS/GOTS/NDI solutions or rapid development efforts, the Lead FCB and JRAC review will identify any related JUONs, JEONs, ICDs, CDDs, and CPDs, and the potential to deploy

early prototypes from ongoing acquisition programs or S&T efforts as a rapid means to address the JUON or JEON.

(4) Identification of a potential solution approach is a desired outcome to assist in cost and schedule estimations but is not a required outcome, as the ultimate approach to fulfilling the JUON or JEON will be determined following the requirement validation process. Staffing a JUON or JEON will not be unnecessarily delayed to assess potential solutions.

(5) At the end of their assessment, the Chair of the lead FCB, along with a representative from JRAC, makes a recommendation to the validation authority either for or against validation along with recommended solution approaches, if applicable.

d. Validation Authority

(1) The J-8/DDR is the validation authority for JUONs.

(2) The JROC, or JCB if designated by the VCJCS, is the validation authority for JEONs.

e. Validation Decision

(1) The validation authority provides validation that the JUON or JEON meets the definitions detailed in this section and considered the following:

(a) In support of reference gg, consideration of both the operational timeframe, risk, and the likely impact on mission success or the safety of forces justifies validation of the capability requirement and associated capability gap presented in the JUON or JEON.

(b) The capability requirements and proposed IOC/FOC for fielding capability solutions meet the national military strategy and the urgent/emergent needs of the CCMD(s).

(c) The capability requirements are prioritized higher than all non-urgent/emergent capability requirements, and do not represent unnecessary redundancy in capabilities across the joint force.

(d) Capability solutions have had appropriate consideration of tradeoffs between life cycle cost, schedule, performance, and quantity, with emphasis given to meeting schedule over other factors.

(e) Estimated resource levels required to satisfy the capability requirement are consistent with the priority of the capability requirement, and

in the case of JEONs, consistent with the likelihood of the anticipated contingency operation being executed.

(2) The validation authority will make one of the following decisions:

(a) Validate the JUON or JEON. In addition to the validations outlined above, the validation authority validates that the urgency of resourcing and initiating efforts to satisfy the identified capability requirements to support ongoing or anticipated contingency operations makes use of the deliberate requirements validation process or other processes (GFM process, JMVP, etc.) impractical. Following validation of the JUON or JEON, JRAC will designate a solution Sponsor to rapidly fund, develop, acquire, field, and sustain a capability solution in accordance with reference gg.

(b) Validate part of the JUON or JEON. If it is clear that the Sponsor's capability requirement is best validated through a mix of urgent and deliberate requirements validation processes, the validation authority will validate part of the capability requirement as a JUON or JEON, and recommend the Sponsor re-submit the remainder of the capability requirement for validation in the deliberate requirements validation process or other processes (GFM process, JMVP, etc.).

(c) Reject the JUON or JEON. If the JRAC, FCBs, and/or validation authority anticipate technology challenges or other issues which would prohibit the fielding of a militarily useful solution in the operational timeline, or if the validation authority determines that the criteria for being a JUON or JEON are not met, the validation authority will reject the capability requirement with recommendation that the Sponsor accept risk, adopt a non-materiel approach, or pursue the capability requirement through the deliberate requirements validation process or other processes (GFM process, JMVP, etc.).

f. Validation Duration

(1) Validated JUONs and JEONs remain valid for the timeframe and scope articulated in the original JUON or JEON unless withdrawn by the requirement Sponsor, de-validated by the validation authority, or enduring capability requirements are validated in support of transition of a rapidly fielded capability solution to, or replacing the rapidly fielded capability solution with, an enduring POR.

(2) Limits, if any, on continuing validity of DOD Component UONs are at the discretion of the DOD Component validation authority.

g. Validation Documentation

(1) Validated capability requirements are communicated from the validation authority to the Director, JRAC, via a DDR validation memorandum for JUONs or JROCM for JEONs. Validation documentation typically identifies some or all of the following:

(a) Requestor and general overview of the capability requirement.

(b) Recommended Solution Sponsor. This is the DOD component proposed to be responsible for funding, developing, and fielding the capability solution, in support of the Requirement Sponsor.

(c) Cost. Projected life cycle costs associated with satisfying the urgent/emergent capability requirement, including sustainment costs for the limited period of anticipated use.

(d) Schedule. Specifies the latest allowable fielding date for the capability solution. If incremental fielding is specified, the memo will break the validation into increments, and provide life cycle cost, schedule, performance, and quantity levels for each increment.

(e) Performance. Minimum acceptable performance, in terms of the capability requirements and capability gaps being addressed.

(f) Quantity. Estimated quantity of items necessary to address the capability requirement, including quantities for training and spares, below which the Sponsor's request is no longer relevant/militarily significant, e.g., request 20 vehicles when 10 will not constitute a credible force.

(2) If the JUON or JEON is not validated, the validation authority sends a memorandum to the requirement Sponsor.

(3) Validation decisions will be uploaded to the KM/DS system for archival purposes and to facilitate access to documentation for statutory reporting purposes.

(4) Any changes proposed by the Sponsor which relate directly to the substance of the validation - performance, life cycle cost, schedule, and/or quantity – will be coordinated with the validation authority to determine the level of review required for revalidation by the validation authority.

(5) The validation authority may rescind a previous validation and/or direct changes to or re-staffing of a validated document at any time. The validation authority will notify the document Sponsor in writing, with rationale for the rescission.

3. <u>Modifications to Validated JUONs and JEONs</u>

a. Modification Review. Upon notification from the Joint Staff Gatekeeper of a proposed modification to a previously validated JUON or JEON, the Lead FCB, in coordination with JRAC, will review the proposed changes.

b. Validation Recommendation. The Lead FCB, in coordination with JRAC, will make a validation recommendation to the validation authority.

c. Validation Decision. The validation authority will generate a memorandum either validating the modifications to the JUON or JEON, or documenting the decision to not validate the modifications.

d. Exceptions. Changes to an acquisition program which are consistent with the capability requirement and associated capability gap validated in the original JUON or JEON do not require revalidation.

4. Periodic Validation Reviews

a. Quarterly Review. The Joint Staff Gatekeeper, together with the JRAC, reviews validated JUONs and JEONs quarterly to assess progress toward fielding capability solutions in a timely manner. Similar reviews of validated DOD Component UONs, if used, are at the discretion of the DOD Component validation authority.

b. Biannual Review. Unless withdrawn earlier by the validation authority or requirement Sponsor, or supported by an assessment of limited duration sustainment or proposing validation of enduring capability requirements, the validation authority reviews validated JUONs and JEONs two years after the validation date. This ensures that the urgent capability requirements remain valid, or facilitates validation of enduring capability requirements to support transition of rapidly fielded capability solutions to the deliberate acquisition processes where appropriate. Similar reviews of validated DOD Component UONs, if used, are at the discretion of the DOD Component validation authority.

(1) The Joint Staff Gatekeeper will communicate with the CCMD and the solution Sponsor to see if the capability requirement has changed or if either a capability solution is working or development is expected to produce a suitable capability solution.

(2) In cases where a JUON or JEON was validated and tech-development took longer than two years, the FCB and JRAC will assess whether continued development of the capability solution would be more effectively accomplished by validation of enduring capability requirements and transition to the deliberate acquisition process.

(a) If a JUON or JEON is not making satisfactory progress toward a capability solution for technology development reasons, a recommendation for withdrawal of the JUON or JEON validation may be initiated by the requirement Sponsor, JRAC, or validation authority.

(b) Where appropriate, the withdrawal of the validation by the validation authority will include a mutually agreed to recommendation for an appropriate point in the deliberate process to initiate a deliberate development effort.

(3) This review also serves as a driver to determine if validation of enduring capability requirements and transition of a successfully fielded capability solution to an enduring POR is appropriate, if not already initiated by the Sponsor.

5. Assessment of Operational Utility

a. Timing. For any rapidly fielded capability solution delivered to operational users in response to a JUON or JEON, the original requirement Sponsor will generate an assessment of the capability solution no later than six months after initial delivery to facilitate transition, sustainment, or alternate approaches.

b. Intent. The assessment is intended to be brief and provide feedback against the original capability requirements submitted in the JUON or JEON. These assessments are specifically intended to inform validation authority decision making with respect to:

(1) Making timely changes, where appropriate, to capability requirements validated in JUONs and JEONs, or providing de-validation of capability requirements when no longer required by the original requirement Sponsor.

(2) Validating enduring capability requirements based upon the JUON or JEON, when deemed by the validation authority to be in the best interest of the joint force, to support transition of rapidly fielded capability solutions to enduring PORs.

c. Tailorability

(1) To facilitate follow-on development efforts, the assessment may also document applicable shortcomings in the fielded capability solution and what might be improved in a follow-on effort. It does not limit the ability of the solution Sponsor to provide more in-depth operational testing and assessment as part of acquisition efforts, and does not relieve the PM from conducting acquisition assessments in accordance with reference bb.

(2) If the assessment of operational utility is not practical due to capabilities not being fielded to the user, or insufficient quantities being delivered in the first six months, the validation authority may waive the assessment or specify alternative measures for capturing the intent of the assessment.

d. Disposition. To provide authoritative disposition of rapidly fielded capability solutions, any assessments recommending enduring capability requirements will be endorsed by the original authorizing official (CCMD Commander, Deputy Commander, or Chief of Staff), reviewed by the WG/FCB, and validated by the appropriate validation authority as determined by the Joint Staff Gatekeeper.

(1) For recommendations to transition JUONs or JEONs to enduring capability requirements, the FCB Chair and other stakeholders will evaluate the impact of the transition to the capability requirement portfolio and the priorities of related capabilities.

(a) Note that the transition recommendation is with respect to the capability requirement, and might not result in long term sustainment of the rapidly fielded system if a more appropriate and cost effective replacement can be used.

(b) In cases where the original authorizing official does not recommend a transition to enduring capability requirements, the FCB may still provide recommendations to the validation authority for enduring capability requirements when such a recommendation is in the interest of managing the capability requirement portfolio.

(2) As with other deliberate acquisition programs, the MDA, with validation authority input, will direct via ADM the solution Sponsor to generate JCIDS documents appropriate to the level of follow-on development efforts required – in general a CDD or CPD – to facilitate validation of enduring capability requirements and transition of a rapidly fielded capability solution to a POR for the balance of development, fielding, and sustainment efforts.

(3) The validated JUON or JEON and related assessment of operational utility should be leveraged to minimize the effort required to generate JCIDS documents for follow-on efforts.

(4) Proposals to validate enduring capability requirements and transition a capability solution to a POR must also include an appropriate level of follow-on analysis to ensure that the capability requirements are set appropriately, given an enduring rather than urgent/emergent timeframe, and that the rapidly fielded capability solution remains the most appropriate

alternative for enduring use and sustainment. While some level of assessment was likely performed in support of the rapid acquisition decisions, the timeliness of a solution may have carried greater weight than the life cycle cost or other evaluation factors typical of the deliberate requirements and acquisition processes. In addition, an assessment must be made to ensure that normal acquisition activities and considerations omitted for expediency in the rapid acquisition, are addressed in the validation of enduring capability requirements and planning for transition of a rapidly fielded capability solution to a POR.

f. Archiving. Upon completion, the assessment is posted to the KM/DS studies repository to facilitate sustainment and follow-on efforts.

g. Example Assessment Content. An assessment of operational utility is intended to be documented in memo format and consist of the following sections:

(1) Header info. Date, original requirement/source document and validation date, assessing organization (Requirement Sponsor), POC info, capability solution being assessed, solution organization (Solution Sponsor), POC info, etc.

(2) Assessment period. Identify initial date capability solution was first provided to the end user and length of time upon which the assessment is based. Notional target is for assessments to be provided back to the Joint Staff Gatekeeper no later than six months after initial fielding - balance of providing timely feedback with allowing time for use and assessment. Assessment may be submitted in shorter timeframes, particularly in situations where it is quickly determined that the capability solution does not deliver the required operational utility.

(3) Conclusion. The three categories for the conclusion are:

(a) Failure / Limited Success

1. The fielded capability solution does not provide operational utility satisfying the capability requirements in the validated JUON or JEON. In the assessment, the requirement Sponsor also provides confirmation that the originally requested and validated capability requirements are still appropriate, or identifies any necessary changes for revalidation.

2. The previously validated JUON or JEON does not need to re-enter staffing and validation unless the capability requirement has been changed. For unchanged capability requirements, the JRAC and solution Sponsor will leverage the original validated JUON or JEON to generate a new

funding and fielding plan and develop an alternate capability solution as soon as possible.

(b) Success / Limited Duration Requirement

1. The capability solution satisfies the urgent/emergent capability requirement for the limited duration purposes identified in the validated JUON or JEON.

2. No reassessment of the capability requirements or capability requirement portfolio is required, and the Sponsor will sustain the capability solution for the duration of the validated timeframe and then dispose of the capability solution.

(c) Success / Enduring Requirement

1. The capability solution satisfies the urgent/emergent capability requirement for the limited duration purposes identified in the validated JUON or JEON, but also provides enduring capabilities that should remain in the joint force.

2. For assessments documenting operational utility and an enduring requirement for the rapidly fielded capability solution, the solution Sponsor will continue to sustain the rapidly fielded capability solution until replaced by an alternative capability solution, if applicable.

(4) Required Capability/Performance. Could be as simple as "meets all required capabilities" for a completely successful capability solution. If not delivering all required capabilities, identify shortfalls, limitations, and/or issues with each required capability. Be as specific as possible to better inform further development activities or alternative approaches for delivering the required capabilities.

(5) Changes to CONOPS, Mission(s) and/or Threat(s). Could be as simple as "None" for capability solutions which end up being used exactly as proposed in the original JUON or JEON. If changes were made, either due to the nature of the capability solution, or to innovations/opportunities explored once the capability solution was fielded, identify what has changed and how the capability solution is being used. Details may be used to assist in sustainment and/or further development of the capability solution, as well as provide detail to support validation of enduring capability requirements and transition of capability solutions to a POR when appropriate. (Note that if changes to threat and/or usage drive significant changes to the required capabilities, an update and revalidation of the JUON or JEON may be required.)

(6) Changes to required quantities. Could be as simple as "Same as identified in JUON or JEON" for capability solutions which end up being used exactly as proposed in the original JUON or JEON. If the capability solution has operational utility in a broader sense than originally anticipated, or is being consumed/attrited at a greater rate or over a longer period of time, provide updated estimates of required quantities. (Note that if significant changes are made to the required quantities, an update and revalidation of the JUON or JEON may be required.)

(7) Changes to anticipated sustainment duration (other than for recommendations of enduring capability requirements). Could be as simple as "Same as identified in JUON or JEON" for capability solutions which end up being used exactly as proposed in the original JUON or JEON. If the capability solution has operational utility in the contingency in a broader sense or longer duration than originally anticipated, provide details of anticipated sustainment timeframe. (Align with quantities above, if consumption/attrition is expected to be an issue over the expanded timeframe.)

(8) Other issues/considerations. Identify any other issues which affect the utility and/or sustainment of the capability solution. Issues may include, but are not limited to, fielding, training, reliability/maintainability, interoperability, system security, etc.

(9) Additional opportunities. If the fielded capability solution, or derivatives thereof, is anticipated to provide operational utility to other parts of the joint force, outline any identified opportunities.

(10) Testing data. If any formal or informal testing/evaluation was performed on the capability solution during the assessment period, provide a summary of testing and results. If any follow-on testing is planned, please indicate intended timeframe and scope of testing. Applicable test data and detailed results may be included as an appendix to the assessment. This data can facilitate further refinement/enhancement of the capability solution and provide source data to support proposed validation of enduring capability requirements and support transition of a capability solution to a POR.

(11) Authorized by. Provide release authority's name, rank, and title. Assessments of operational utility must be endorsed by the CCMD Commander, Vice/Deputy Commander, Chief of Staff, or CCMD J8.

DRAFT

ENCLOSURE H

REFERENCES

a. CJCSI 5123.01G, In parallel revision – Date TBD, "Charter of the Joint Requirements Oversight Council"

b. CJCSI 3170.01J, In parallel revision – Date TBD, "Joint Capabilities Integration and Development System"

c. JCIDS Wiki. On NIPRNET – https://www.intelink.gov/wiki/JCIDS. On SIPRNET – http://www.intelink.sgov.gov/wiki/JCIDS.

d. Public Law 109-364, Section 801, 17 October 2006, "Requirements Management Certification Training Program"

e. Defense Acquisition University. On NIPRNET - https://dap.dau.mil

f. DAU "Requirements Management Career Field." On NIPRNET - https://dap.dau.mil/career/rm/Pages/Default.aspx

g. DAU "Student Academic Policies and Information." On NIPRNET - http://www.dau.mil/studentInfo/default.aspx

h. KM/DS System, Version 2. On SIPRNET – http://jrockmdsbpm.js.smil.mil

i. KM/DS Wiki. On SIPRNET – http://www.intelink.sgov.gov/wiki/Portal: JROC_KMDS_Knowledge_Management_and_Decision_Support

j. DOD, "Defense Acquisition Management Information Retrieval (DAMIR)." On NIPRNET – https://ebiz.acq.osd.mil/DAMIR/PortalMain/DamirPortal.aspx

k. DODI 3200.12, 22 August 2013, "DOD Scientific and Technical Information Program (STIP)"

l. DTIC, "Unified Research and Engineering Database." On NIPRNET - https://cbat.dtic.mil/

m. CJCSI 3010.02D, 22 November 2013, "Guidance for Development and Implementation of Joint Concepts." The repository for Joint Concepts is located on NIPRNET – http://www.dtic.mil/futurejointwarfare

n. DODI 8260.2, 21 January 2003, "Implementation of Data Collection, Development, and Management for Strategic Analyses"

DRAFT

o. DODD 8260.05, 7 July 2011, "Support for Strategic Analysis"

p. DOD, 10 August 2012, "DOD Information Enterprise Architecture, Version 2.0". On NIPRNET - http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx

q. Warfighter Mission Area Architecture Federation and Integration Portal (WMA-AFIP). On NIPRNET – https://sadie.nmci.navy.mil/jafe. On SIPRNET – https://ssadie.spawar.navy.smil.mil/sjafe.

r. DODI 3000.04, 24 September 2009, "DOD Munitions Requirements Process (MRP)"

s. DODD 7045.14, 25 January 2013, "The Planning, Programming, Budgeting, and Execution (PPBE) Process"

t. DOD 7000.14-R, "Department of Defense Financial Management Regulation". On NIPRNET – http://comptroller.defense.gov/FMR.aspx.

u. CJCSI 3100.01B, 12 December 2008, "Joint Strategic Planning System"

v. CJCSI 3401.01E, 13 April 2010, "Joint Combat Capability Assessment"

w. CJCSI 3401.02B, 31 May 2011, "Force Readiness Reporting"

x. CJCSI 3460.01C, 9 August 2012, "Combat Support Agency Review Team Assessments"

y. DODI 8260.03, 19 February 2014, "The Global Force Management Data Initiative (GFM-DI)"

z. CJCSM 3130.06, 28 March 2014, "(U) Global Force Management Allocation Policies and Procedures"

aa. DODD 5000.01, 20 November 2007, "The Defense Acquisition System"

bb. DODI Interim 5000.02, 25 November 2013, "Operation of the Defense Acquisition System"

cc. Title 10, USC, section 181, "Joint Requirements Oversight Council"

dd. Title 10, USC, section 2433a, "Critical Cost Growth in Major Defense Acquisition Programs"

ee. Title 10, USC, section 2445c, "Major Automated Information System Programs – Reports: quarterly reports; reports on program changes"

ff. Defense Acquisition Guidebook. On NIPRNET - https://dag.dau.mil.

gg. DODD 5000.71, 24 August 2012, "Rapid Fulfillment of Combatant Commander Urgent Operational Needs"

hh. AFI 10-601, 6 November 2013, "Operational Capability Requirements Development"

ii. AFI 63-114, 4 Jan 2011, "Quick Reaction Capability Process"

jj. AR 71-9, 28 Dec 2009, "Warfighting Capabilities Determination"

kk. TRADOC Regulation 71-20, 28 June 2013, "Concept Development, Capabilities Determination, and Capabilities Integration"

ll. MCO 3900.15B, 10 March 2008, "Marine Corps Expeditionary Force Development System (EFDS)

mm. MCO 3900.17, 17 Oct 2008, "Marine Corps Urgent Needs Process (UNP) and Urgent Universal Needs Statement (Urgent UNS)"

nn. SECNAVINST 5000.2E, 1 Sep 2011, "Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System"

oo. USSOCOM Directive 71-4, 10 May 2012, "Special Operations Forces Capabilities Integration and Development System (SOFCIDS)"

pp. Title 10, USC, section 153, "(Joint Chiefs of Staff:) Chairman: functions"

qq. Title 10, USC, section 163, "(Combatant commands:) Role of Chairman of Joint Chiefs of Staff"

rr. Title 10, USC, section 166, "Combatant commands: budget proposals"

ss. CJCSI 3150.25E, 20 April 2012, "Joint Lessons Learned Program"

tt. JCS J-8 / Force Structure, Resources, and Assessments Directorate, March 2009, "Capabilities-Based Assessment (CBA) User's Guide, Version 3"

uu. TRAC-TD-05-012, 10 May 2010, "Capabilities-Based Assessment (CBA) Guide, Version 3.1"

vv. AFMC - Office of Aerospace Studies, July 2010, "Pre-materiel Development Decision (MDD) Analysis Handbook: A Practical Guide for Analyses from Capabilities-Based Planning to Materiel Development Decision"

ww. CJCSI 5120.02C, 13 January 2012, "Joint Doctrine Development System"

xx. CJCSI 4320.01D, 8 Aug 2008, "Requirement Authorization Documents for Joint Organizations, Joint Task Forces, Special Operations Commands, Standing Joint Force Headquarters, and Other Joint Organizations"

yy. CJCSI 3500.01H, 25 April 2014, "Joint Training Policy for the Armed Forces of the United States"

zz. CJCSI 1800.01D, 15 July 2009 with Change 1 as of 15 December 2011, "Officer Professional Military Education Policy (OPMEP)"

aaa. CJCSI 1805.01A, 1 October 2010 with Change 1 as of 20 September 2011, "Enlisted Professional Military Education Policy"

bbb. CJCSI 1001.01A, 1 October 2010, "Joint Manpower and Personnel Program"

ccc. DODD 4165.06, 13 October 2004, "Real Property"

ddd. DODI 4165.70, 6 April 2005, "Real Property Management"

eee. DODI 5111.16, 27 October 2005, "Policy and Strategy Committee"

fff. CJCSM 3122.01A, 29 September 2006, "Joint Operation Planning and Execution System (JOPES) Volume I – Planning Policies and Procedures"

ggg. CJCSM 3122.02D, 1 April 2011, "Joint Operation Planning and Execution System (JOPES) Volume III –Time-Phased Force and Deployment Data Development and Deployment Execution"

hhh. CJCSM 3130.03, 18 October 2012, "Adaptive Planning and Execution (APEX) – Planning Formats and Guidance"

iii. Joint Publication 5-0, 11 August 2011, "Joint Operation Planning"

jjj. Joint Capability Technology Demonstration Office. On NIPRNET - http://www.acq.osd.mil/rfd

kkk. DODD 2000.19E, 14 February 2006, "Joint Improvised Explosive Device Defeat Organization"

lll. DCMO, April 2013, "Defense Business Systems Investment Management Process Guidance, Version 2.0"

mmm. Global Force Management Board Wiki. On SIPRNET – http://www.intelink.sgov.gov/wiki/Global_Force_Management_Board.

nnn. Title 10, USC, section 2330, "Procurement of contract services: management structure"

ooo. AFMC - Office of Aerospace Studies, June 2013, "Analysis of Alternatives (AoA) Handbook: A Practical Guide to Analyses of Alternatives"

ppp. DOD CIO, August 2010, "DOD Architecture Framework (DODAF), Version 2.02," On NIPRNET – http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework.aspx

qqq. DIA Defense Technology and Long-Range Analysis Office (DIA/TLA), Acquisition Threat Support Division Wiki. On SIPRNET – http://www.intelink.sgov.gov/wiki/TLA-3

rrr. JCS, 10 September 2012, "Capstone Concept for Joint Operations: Joint Force 2020"

sss. CJCSM 3500.04F, 1 June 2011, "Universal Joint Task Manual"

ttt. JROCM 167-03, 22 August 2003, "Joint Command and Control (JC2) Operational Requirement Document (ORD)"

uuu. USD(I) Memorandum, 3 October 2009, "Defense Intelligence Information Enterprise (DIIE) Way Ahead" On NIPRNET – https://intellipedia.intelink.gov/wiki/DI2E_Framework

vvv. PDUSD(P)/DJS Memo to VCJCS, 8 April 2011, "Joint Capability Area (JCA) 2010 Refinement". On NIPRNET - https://jdeis.js.mil/jdeis/jel/training/jca_defs.doc. On SIPRNET – http://jdeis.js.smil.mil/jdeis/jel/futurejointwarfare/jca.htm.

www. DISA Enterprise Content Search and Discovery service. On NIPRNET – https://catalog.ces.mil. On SIPRNET – https://catalog.ces.smil.mil.

DJ-8 and ADNI/SRA Memorandum, 30 July 2013, "Guidelines for Interaction between the Intelligence Community Capability Requirements (ICCR) Process and Joint Capabilities Integration and Development System (JCIDS)"

yyy. Intelligence Community Directive 115, 21 December 2012, "Intelligence Community Capability Requirements Process"

zzz. DJ-8 and DCMO Memorandum, 25 July 2014, "Guidelines for Common Gatekeeping for the Acquisition of Defense Business Systems Documents and

Interactions with the Joint Capabilities Integration and Development System Processes"

aaaa. DODM 5200.01-V2, 24 February 2012 including Change 2 of 19 March 2013, "DOD Information Security Program: Marking of Classified Information"

bbbb. CJCSI 5714.01D, 18 April 2012, "Policy for the Release of Joint Information"

cccc. DODI 8330.01, 21 May 2014, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)"

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

eeee. DODI 2010.06, 29 July 2009, "Materiel Interoperability and Standardization with Allies and Coalition Partners"

ffff. DODI 4120.24, 13 July 2011, Defense Standardization Program (DSP)

gggg. DOD 4120.24-M, March 2000, Defense Standardization Program (DSP) Policies and Procedures

hhhh. DODI 4540.07, 12 October 2004 including Change 1 of 11 Sep 2007, "Operation of the DOD Engineering for Transportability and Deployability Program"

iiii. NR KPP Wiki Page. On NIPRNET – https://www.intelink.gov/wiki/Net_Ready_Key_Performance_Parameter_(NR_KPP)_Manual.

jjjj. JROCM 102-05, 20 May 2005, "Safe Weapons in Joint Warfighting Environments"

kkkk. DODI 5000.69, 9 November 2011, "DOD Joint Services Weapon and Laser System Safety Review Processes"

llll. DOD, 13 May 2011, "DOD Technology Readiness Assessment Guidance" On NIPRNET - https://acc.dau.mil/CommunityBrowser.aspx?id=18545

mmmm. USD(AT&L) Memorandum, 24 April 2013, "Implementation Directive for Better Buying Power 2.0 – Achieving Greater Efficiency and Productivity in Defense Spending"

nnnn. Defense Acquisition Guidebook, Chapter 3, Section 3.2. On NIPRNET - https://dag.dau.mil.

oooo. DOD, October 2012, “Manufacturing Readiness Level (MRL) Deskbook, Version 2.2.1”

pppp. DOD RAM-C Manual, 1 Jun 2009, “Department of Defense Reliability, Availability, Maintainability, and Cost Rationale Report Manual”

qqqq. DOD Directive 8000.01, 10 February 2009, "Management of the Department of Defense Information Enterprise”

rrrr. Joint Publication 3-0, 11 August 2011, “Joint Operations”

ssss. DODI 6055.15, 4 May 2007, “DOD Laser Protection Program”

tttt. DODI 3150.09, 17 September 2008 (with Change 1, 17 August 2009), “The Chemical, Biological, Radiological, Nuclear (CBRN) Survivability Policy”

uuuu. DODD S-5210.81, 8 August 2005, “United States Nuclear Weapons Command and Control, Safety, and Security (U)”

vvvv. DODI 6055.01, 19 August 1998, “DoD Safety and Occupational Health (SOH) Program”

wwww. MIL-STD-1472G, 11 January 2012, “DOD Design Criteria Standard – Human Engineering”

xxxx. JSSG-2010-10, 30 October 1998, “Crew Systems Oxygen Systems Handbook”

yyyy. 29 CFR 1910.95 , “Code of Federal Regulations – Occupational Noise Exposure”

zzzz. JSSG-2010-7, 30 October 1998, “Crew Systems Crash Protection Handbook”

aaaaa. CJCSI 6130.01E, 1 May 2013, “2013 CJCS Master Positioning, Navigation, and Timing Plan (MPNTP)”

bbbbb. DODI 8500.01, 14 March 2014, “Cybersecurity”

ccccc. DODI 5200.44, 5 November 2012, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”

ddddd. CAPE O&S Cost Estimating Structure, on NIPRNET: http://dcarc.pae.osd.mil/reference/osd_ces_index.aspx

DRAFT

eeeee. JROCM 095-09, 1 Jun 2009, "Global Information Grid 2.0 Initial Capabilities Document"

fffff. DOD 4650.1-R1, 26, April 2005, "Link 16 Electromagnetic Compatibility (EMC) Features Certification Process and Requirements"

ggggg. Joint Mission Threads. On NIPRNET – https://wmaafip.csd.disa.mil/Home/Index/?aId=26

hhhhh. Joint Common System Function List, Defense Knowledge Online. On NIPRNET – https://www.intelink.gov/wiki/Joint_Common_System _Function_List. On SIPRNET – http://www.intelink.sgov.gov/wiki/ Joint_Common_System_Function_List.

iiiii. DODI 8410.03, 29 August 2012, "Network Management (NM)"

jjjjj. WMA Architecture Federation Discovery Process. On NIPRNET - https://wmaafip.csd.disa.mil/

kkkkk. CJCSI 6215.01C, 9 November 2007, "Policy for Department of Defense (DOD) Voice Networks with Real Time Services (RTS)"

lllll. Deputy Secretary of Defense, 23 Sep 2010, "Strategic Plan for the Next Generation of Training for the Department of Defense"

mmmmm. DODD 1322.18, 13 January 2009, "Military Training"

nnnnn. CJCSI 3901.01D, 29 March 2013, "Requirements for Geospatial Information and Services"

ooooo. DODI 5000.56, 9 July 2010, "Programming Geospatial Intelligence (GEOINT), Geospatial Information and Services (GI&S), and Geodesy Requirements for Developing Systems"

ppppp. Intelligence Community Directive, ICD 503, 15 September 2008, "Protecting Sensitive Compartmented Information within Information Systems"

qqqqq. Intelligence Community Directive, ICD 705, 26 May 2010, "Physical Security Standards for Sensitive Compartmented Information Facilities"

rrrrr. JP 3-60, 31 January 2013, "Joint Targeting"

sssss. CJCSI 3505.01B, 10 January 2013, "Target Coordinate Mensuration Certification and Program Accreditation"

ttttt. DODD 5250.01, 22 January 2013, "Management of Intelligence Mission Data (IMD) in DOD Acquisition"

uuuuu. DIA Intelligence Mission Data SharePoint Site. On SIPRNET – http://intelshare.intelink.sgov.gov/sites/imdc/lmdppublicshare/default.aspx

vvvvv. JP 3-14, 29 May 2013, "Space Operations"

wwwww. JP 2-01.2, 16 March 2011 incorporating Change 1 of 26 August 2011, "Counterintelligence and Human Intelligence in Joint Operations (U)"

xxxxx. DODI 5200.39, 16 July 2008 incorporating Change 1 of 28 December 2010, "Critical Program Information (CPI) Protection Within the Department of Defense"

yyyyy. DIAD 5000.200, 1 February 2013, "Intelligence Threat Support for Major Defense Acquisition Programs"

zzzzz. DIAI 5000.002, 1 February 2013, "Intelligence Threat Support for Major Defense Acquisition Programs"

aaaaaa. MIL-STD-882E, 11 May 2012, "Department of Defense Standard Practice for System Safety"

bbbbbb. JROCM 235-06, 6 Nov 2006, "Insensitive Munitions Standards and Passing Criteria"

cccccc. MIL-STD-2105D, 19 Apr 2011, "Hazard Assessment Tests for Non-Nuclear Munitions"

dddddd. MIL-STD-1316E, 10 July 1998 with Notice 1 of 14 January 1999, "DOD Design Criteria Standard: Safety Criteria for Fuze Design"

eeeeee. JOTP-051, 10 February 2012, "Technical Manual for the Use of Logic Devices in Safety Features"

ffffff. JOTP-052, 17 March 2012, "Guideline for Qualification of Fuzes, Safe and Arm (S&A) Devices, and Ignition Safety Device (ISDs)"

gggggg. DODD 5160.62, 3 June 2011, "Single Manager Responsibility for Military Explosive Ordnance Disposal Technology and Training (EODT&T)"

hhhhhh. MIL-STD-464C, 1 December 2010, "Electromagnetic Environment Effects Requirements for Systems"

DRAFT

iiiiii. MIL-STD-461F, 10 December 2007, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment"

jjjjjj. DOD 6055.09-M (Volumes 1-8), 29 February 2008, "DOD Ammunition and Explosives Safety Standards"

kkkkkk. CJCSI 5250.01, 15 February 2007, "Special Access Program (SAP) Policy"

llllll. DODD 5205.07, 1 July 2010, "Special Access Program (SAP) Policy"

mmmmmm. JROCM 105-08, 17 May 2008, "Joint Requirements Oversight Council Administrative Procedures and Reference" On SIPRNET – http://www.intelink.sgov.gov/wiki/Joint_Requirements_Oversight_Council_Admin_Guide

nnnnnn. JROCM 067-07, 23 March 2007, "Funding Guidance for Joint Requirement Oversight Council Directed Actions"

oooooo. USD(AT&L) Memorandum, 21 July 2004, "Insensitive Munitions (IM) Strategic Planning"

pppppp. USD(AT&L) Memorandum, 19 March 2007, "Insensitive Munitions Strategic Planning"

qqqqqq. Joint Information Architecture Operational Reference Architecture (JIE ORA) / Warfighting Enterprise Architecture (WEA). On NIPRNET – https://wmaafip.csd.disa.mil/

rrrrrr. DOD Instruction 3222.03, 25 August 2014, "DOD Electromagnetic Environmental Effects (E3) Program"

ssssss. DODI 4650.01, January 9, 2009, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum,"

tttttt. Intelligence Community Joint Architecture Reference Model (IC JARM). On NIPRNET – https://www.intelink.gov/wiki/Joint_Architecture_Working_Group

DRAFT

GLOSSARY

PART I – ACRONYMS

ACAT	Acquisition Category
ACCM	Alternative Compensatory Control Measure
ADM	Acquisition Decision Memorandum
ADNI/SRA	Associate Director of National Intelligence for Systems and Resource Analysis
AO	Action Officer
AoA	Analysis of Alternatives
AOR	Area of Responsibility
APA	Additional Performance Attribute
APB	Acquisition Program Baseline
APUC	Average Procurement Unit Cost
ASD(OEPP)	Assistant Secretary of Defense for Operational Energy Plans and Programs
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
AV-#	(DODAF) All View
BA	Battlespace Awareness (FCB or JCA)
BDA	Battle Damage Assessment
BES	Budget Estimate Submission
BIT	Built-In Test
C2	Command and Control
C&P	Characteristics and Performance
CAC	Common Access Card
CAE	Component Acquisition Executive
CAIV	Cost As an Independent Variable
CAPE	Cost Assessment and Program Evaluation
CAR	Component Appointed Representative
CARD	Cost Analysis Requirements Data
CBA	Capabilities-Based Assessment
CBP	Capabilities-Based Planning
CBRN	Chemical, Biological, Radiological, and Nuclear
CCDR	Combatant Commander
CCJO	Capstone Concept for Joint Operations
CCMD	Combatant Command
CD	Capability Drop
CDD	Capability Development Document
CDR	Critical Design Review
CGA	Capability Gap Assessment
CI	Counterintelligence
CIP	Critical Intelligence Parameter

CJA	Comprehensive Joint Assessment
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CML	Capability-Mission Lattice
CNGB	Chief, National Guard Bureau
COI	Community of Interest
CONOPS	Concept of Operations
CONPLAN	Concept Plan
COP	Community of Practice
COTS	Commercial Off-the-Shelf
CPA	Chairman's Program Assessment
CPD	Capability Production Document
CPM	Capability Portfolio Management
CPR	Chairman's Program Recommendation
CRA	Chairman's Risk Assessment
CSA	Combat Support Agency
CTA	Capstone Threat Assessment
CTC	Combat Training Center
CV-#	(DODAF) Capability View
DAB	Defense Acquisition Board
DAES	Defense Acquisition Executive Summary
DAS	Defense Acquisition System
DASD(MR)	Deputy Assistant Secretary of Defense for Materiel Readiness
DAU	Defense Acquisition University
DAWIA	Defense Acquisition Workforce Improvement Act
DBC	Defense Business Council
DBS	Defense Business System
DCMO	Deputy Chief Management Officer
DCR	DOTmLPF-P Change Recommendation
DI2E	Defense Intelligence Information Environment
DIA	Defense Intelligence Agency
DIA/TLA	DIA Defense Technology and Long-Range Analysis Office
DJ-2	Director, Joint Staff J-2 Directorate for Intelligence
DJ-4	Director, Joint Staff J-4 Directorate for Logistics
DJ-7	Director, Joint Staff J-7 Directorate for Joint Force Development
DJ-8	Director, Joint Staff J-8 Directorate for Force Structure, Resources, and Assessment
DNI	Director of National Intelligence
DOD	Department of Defense
DODAF	DOD Architecture Framework
DOD CIO	DOD Chief Information Officer
DODD	Department of Defense Directive

DRAFT

DODI	Department of Defense Instruction
DOD IEA	DOD Information Enterprise Architecture
DODIN	DOD Information Network
DOTmLPF-P	Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy
DPG	Defense Planning Guidance
DSMC	Defense Systems Management College
DSN	Defense Switching Network
DT	Dwell Time
DTED	Digital Terrain Elevation Data
DUSD(A&T)	Deputy Under Secretary of Defense for Acquisition and Technology
E3	Electromagnetic Environmental Effects
EA	Electronic Attack
EA	Enterprise Architecture
ELINT	Electronic Intelligence
EM	Electromagnetic
EMD	Engineering and Manufacturing Development (Phase of Acquisition)
EMP	Electromagnetic Pulse
ESOH	Environment, Safety, and Occupational Health
EWIR	Electronic Warfare Integrated Reprogramming
FA	Force Application (FCB or JCA)
FCB	Functional Capabilities Board
FCB WG	FCB Working Group
FDD	Full Deployment Decision
FIPT	Functional IPT
FISINT	Foreign Instrumentation Signals Intelligence
FOC	Full Operational Capability
FoS	Family of Systems
FP	Force Protection (KPP)
FUE	first unit equipped
GI&S	Geospatial Information and Services
GEOINT	Geospatial Intelligence
GO/FO	General Officer/Flag Officer
GEF	Guidance for the Employment of the Force
GFM	Global Force Management
GFM	Global Force Management Board
GOTS	Government Off-the-Shelf
GSD	Ground Sample Distance
HERF	Hazards of Electromagnetic Radiation to Fuels
HERP	Hazards of Electromagnetic Radiation to Personnel

DRAFT

HSI	Human Systems Integration
HUMINT	Human Intelligence
IA	Information Assurance
IC	Intelligence Community
IC	International Cooperation
ICCR	Intelligence Community Capability Requirements
ICD	Initial Capabilities Document
ICE	Independent Cost Estimate
IED	Improvised Explosive Device
IM	Insensitive Munition
IMD	Intelligence Mission Data
IOC	Initial Operational Capability
IPL	Integrated Priority List
IPOE	Intelligence Preparation of the Operational Environment
IPT	Integrated Process Teams
IRB	Investment Review Board
IS	Information Systems
ISA	Intelligence Supportability Analysis
ISC	Integrated Security Construct
IS-CDD	Information Systems Capability Development Document
IS-ICD	Information Systems Initial Capabilities Document
ISP	Information Support Plan
ISR	Intelligence, Surveillance, and Reconnaissance
ISSA	Intelligence Sensitivity Systems Assessment
IT	Information Technology
ITEA	Initial Threat Environment Assessment
J-2	Joint Staff Directorate for Intelligence
J2C	Joint Command and Control
J283/IRCO Office	Joint Staff J-2 / Intelligence Requirements Certification
J-4	Joint Staff Directorate for Logistics
J-4/ED	Joint Staff J-4, Engineering Division
J-4/MXD	Joint Staff J-4, Maintenance Division
J-5	Joint Staff Directorate for Strategic Plans and Policy
J-6	Joint Staff J6, Deputy Director for Command and Control Integration
J-7	Joint Staff Directorate for Joint Force Development
J-7/DDI	Joint Staff J-7, Deputy Director for Integration
J-7/JIB	Joint Staff J-7, Joint Integration Branch
J-8	Joint Staff Directorate for Force Structure, Resources, and Assessment
J-8/CAD	Joint Staff J-8, Capabilities and Acquisition Division
J-8/DDC4	Joint Staff J-8, Deputy Director for C4
J-8/DDFP	Joint Staff J-8, Deputy Director for Force Protection

J-8/DDR	Joint Staff J-8, Deputy Director for Requirements
J-8/DDRA	Joint Staff J-8, Deputy Director for Resources and Acquisition
J-8/JRAD	Joint Staff J-8, Joint Requirements Assessment Division
J-8/PBAD	Joint Staff J-8, Program and Budget Analysis Division
J-8/SAPCOORD	Joint Staff J-8, Special Access Program Coordinator
JCA	Joint Capability Area
JCB	Joint Capabilities Board
JCD	Joint Concept Development
JCCA	Joint Combat Capability Assessment
JCIDS	Joint Capabilities Integration and Development System
JCTD	Joint Capability Technology Demonstration
JDEIS	Joint Doctrine, Education, & Training Electronic Information System
JDIR	Joint Staff Director
JEON	Joint Emergent Operational Need
JIE	Joint Intelligence Estimate
JIE ORA	Joint Information Environment Operational Reference Architecture
JIEDDO	Joint Improvised Explosive Device Defeat Organization
JIPOE	Joint Intelligence Preparation of the Operational Environment
JITC	Joint Interoperability Test Command
JLE	Joint Logistics Estimate
JMT	Joint Mission Thread
JMVP	Joint Manpower Validation Process
JPE	Joint Personnel Estimate
JRAC	Joint Rapid Acquisition Cell
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JSA	Joint Strategic Assessment
JSAP	Joint Staff Action Processing (task)
JSCP	Joint Strategic Capabilities Plan
JSD	Joint Staffing Designator
JSPS	Joint Strategic Planning System
JSR	Joint Strategic Review
JTRS	Joint Tactical Radio System
JUON	Joint Urgent Operational Need
JWICS	Joint Worldwide Intelligence Communications System
JWSTAP	Joint Weapons Safety Technical Advisory Panel
KM/DS	Knowledge Management/Decision Support
KPP	Key Performance Parameter
KSA	Key System Attribute
LCCE	Life Cycle Cost Estimate

LMDP	Life cycle Mission Data Plan
MAIS	Major Automated Information System
MASINT	Measurement and Signatures Intelligence
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDD	Materiel Development Decision
MEA	Munitions Effects Assessment
MEF	Mission Essential Functions
MER	Manpower Estimation Report
METOC	Meteorological and Oceanographic
MILCON	Military Construction
MILPERS	Military Personnel
MIP	Military Intelligence Program
MOE	Measure of Effectiveness
MOP	Measure of Performance
MQR	MAIS Quarterly Report
MRA	Manufacturing Readiness Assessment
MRP	Munitions Requirements Process
MS	Milestone
MSA	Materiel Solution Analysis (Phase of Acquisition)
MSA	Major System Acquisition
MSFD	Multi-Service Force Deployment
MT	Mission Thread
NDI	Non Developmental Item
NDS	National Defense Strategy
NETOPS	Network Operations
NGA	National Geospatial-Intelligence Agency
NIIRS	National Imagery Interpretability Rating Scale
NIP	National Intelligence Program
NIPRNET	Non-secure Internet Protocol Router Network
NMS	National Military Strategy
NR	Net-Ready (KPP)
NSA	National Security Agency
NSS	National Security Strategy
NSS	National Security System
O&M	Operations and Maintenance
O&S	Operating and Support (Cost)
O&S	Operations and Support (Phase of Acquisition)
OIPT	Overarching Integrated Process Team
OOB	Order of Battle
OMB	Office of Management and Budget
OMS/MP	Operational Mode Summary/Mission Profile
OPLAN	Operation Plan

DRAFT

OPR	Office of Primary Responsibility
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OV-#	(DODAF) Operational View
P&D	Production and Deployment (Phase of Acquisition)
PAUC	Program Acquisition Unit Cost
PBR	Program and Budget Review
PDR	Preliminary Design Review
PDUSD(P)	Principle Deputy Undersecretary of Defense for Policy
PED	Processing, Exploitation, and Dissemination
PES	Physical Exchange Specification
PIIT	Platform Integration Information Table
PKI	Public Key Infrastructure
PM	Program Manager
PNT	Positioning, Navigation, and Timing
POC	Point of Contact
POM	Program Objective Memorandum
POR	Program of Record
PPBE	Planning, Programming, Budgeting, and Execution
PPP	Program Protection Plan
PSA	Principal Staff Assistant
QDR	Quadrennial Defense Review
RFC	Request for Capabilities
RFF	Request for Forces
RFP	Request for Proposals
RMCT	Requirements Management Certification Training
RDP	Requirements Definition Package
RDT&E	Research, Development, Test, and Evaluation
S&T	Science and Technology
SAASM	Selective Availability Anti-Spoofing Module
SAP	Special Access Program
SAPCO	Special Access Program Control Office
SAR	Selected Acquisition Report
SAR	Special Access Required
SATCOM	Satellite Communication
SCI	Sensitive Compartmented Information
SEP	Systems Engineering Plan
SES	Senior Executive Service
SIG	Senior Integration Group
SIGINT	Signals Intelligence
SIPRNET	SECRET Internet Protocol Router Network
SME	Subject Matter Expert

DRAFT

SoS	System of Systems
SS	System Survivability (KPP)
SSA	Support for Strategic Analysis
STA	System Threat Assessment
STAR	System Threat Assessment Report
SV-#	(DODAF) Systems View
SWAP-C	Space, Weight, Power, and Cooling
T&E	Test and Evaluation
TDL	Tactical Data Link
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction
TOA	Total Obligation Authority
TOC	Total Ownership Cost
TOS	Time on Station
TRA	Technology Readiness Assessment
TRL	Technology Readiness Level
UCP	Unified Command Plan
UJT	Universal Joint Task
UJTL	Universal Joint Task List
UON	Urgent Operational Need
URL	Uniform Resource Locator
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)	Under Secretary of Defense (Comptroller)
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSOCOM	United States Special Operations Command
UXO	Unexploded Ordnance
VCJCS	Vice Chairman of the Joint Chiefs of Staff
VTC	Video Teleconference
WARM	Wartime Reserve Mode
WEA	Warfighting Enterprise Architecture
WMA	Warfighter Mission Area
WMA-AFIP	WMA Architecture Federation and Integration Portal
WSE	Weapon Safety Endorsement

DRAFT

PART II — DEFINITIONS

Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this manual only.

Capability – The ability to complete a task or execute a course of action under specified conditions and level of performance. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Capability Gap – The inability to meet or exceed a capability requirement, resulting in an associated operational risk until closed or mitigated. The gap may be the result of no fielded capability, lack of proficiency or sufficiency in a fielded capability solution, or the need to replace a fielded capability solution to prevent a future gap. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Capability Gap Assessment (CGA) – A deliberate assessment of the future years defense program that reviews CCMD IPLs and other issues and perspectives from the Services and other DOD Components, relative to fielded materiel and non-materiel capability solutions, and development efforts which may already be underway to address capability gaps. (SOURCE: CJCSI 5123.01/3170.01)

Capability Need – see "Capability Requirement".

Capability Requirement – A capability which is required to meet an organization's roles, functions, and missions in current or future operations. To the greatest extent possible, capability requirements are described in relation to tasks, standards, and conditions in accordance with the Universal Joint Task List or equivalent DOD Component Task List. If a capability requirement is not satisfied by a capability solution, then there is also an associated capability gap. A requirement is considered to be 'draft' or 'proposed' until validated by the appropriate authority. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Capability Requirement Document – Any document used to articulate either deliberate or urgent/emergent capability requirements and associated information pertinent to review and validation. (SOURCE: CJCSI 5123.01/3170.01)

Capability Solution – A materiel solution or non-materiel solution to satisfy one or more capability requirements and reduce or eliminate one or more capability gaps. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Contingency Operation – A military operation that (a) is designated by the Secretary of Defense as an operation in which members of the armed forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing military force; or (b) results

in the call or order to, or retention on, active duty of members of the uniformed services under section 688, 12301(a), 12302, 12304, 12304a, 12305, or 12406 of [Title 10], chapter 15 of [Title 10], section 712 of title 14, or any other provision of law during a war or during a national emergency declared by the President or Congress. (SOURCE: 10 USC 101)

Core Mission Area – DOD core mission areas identified under the most recent Quadrennial Roles and Missions (QRM) review are: Homeland Defense and Civil Support (HD/CS); Deterrence Operations; Major Combat Operations (MCOs); Irregular Warfare; Military Support to Stabilization Security, Transition, and Reconstruction Operations; Military Contribution to Cooperative Security. (SOURCE: 2009 Quadrennial Roles and Missions Review Report)

Document Sponsor – The organization submitting a capability requirement document. Solution Sponsors for successor documents – Capability Development Documents (CDDs), Capability Production Documents (CPDs), and Joint DOTmLPF-P Change Recommendations (Joint DCRs) - may be different than the Requirement Sponsors for initial documents – Initial Capabilities Documents (ICDs), Urgent Operational Needs (UONs), Joint UONs (JUONs), and Joint Emergent Operational Needs (JEONs). Different Sponsors for requirements and solutions can occur when the initial document Sponsor does not have acquisition authority and a different organization is designated to develop and field a capability solution, or when one Sponsor elects to leverage a previously validated document generated by a different Sponsor. (SOURCE: CJCSI 5123.01/3170.01)

DOD Components – The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the CCMDs, the Office of the Inspector General of the Department of Defense, the Department of Defense Agencies, field activities, and all other organizational entities in the Department of Defense. (SOURCE: CJCSI 5123.01/3170.01)

Gap – See "Capability Gap".

Integrated Priority List (IPL) – A list of a combatant commander's highest priority requirements, prioritized across Service and functional lines, defining shortfalls in key programs that, in the judgment of the combatant commander, adversely affect the capability of the combatant commander's forces to accomplish their assigned mission. Also called IPL. (JP 1-02. SOURCE: JP 1-04)

Joint – Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JP 1-02. SOURCE: JP 1)

Note that this definition of "joint" is applicable to requirement documents and capability solutions which apply to more than one DOD Component. See "joint

military requirement" for the definition applicable to Title 10 JROC responsibilities.

Joint Emergent Operational Need (JEON) – UONs that are identified by a CCMD, CJCS, or VCJCS as inherently joint and impacting an anticipated contingency operation. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Joint Military Requirement – A capability necessary to fulfill or prevent a gap in a core mission area of the Department of Defense. (SOURCE: 10 USC 181)

Note that the Title 10 responsibilities of the JROC over "joint military requirements" include both joint requirements and single DOD Component requirements which makeup the entirety of the capabilities of the joint force and enable the DOD core mission areas.

Joint Urgent Operational Need (JUON) – UONs that are identified by a CCMD, CJCS, or VCJCS as inherently joint and impacting an ongoing contingency operation. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Materiel (Capability Solution) – All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. See also equipment; personal property. (JP 1-02. SOURCE: JP 4-0)

Need – See "Capability Requirement".

Non-materiel (Capability Solution) – Changes to doctrine, organization, training, (previously fielded) materiel, leadership and education, personnel, facilities, and/or policy, implemented to satisfy one or more capability requirements (or needs) and reduce or eliminate one or more capability gaps, without the need to develop or purchase new materiel capability solutions. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Rapid Acquisition – A streamlined and tightly integrated iterative approach, acting upon validated urgent or emergent capability requirements, to: conduct analysis and evaluate alternatives and identify preferred solutions; develop and approve acquisition documents; contract using all available statutory and regulatory authorities and waivers and deviations of such, appropriate to the situation; identify and minimize technical development, integration, and manufacturing risks; and rapidly produce and deliver required capabilities. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Requirement – See "Capability Requirement".

Requirement Sponsor – See "Document Sponsor".

Solution – See "Capability Solution".

Solution Sponsor – See "Document Sponsor".

Sponsor – See "Document Sponsor".

Threat – The sum of the potential strengths, capabilities, and strategic objectives of any adversary which can limit or negate mission accomplishment or reduce force, system, or equipment effectiveness. It does not include (a) natural or environmental factors affecting the ability or the system to function or support mission accomplishment, (b) mechanical or component failure affecting mission accomplishment unless caused by adversary action, or (c) program issues related to budgeting, restructuring, or cancellation of a program. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Urgent Operational Need (UON) – Capability requirements identified as impacting an ongoing or anticipated contingency operation. If left unfulfilled, UONs result in capability gaps potentially resulting in loss of life or critical mission failure. When validated by a single DOD Component, these are known as DOD Component UONs. DOD Components, in their own terminology, may use a different name for a UON. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

Validation – The review and approval of capability requirement documents by a designated validation authority. The JROC is the ultimate validation authority for capability requirements unless otherwise delegated to a subordinate board or to a designated validation authority in a Service, CCMD, or other DOD Component. (Proposed for JP 1-02. SOURCE: CJCSI 5123.01/3170.01)

DRAFT