AF/A5/7
CAPABILITY DEVELOPMENT GUIDEBOOK

Volume 2D

JCIDS Document Development

October 2023

Air Force Futures, Center 2, Requirements Oversight Team

AF/A5DR, Pentagon 5C858

PREFACE

This Guidebook is one in a series of AF/A5DR developed guides describing the Air Force process for validation of operational capability requirements in support of overarching Capability Development efforts. This guidebook describes the specific requirements actions that support Joint Capabilities Integration and Development System (JCIDS) document development.

This Guidebook is based on the 2023 DRAFT JCIDS Manual and will be updated when the Manual is published.

This Guidebook is a "how to" guide for use by all stakeholders participating in the USAF requirements process, and in some cases, it includes answers to the questions like, "why do we have to do it that way," "where is that written," and "where do we find additional information."

Although the AF/A5/7 Capability Development Guidebooks are not statutory or regulatory in nature, they represent official guidance and recommended standard procedures developed by AF/A5D to ensure compliance with and implementation of overarching Requirements and Acquisition policies. Per AF/A5/7 direction and authority under HAF Mission Directive 1-57, Air Force requirements sponsors will follow the guidance and procedures described in these guidebooks or coordinate with AF/A5D through the AF/A5DR Requirements Oversight Enabling Team for case-by-case tailoring.

There are no restrictions on release or distribution of this guidebook.

Additional guidance and information to supplement this Guidebook is located on the AF/A5DR Requirements Policy & Integration Portal Page:

- Go to https://www.my.af.mil
- Navigate to "BASE, ORG & FUNCTIONAL AREA", select, Organizations A-Z
- On the "Organizations A-Z ribbon, select, "HAF"
- Scroll down and select AF/A5/7 -Air Force Futures
- On the left ribbon, select "SUB-ORGANIZATIONS," then, "AF/A5DR – Requirements Policy & Integration"

If you have questions regarding the Volume 2-series Capability Development Guidebooks or if you have suggestions for improvements, please contact:

AF Gatekeeper: Mr. Richard "Bullet" Tobasco, richard.tobasco.2@us.af.mil, (703)692-4197, DSN 222

Guidebook OPR: Mr. Jeff "Shredder" Hackman, jeffrey.hackman.1@us.af.mil, (703)692-1087, DSN 222

CHANGE SUMMARY

Change Summary	Date
This document captures updated organizations, roles, responsibilities, DoD and DAF guidance for operational requirements development and must be reviewed in its entirety. Portions of this guidebook were derived from the AF/A5R Requirements Guidebook Volume 3 (24 June 2020, Version 5.02), which is rescinded and replaced by this Capability Development Guidebook Volume 2D.	N/A
Removed references to CDC and CDWG. Removed AoA process as it is now in Guidebook Vol 2D, Annex A. Office symbol updates and Admin changes.	Oct 2022
Added document checklists	Jan 2023
Updated document checklists. Revised to meet 2023 JCIDS Manual (draft). Revised process charts. Included RAI guidance and checklist.	May 2023
Added Software-ICD process and checklist. Added typical staffing timelines to process charts.	Jul 2023
Admin changes.	September 2023
Included language that allows CPMR data to be used in-lieu-of a CBA. Admin changes.	October 2023

TABLE OF CONTENTS

SECTION 1. INTRODUCTION

1.1. Overview and Background. This guidebook outlines the requirements activities to support the Joint Capabilities Integration and Development System (JCIDS). JCIDS enables the Joint Requirements Oversight Council (JROC) and the Air Force Requirements Oversight Council (AFROC) to execute their statutory duties to assess military capabilities, and identify, approve, and prioritize gaps in these capabilities, to meet applicable requirements in the National Defense Strategy (NDS). This guidebook describes the USAF implementation of the JCIDS process.

1.2. JCIDS Document Descriptions. Below are summaries of the documents used to articulate capability requirements and associated gaps. All documents, supporting documentation, and decision memoranda are archived in the Information and Resource Support System (IRSS) except for Capability Development Plans (CDP) and System Development Plans (SDP) which are archived in the AF/A5D CDP/SDP repository.

1.2.1. Initial Capabilities Document (ICD) and Variants. An ICD specifies capability requirements and associated gaps which represent unacceptable operational risk if left unmitigated. The ICD also recommends partial or complete mitigation of identified gaps with materiel solutions, non-materiel solutions or some combination of both. A validated ICD is an entry criterion for the Materiel Development Decision and guides activities during the Materiel Solution Analysis phase of acquisition. The development and validation process is described in Section 2.3.2.

1.2.1.1. The Information Systems (IS)-ICD is a variant of the regular ICD, implementing the Information Technology (IT) Box construct described in Section 2.4 of this Guidebook. IS-ICDs streamline the requirements process by delegating oversight and formats for subsequent documents as identified in the IS-ICD.

1.2.1.2. The Software (SW)-ICD facilitates efficient and timely software development efforts using an expedited process. The SW-ICD is designed to enable modern software development practices and rapidly deliver mission impactful software. SW-ICDs are not appropriate for hardware development efforts or capturing capability requirements that span a broad scope of hardware, software, and/or Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities, and Policy (DOTmLPF-P) efforts. The SW-ICD does not use the IT Box construct for governance. Special considerations for software development are discussed further in section 1.2.5.

1.2.2. Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities – Policy Change Recommendation. A Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities – Policy (DOTmLPF) Change Recommendation (DCR) recommends mitigating identified capability gaps with a non-materiel approach, through changes in one or more of the DOTmLPF-P areas. A DCR may be used to propose non-materiel and/or non-developmental materiel (little “m”) capability solutions as an alternative to or in conjunction with developmental materiel solutions (Big “M”). The letter “m” in the acronym is usually lower case, since DCRs do not advocate new materiel development, but rather advocate increased quantities or alternate applications of existing materiel to include commercial off-the-shelf, government off-the-shelf, or non-developmental item. Regardless of the solution, Interoperability and Exportability: Allied Partner/Coalition Use should be considered and addressed. A DCR may be initiated during any phase of the JCIDS or acquisition process. A Joint DCR is used when proposed solutions require implementation of DOTmLPF-P changes by other organizations outside the USAF. The development and validation process is described in Section 2.3.1.

1.2.3. Capability Development Document (CDD) and Variants. The CDD provides traceability to predecessor documents and validated capability requirements, provides supporting data for certifications and endorsements, identifies related DOTmLPF-P impacts of the proposed capability solution, and outlines projected lifecycle costs that are expected to result from pursuing the capability solution. A CDD

proposes development of a materiel capability solution intended to satisfy approved capability requirements wholly or partially to close or mitigate associated capability gaps for which the DoD does not want to accept operational risk. A CDD specifies requirements, in terms of system level performance attributes which include Key Performance Parameters (KPP), Key System Attributes (KSA), and Additional Performance Attributes (APA) to support development of one or more increments of a materiel capability solution. A validated CDD is necessary for the Development Request for Proposal (RFP) release decision point prior to the Milestone B acquisition decision for Major Capability Acquisitions. Special cases where program milestones are waived or combined may also require validated CDDs. See Enclosure A of the JCIDS Manual for details. The development and validation process is described in Section 2.3.3.

In an incremental development approach, a Sponsor describes the system and performance attributes of the initial capability solution in a base CDD. As a capability is added to the base system over time as block upgrades are developed, the Sponsor may document this in an Annex to the base CDD.

In a Family of Systems (FoS) approach, Sponsors develop unique capabilities which are provided through different interdependent systems in a base CDD that describes the core characteristics and attributes. The base FoS CDD will specify attributes for the entire FoS and CDD Annexes will specify additional attributes for the individual systems. The CDD Annexes are used to specify the unique performance attributes for each variant system in the FoS capability over time. The Sponsor may develop a base CDD concurrently with the Annexes for each individual interdependent systems within the family. The base CDD may be validated for the first increment, and then use CDD Annexes, separated by time, to validate each subsequent additional capability.

In a Systems of Systems (SoS) approach where a set of independent systems are integrated to deliver a unique capability solution, the Sponsors should develop individual CDDs for each system within the SoS. In this approach, an ICD may lead to multiple independent CDDs. The CDD variants described below can be applied to each individual SoS CDD.

1.2.3.1. A CDD Update is developed in the same format as the original validated CDD and contains knowledge gained during source selection and Engineering, Management, and Development phase activity. Performance attributes set in the initial CDD may change as more information is gained. If excessive time has passed, certifications and endorsements may need to be updated due to capability, threat, or mission changes, Joint Performance Requirement (JPR)/KPP attribute additions/deletions, or the current JCIDS Manual has mandatory requirements that shall be addressed. In this case, the original validated document will be updated to the most current JCIDS Manual for format and content and reviewed in its entirety. An update may also be required because of JROC/Joint Capabilities Board (JCB) Tripwire, Critical Intelligence Parameter (CIP) breach reviews, Nunn-McCurdy Breach, or Major Automated Information System Critical Change Report reviews. A CDD Update follows the same development and staffing processes as a full CDD.

1.2.3.2. A CDD Annex is used for FoS, System of Systems (SoS), and Incremental approaches and only identifies changes to the CDD upon which it is based. They are used to specify the unique performance attributes for each variant system or increment over time. Annexes may be developed concurrently with the base CDD for each individual interdependent systems within the family or system. The CDD Annex follows the same rules for format, content, and staffing as the CDD and CDD Update. The CDD Annex is always staffed with and accompanied by its base CDD.

1.2.3.3. A draft CDD (dCDD) is a stand-alone document with limited scope and content that outlines the minimum essential information for technology maturation and preliminary design for development of a materiel solution or capability increment and should describe a Minimum Viable Product to ensure RFPs and other documents are clear on the capability needed. The dCDD is prepared post Analysis of

Alternatives (AoA) and is required to support Milestone A and Technology Maturation and Risk Reduction (TMRR). There is no mandatory content. The Milestone A Milestone Decision Authority (MDA) should provide content requirements. The dCDD does not require Joint review or validation. A dCDD Annex may be developed for an incremental program as a precursor to a CDD Annex to a previously validated CDD.

1.2.4. Document Sequencing. The deliberate JCIDS documents do not have to follow a linear sequence and may follow variations such as those as shown in Figure 1.1. For example, A CDD does not always require a CDD, or a single ICD may spawn multiple CDDs. Consult the AF/A5DR and the AF Gatekeeper for options.

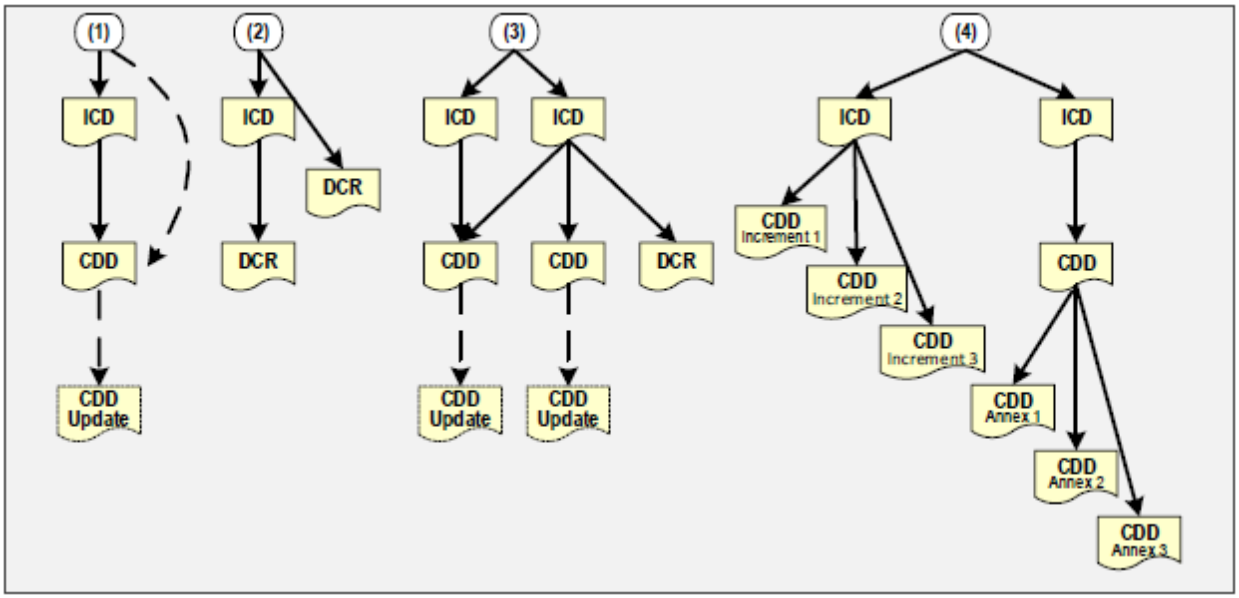

Figure 1.1. Document Sequences

1.2.5. Other Capability Development Process Documents.

1.2.5.1. Joint Urgent Operational Need (JUON), Joint Emergent Operational Need (JEON), and USAF Urgent Operational Need (UON). A JUON, JEON, or USAF UON specifies requirements driven by ongoing or anticipated contingency operations, which if left unfulfilled, would result in capability gaps leading to loss of life or critical mission failure. A validated JUON, JEON, or USAF UON, or other validated requirement, is necessary to initiate urgent capability acquisition efforts. JUONs and JEONs are initiated by Combatant Commands and go through a Joint Process that includes the Functional Capability Boards (FCB). The USAF UON process is covered in AF/A5/7 Capability Development Guidebook Volume 2G.

1.2.5.2. The Middle Tier Acquisition (MTA) documents are outside the JCIDS process but much of the content is referenced in the JCIDS Manual. MTA is a rapid acquisition approach within the Adaptive Acquisition Framework that focuses on rapidly delivering capability to fill an identified mission capability gap. MTA capability requirements are documented in a Rapid Prototyping Requirements Document or a Rapid Fielding Requirements Document. These documents are staffed within USAF only and then provided for information to the Joint Staff Gatekeeper. There may be special cases where MTA documents are staffed to USSF as well for combined DAF signatures. Format, content, and staffing details are in AF/A5/7 Capability Development Guidebook Volume 2F.

1.2.5.3. The Capabilities Based Assessment (CBA) provides a robust assessment of a 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 and provides an analytic basis to identify capability and associated

capability gaps prior to development and submission of JCIDS documents for review and validation. USAF CBA guidance is in AF/A5/7 Capability Development Guidebook Volume 2C.

1.2.5.4. The Analysis of Alternatives (AoA) is an analytical comparison of the operational effectiveness, suitability, risk, and life cycle cost of potential alternatives under consideration to satisfy the validated capability needs that are usually stipulated in a validated ICD. USAF AoA guidance is in AF/A5/7 Capability Development Guidebook Volume 2D, Annex A.

1.2.5.5. The Strategic Requirements Document is a USAF-only, strategic level requirements document that validates the need for early capability development activities. It broadly describes the required capabilities within a future context and outlines the primary capability gaps the USAF must address to achieve success. Solution possibilities may lead to agile and innovative capability development using JCIDS or non-JCIDS requirements documentation and authorities within the USAF and Joint requirements processes. Guidance is in AF/A5/7 Capability Development Guidebook Volume 2E.

1.2.5.6. The Capability Needs Statement (CNS) and its companion document, the User Agreement (UA) are AF-only documents that define the requirements for the non-JCIDS Software Acquisition Pathway and provide a commitment to continuous user involvement during development. Special considerations for software requirements development are discussed further in section 1.2.5. CNS and UA guidance are in AF/A5/7 Capability Development Guidebook Volume 2I.

1.2.5.7. The AF Form 1067 provides a means to initiate and document the submission, review, and approval of requirements for permanent sustainment and capability modifications, track modification proposals through the approval/funding process, and to initiate actions to maintain configuration control of items affected by the modification, even though the capability is described in a previously approved capability requirements document. The procedures for the staffing and validation of the AF Form 1067 are in AF/A5/7 Capability Development Guidebook Volume 2H. Detailed instructions for completing the AF Form 1067 are in AFI63-101/20-101, Chapter 9 and Attachment 2.

1.2.5.8. There are two USAF-internal, foundational Capability Development documents. They are not formal JCIDS documents; however, they do form the basis for all follow-on capability requirements development. Guidance is in AF/A5/7 Capability Development Guidebook Volume 2B.

1.2.5.8.1. The CDP is a written proposal describing a plan of action to implement the capabilities needed to address strategic mission gaps and describes the activities that will be pursued to provide the needed capability to the warfighter. The CDP also serves to sequence, prioritize and structure the SDP that capture plans to field the validated operational requirements into capability solutions.

1.2.5.8.2. The SDP show how Requirements, Acquisition, and Resourcing products and decisions are aligned to ensure capability solutions described in CDPs field on time. They capture all the activities that are necessary to bring the capability online.

1.2.6. Software Requirements Development. As noted above, two solutions pathways are available for software only acquisition. Both rely on the key tenets of Agile Software development.

1.2.6.1. Key Tenets of Agile Software Requirements Development. The key to agile software development is to form a collaborative cross-functional team with a focus on involvement from the customer/end-user of the system. Software development necessitates a unique approach that is drastically different from traditional materiel solution development for hardware systems. While hardware development requires explicit requirements up front to drive the system design and development, software development should not. Agile software development works best with flexible requirements up front, without the rigid specificity and detailed documentation that is typical of the material solution requirements process.

The focus of software development is on solution development; end users over process. An emphasis on early delivery of capability followed by iterative and evolutionary updates for continual improvement to the product based on user needs and continuous feedback that is responsive to user needs, rather than adhering to plans and milestones. The primary metric is delivery of useable solutions, not documentation. The team should encourage the evolution of requirements to avoid obsolescence.

Agile Software Development requires a team of competent, dynamic, and effective participants and stakeholders. The entire team needs to work as one toward a shared vision. A project plan or roadmap is useful and necessary, but it must not be seen as a rigid set of milestones or limitations – the metric of success is not simply to lay out a plan and follow it relentlessly. The metric is to produce value for the warfighter. Traditional or linear approaches to program plans and roadmaps cannot replace the need for flexibility and adaptability to get things done, which may include abandoning the previous plan. This type of approach requires close and continuous collaboration and trust relationships between all the team members in both the Planning and Execution Phases.

The Sponsor and the AF/A5/7 SME must engage with the appropriate Acquisition Program Office, SAF/AQX, SAF/FMB, AF/A8P, and AF/A8X to determine the timing and scale of resources required for the Document Writing Team (DWT) and overall software development effort. The Sponsor and the AF/A5/7 SME must also engage with SAF/AQR, SAF/AQX, and other relevant acquisition stakeholders to build consensus on the appropriate software acquisition pathway.

1.2.6.2. Software Requirements Documents

1.2.6.2.1. JCIDS includes a software pathway to capture requirements for software development using a SW-ICD. The SW-ICD is not to be confused with the Information Systems JCIDS documents. The Information Systems documents are governed by the Information Technology (IT)-Box and include hardware components. The SW-ICD is a separate and distinct process, will not include hardware, and is not governed by the IT-Box.

The SW-ICD facilitates efficient and timely software development efforts by using an expedited process within the JCIDS structure to enable modern software development practices and rapidly deliver mission impactful software. It is not appropriate for hardware development efforts or for capturing capability requirements that span a broad scope of hardware, software, and/or Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P) efforts. SW-ICDs may be used to document embedded software requirements for a capability solution developed under other validated JCIDS documents. In this case, since the software requirements were validated as part of the overall capability solution, the SW-ICD does not require further staffing.

The SW-ICD is the preferred method for software programs that the Joint Staff J8 believes warrant their oversight. Software capability requirements that the Joint Staff determines to have Joint Equities must use the SW-ICD format and validation procedures. Following AF review and validation, AF/A5DR will send the SW-ICD to the Joint Staff Gatekeeper (JSGK) for expedited staffing and validation. Programs that do not have Joint equities may use the Software Acquisition Pathway described in AF/A5/7 Capability Development Guidebook Vol 2I.

Software acquisition from a validated SW-ICD is governed by the overarching acquisition policies and management principles of the Defense Acquisition System as described in DoD Directive 5000.01 and DoD Instruction 5000.02. Acquisition governance is outside the scope of this Guidebook, but requirement sponsors should be familiar with the acquisition system being pursued. The document development process is identical to the ICD detailed in section 2.3.2.

1.2.6.2.2. The Capability Needs Statement (CNS) is an AF-only document that defines the requirements for the non-JCIDS Software Acquisition Pathway. It is a high-level document that captures the need and

provides enough information to define the software solution space in view of the overall threat environment. The document identifies mission deficiencies, required enhancements to existing operational systems, features, interoperability needs, legacy interfaces, and other attributes required for new software-intensive systems, sub-systems, or upgrades to existing systems or sub-systems. Special considerations for software requirements development are discussed further in section 1.2.5. CNS guidance is in AF/A5/7 Capability Development Guidebook Volume 2I.

The companion document to the CNS is the User Agreement (UA). The UA is an agreement between the operational and acquisition communities to gain commitment to continuous user involvement and assign decision-making authority in the development and delivery of software capability releases, ensuring proper resourcing of operational user involvement. UA guidance is also in AF/A5/7 Capability Development Guidebook Volume 2I.

SECTION 2. AF PROCEDURES FOR JCIDS DOCUMENT DEVELOPMENT

2.1. General Guidance.

2.1.1. Format and Content. The format and content guidelines for JCIDS Documents described in paragraphs 1.2.1 through 1.2.3 above are in the JCIDS Manual; checklists are in this Guidebook's appendixes. Format and content for all documents defined in sections 1.2.4. are described in their respective Guidebooks.

JCIDS documents designated by the Joint Staff Gatekeeper as JCB Interest or JROC Interest, must strictly comply with JCIDS Manual format and content specifications. For JCIDS documents designated as Joint Information, Sponsors should comply with the JCIDS guidance to the maximum extent practical. Sponsors should ensure the documents capture the appropriate information at the necessary level of detail to support decision making and stakeholder coordination. Refer to Section 3 of this Guidebook for more detail.

To maintain consistency, all JCIDS documents, regardless of staffing designator, are drafted based on guidance and the formats in this manual and are provided to the Joint Staff Gatekeeper for initial screening and review before submission for staffing.

Sponsors should work through AF/A5DR to initiate a dialogue with Joint Staff Gatekeeper early in the document development process regarding proposed Joint Staffing Designator (JSD) and potential JPRs or Joint KPPs. This will ensure the staffing and approval process goes as smoothly and quickly as possible.

Sponsors are encouraged to work through the HAF functional, AF/A2 (Threat and Intelligence), AF/A3T (Operational Training Infrastructure), AF/A6 (Net Ready attribute), SAF/IEN (Energy KPP), etc., and the AF/A5D Subject Matter Expert (SME) and AF/A5DR FCB representatives to engage the JCIDS process stakeholders prior to formal staffing to ensure documents are developed in a way that does not require significant rework during staffing. This is particularly important when a Sponsor intends to request a waiver or exemption for any certifications or endorsements. Depending on the nature of the requirement(s), Sponsors may need to secure additional joint certifications or endorsements during the staffing process. Refer to the JCIDS Manual for additional guidance on the joint certification/endorsement process.

Sponsors should engage with the AF/A5DR team to discuss current JCIDS requirements for mandatory performance attributes and special interest items. Waivers for mandatory document content are best worked prior to writing the document.

2.1.2. Special Interest Items.

2.1.2.1. Responsible Artificial Intelligence (RAI) is a DepSecDef special interest item. Sponsors will consider Artificial Intelligence (AI) Ethical Principles in all acquisition pathways as soon as an AI-enabled capability has been identified as a potential solution and include the five RAI principles when a solution approach includes AI-enabled capabilities. See Appendix 3 for definitions of the five AI Ethical Principles, recommendations on how to document RAI efforts early in the development process, and a list of additional items for consideration. Contact AF/A5DQ, the AI Capability Development Team, for the most current guidance.

A May 2021 DepSecDef memorandum established the DoD's holistic, integrated, and disciplined approach to RAI and directed DoD Agencies and Components to, "Incorporate RAI into all applicable AI requirements … to ensure RAI inclusion in appropriate DoD AI capabilities." The memo introduced five DoD AI Ethical Principles: Responsible, Equitable, Traceable, Reliable, and Governable. These five Ethical Principles apply to all DoD AI capabilities at any scale, used in warfighting and business applications, to include AI-enabled

autonomous systems. In the absence of explicit policy guidance and digital tools, sponsors should document any efforts to comply with the RAI tenets and each of the DoD RAI Ethical Principles.

AI-enabled capabilities continue to mature and offer unique solutions to capability gaps that have previously been unattainable. The AF must integrate these offerings responsibly. Implementation of RAI guards against AI-enabled capabilities that may be applied unethically or irresponsibly.

2.1.2.2. Energy supportability and demand reduction is a DepSecDef special interest item. Sponsors will consider energy supportability and demand reduction in all acquisition pathways as soon as an energy enabled capability has been identified as a potential solution.

The Energy KPP statutorily required, but investigation has determined that implementation has been inconsistent. The Apr 2022 DepSecDef memo directed energy supportability and demand reduction assessments for all JCIDS capability development activities. Annex E to Appendix G to Enclosure B of the JCIDS Manual contains detailed guidance on conducting the assessment and developing the Energy KPP.

2.1.3. Training. In accordance with JCIDS guidance, any document subject to JCIDS oversight requires the document writing team (DWT) lead, and the acquisition representative to be Requirements Management Certification Training (RMCT) Level B certified. All other team members must minimally complete RMCT Level A and are highly encouraged to be RMCT Level B certified. See AF/A5/7 Capability Development Guidebook, Volume 2A for details on RCMT.

2.1.4. Approval to Develop Requirements. HAF-level review and AF/A5D approval of the Solution Pathway Review (SPR) Worksheet is required for development of any AF-sponsored JCIDS document. Early and frequent collaboration with the AF/A5DR Team is advised.

2.1.5. Validation. The validation of a requirements document does not expire unless specifically withdrawn by the validation authority or the document sponsor, and if the strategic guidance, operational plans, Service and Joint concepts, Concept of Operations (CONOPS), and other guidance justifying the validation of the original capability requirement document are still valid. Significant changes to the strategic guidance, threats, or available funding may require reassessment, update, and revalidation of previously validated capability requirement documents by an appropriate validation authority.

2.1.6. Updates to Validated Documents. Capability requirements are not expected to be static during the product life cycle. As knowledge and circumstances change, consideration of adjustments or changes may be requested by acquisition, budgeting, or requirements officials. Any requested changes relating directly to the substance of the document such as performance attributes, cost, schedule, or quantity, render the document invalid for the purpose of follow-on processes until the requirements document is updated, reviewed, and revalidated by the appropriate JCIDS validation authority.

For sustainment of previously fielded capability solutions, a new document is not required to retain or restore capabilities or perform technology refresh of fielded systems that have a validated requirements document. 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. However, if the MDA or other decision maker requires capability document(s) “revalidation” prior to supporting additional production or technology refresh, the legacy documents shall be transcribed into current document formats and content prior to submitting for review and validation.

For any proposed JCIDS document change/update, the Sponsor, working through their MAJCOM/Agency requirements policy and process office contacts AF/A5DR to determine the appropriate level of AF and Joint review and approval. Proposed changes are accompanied by a funding strategy and schedule that

have been coordinated with the appropriate program office, Program Manager, and Program Executive Officer.

Formal AF decisions regarding document change/update or revalidation are documented in an official memorandum. AF/A5DR posts the updated document and memorandum to IRSS and provides a copy of the decision memo and updated document to the Joint Staff Gatekeeper for archiving.

2.1.7. Exceptions. The USAF organizations that have been granted specific authority to determine requirements for their assigned area are listed in the AF/A5/7 Capability Development Guidebook, Vol 2A, Overview and Governance. These organizations should have their own processes and forms of documentation. Organizations choosing to use the documents specified in the AF/A5/7 Guidebooks must follow the AF/A5/7 process for document development and approval. Organizations without specific authorization to independently develop requirements may not develop or approve/validate any of the documents described in the AF/A5/7 Guidebooks.

In some cases, expedited document development, and/or rapid/tailored staffing is necessary. Desired exceptions should be discussed and approved at the SPR. For exceptions after the SPR, contact AF/A5DR for guidance.

2.2. Initiation of the JCIDS Pathway. Capability Development initiatives can be either "top-down" directed by HAF-level or higher, or "bottom up" initiated by a MAJCOM or Agency Sponsor. Strategies to fill gaps identified due to changes to the NDS, Joint Warfighting Concepts, Air Force Concepts, Wargames, or direction from Senior Leader forums are documented in CDPs and informed by a CBA or similar studies. These processes are covered in Volumes 2B and 2C of the AF/A5/7 Capability Development Guidebook, respectively. Additionally, capability requirements and capability gaps identified in a JROC directed Capability Portfolio Management Review (CPMR), given sufficient rigor and details, may satisfy as a CBA for entry into the capability development process. Details of the content and conduct of the CPMR are in the JCIDS Manual. Contact AF/A5DR for CPMR guidance.

The resulting analysis, plans, and roadmaps are presented to AF/A5D at the CDP review. If the AF/A5D approves a CDP for solution development, the MAJCOM/Agency Sponsor will request an AF/A5D chaired SPR. The SPR chair will approve development of the appropriate JCIDS document. See AF/A5/7 Capability Development Guidebook, Volume 2A for details on the SPR.

2.3. JCIDS Document Processes. The staffing and validation processes are generally identical for all documents. The common processes for Initial Staffing, electronic AFROC (eAFROC), and Validation processes are detailed in Section 3. Differences will be noted in the individual document sections.

2.3.1. DCR Process. Figure 2.1 and the following text describes the deliberate AF DCR and Joint DCR processes. The content and processes are identical except a Joint DCR will complete Joint Staffing and validation.

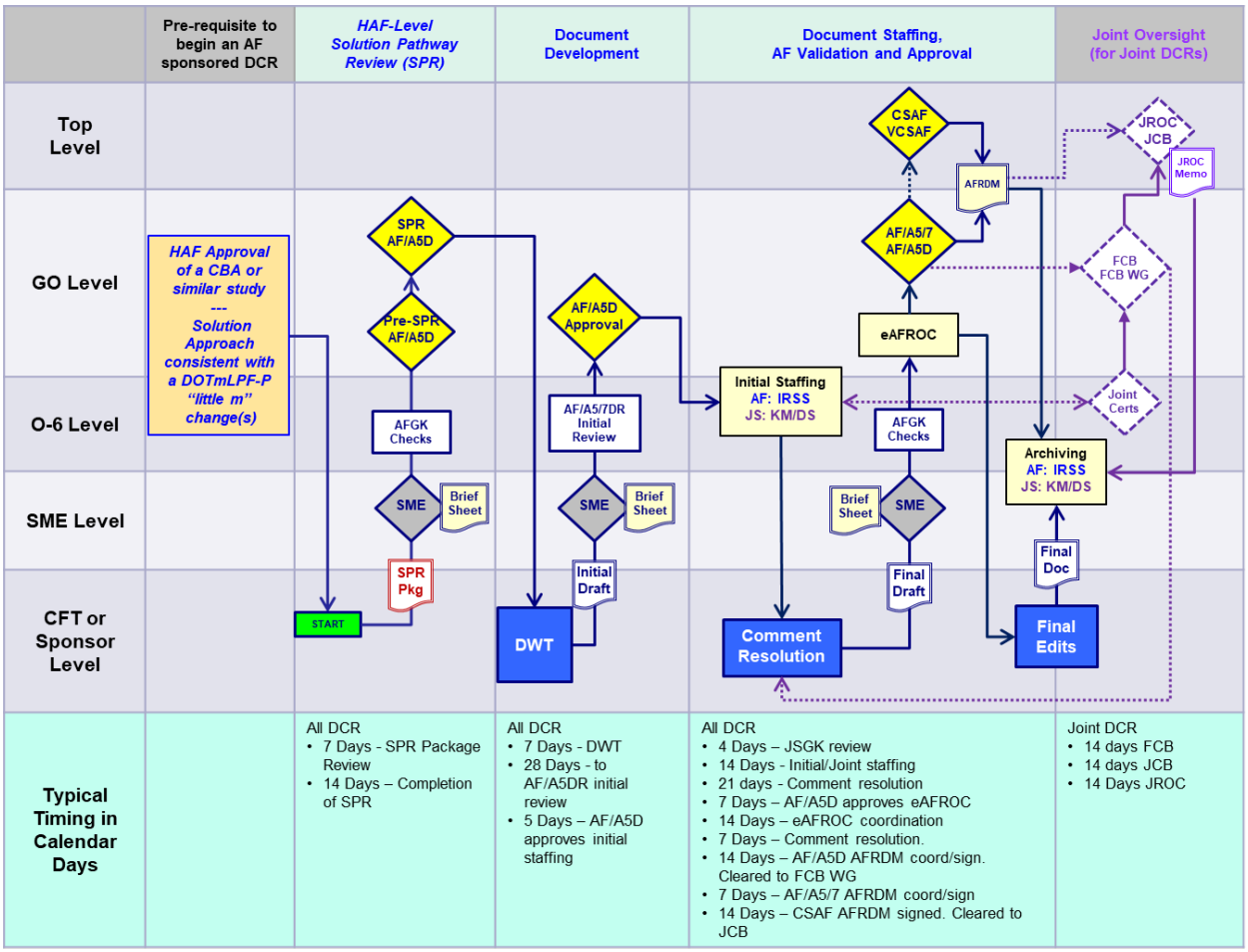

Figure 2.1 DCR Process

Entry Criteria. Results from a CBA or similar study, DOTmLPF-P analysis, or assessment are used to identify the change recommendations. The analysis provides the background and rationale to justify gap mitigation using a DOTmLPF-P approach. Analysis other than an approved CBA will be approved at the SPR. There is risk in deriving valid requirements from non-AF documents and analysis sponsored by other agencies. The context, mission needs, gaps, risk, and potential solution approach may not be relevant to the USAF. Although the mission may be similar, the gaps may require a different solution pathway.

The DCR pathway requires close collaboration with stakeholders and functional process owners (FPO) to ensure the solution approach will address the required capabilities. Sponsors must establish dialog with key stakeholders to fully develop the solution approach and DWT membership. The AF FPOs are identified in Table 2.1 below. If the DCR will be Joint, include the Joint stakeholders in all aspects of the process. The list of Joint FPOs is in the JCIDS Manual, Annex F to Appendix G to Enclosure B.

DOTmLPF-P Area	AF Functional Process Owners
AF Doctrine	Air University
AF Organizations	Air Staff – A1
AF Training	HQ AETC and Air Staff - A3T
AF Materiel	SAF/AQ and AFMC
AF Leadership & Education	HQ AETC / Air University
AF Personnel	Air Staff – A1
AF Facilities	Air Staff – A4
AF Policy	Various POCs – Topic Specific

Table 2.1. AF Functional Process Owners

Solution Pathway Review. The SPR will ensure the Sponsor is on the correct pathway for development of the right document at the right time, with the right people involved. Refer to AF/A5/7 Capability Development Guidebook, Vol 2A for details on SPR conduct and expectations.

Sponsors, in collaboration with the AF/A5D SME, will complete a SPR Worksheet, a Plan of Action and Milestones (POA&M) that reflects the anticipated approval and validation date of the document, and any additional supporting material. The Sponsor's IRSS Point of Contact (POC) will create a Document Record in IRSS, change the Status to "Solution Pathway Review", and send AF/A5DR a "Solution Pathway Review Request" task, followed by an email notification from their Requirements Policy Shop's O-6 to the Air Force Gatekeeper (AFGK). The email can be sent via NIPRNET or SIPRNET and must include the completed SPR Worksheet and POA&M.

The SPR package must address:

- Ensure entry criteria are met as described above.
- Proposed nomenclature. The DCR title should reflect the mission/functional area.
- Specific gaps which are to be mitigated in the DCR.
- Timeframe when the recommendations need to be implemented.
- Potential interdependencies with other AF or joint systems/solutions or other enablers.
- Where applicable, cost estimates and funding sources to ensure the solutions remains affordable with respect to available funding.
- Proposed DWT members, location, dates, and format (live or virtual), including any issues/concerns with support, funding, security, etc. TBDs are not permitted.
- RMCT status and experience of Team Leaders and Acquisition POC(s).
- Proposed POA&M with a timeline for completion of the DCR.
- Any requested waivers to mandatory JCIDS Manual content.
- Expected staffing-ready document submission date.
- When required, projected follow-on requirements oversight/reviews, and interaction with stakeholders from the Joint Staff, other Services and OSD.

- Proposed AF Validation Authority and proposed JSD when applicable.

Any changes to the above after SPR approval to proceed must be submitted to AF/A5DR for approval.

Document Writing Event. An AF/A5D SPR Decision Memorandum documents the approval of the SPR package and directs the sponsor to convene a DWT. The document sponsor will assemble the DWT as planned and write the initial draft of the document. If the SPR directed document delivery date is exceeded by 30 days, the document sponsor must notify the AFGK and request an extension.

Initial Review. See Section 3.2.

Initial Staffing. See Section 3.2.

The eAFROC. See Section 3.2.

DCR Validation. See Section 3.2. Differences are noted below.

In validating a DCR, the validation authority:

- Validates the proposed non developmental materiel capability solution(s) fulfills a gap in USAF or joint military capabilities or is otherwise necessary to meet requirements in the NDS.
- Approves the document and supporting data, including the recommended changes and implementation plans.
- Assigns the Office of Primary Responsibility (OPR) to accomplish each action listed in the implementation plan.
- Verifies all applicable certification and endorsements have been granted.

If Joint validation is required, the sponsor will collaborate with the AF/A5DR Joint Integration Team, the AF/A5D SME, and the Joint Staff to build and present the briefing products to the FCB WG, FCB, JCB and JROC. Normally, no briefing is required for AF validation.

Completion/Exit Criteria. A copy of the final document with the validation page posted in IRSS and submitted to the Joint Staff for archiving in the Knowledge Management & Decision Support (KM/DS) system.

2.3.2. ICD and Variants Process.

2.3.2.1. Deliberate ICD and IS-ICD Process. Figure 2.2 and the following text describes the Deliberate and IS-ICD processes. Although the content and governance are different, the document development and validation process are identical.

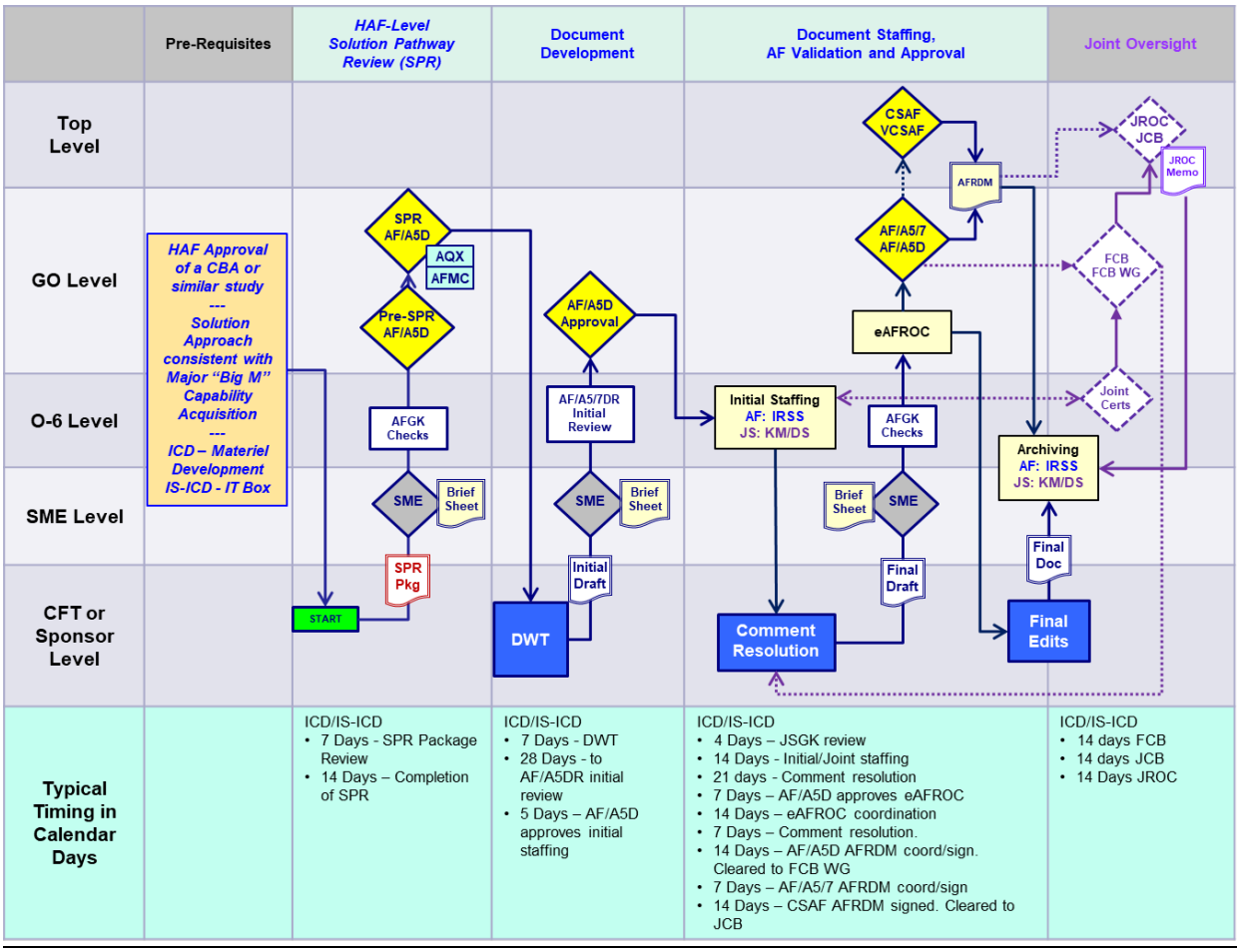

Figure 2.2 Deliberate ICD and IS-ICD Process

Entry Criteria. The results from a CBA or similar study are the basis of the ICD. The CBA/analysis must provide the rationale and analysis to justify gap mitigation via a materiel development approach. Use of analysis other than an approved CBA will be approved at the SPR. There is risk in seeking valid requirements from documents and analysis sponsored by other agencies. The context, mission needs, gaps, risk, and potential solution approach for the other agency may not be relevant to the USAF. Although the mission may be the same or similar, the gaps or needs may necessitate a different solution pathway.

The solution pathway selection requires extensive and close collaboration with key stakeholders and other process owners to ensure the requirements document strategy is consistent with the solution approach. Sponsors are expected to establish effective dialog with key stakeholders to fully develop the solution approach and DWT membership.

Solution Pathway Review. The SPR will ensure the Sponsor is on the correct pathway for development of the right document at the right time, with the right people involved. Refer to AF/A5/7 Capability Development Guidebook, Vol 2A for details on SPR conduct and expectations.

Sponsors, in collaboration with the AF/A5D SME, will complete a SPR Worksheet, a POA&M that reflects the anticipated approval and validation date of the document, and any additional supporting material. The Sponsor's IRSS POC will create a Document Record in IRSS, change the Status to "Solution Pathway Review", and send AF/A5DR a "Solution Pathway Review Request" task, followed by an email notification

from their Requirements Policy Shop's O-6 to the AFGK. The email can be sent via NIPRNET or SIPRNET and must include the completed SPR Worksheet and POA&M.

The SPR package must address:

- Justification for use of an ICD rather than an alternative agile/rapid process such as MTA, Section 800 Software Pathway, AF Form 1067 Modification Proposal, etc.
- Ensure entry criteria are met as described above.
- Proposed nomenclature that reflects the proposed type of approach associated with the core mission or gap area being addressed. For example:
    - *TAC-P Modernization*, describes an ICD recommending a modernization approach.
    - *Tanker Recapitalization*, describes an ICD recommending a recapitalization approach.
    - *"Next Gen…,"* describes an ICD recommending a transformational approach.
- Timeframe when the capability needs to be delivered; Initial Operational Capability (IOC)/Full Operational Capability (FOC).
- Potential interdependencies with other AF or joint systems/solutions or other enablers.
- Proposed DWT members, location, dates, and format (live or virtual), including any issues/concerns with support, funding, security, etc. TBDs are not permitted.
- RMCT status and experience of Team Leaders and Acquisition POC(s).
- Proposed POA&M with a timeline for completion of the ICD.
- Any requested waivers to mandatory JCIDS Manual content to include mandatory performance attributes and special interest items.
- Consider the impact of mandatory performance attributes and special interest items on quantitative parameters and metrics.
- Expected date when the Sponsor expects to submit the document for initial staffing.
- When required, projected follow-on requirements oversight/reviews, and interaction with stakeholders from the Joint Staff, other Services and OSD.
- Proposed AF Validation Authority, proposed JPRs when applicable, and proposed JSD when applicable.

Any changes to the above after SPR approval to proceed must be submitted to AF/A5DR for approval.

Document Writing Event. An AF/A5D SPR Decision Memorandum documents the approval of the SPR package and directs the sponsor to convene a DWT. The document sponsor will assemble the DWT as planned and write the initial draft of the document. If the SPR directed document delivery date is exceeded by 30 days, the document sponsor must notify the AFGK and request an extension.

Initial Review. See Section 3.

Initial Staffing. See Section 3.

The eAFROC. See Section 3.

Validation.

In validating an ICD, the validation authority:

- Validates the capability requirements as being necessary to fulfill joint military capabilities in support of the NDS and approves prioritization of associated capability gaps.
- Approves the document and supporting data, including the recommended approach(es) to address the validated capability requirements and eliminate or mitigate the capability gaps.
- Includes, where applicable, recommendations for development of the AoA guidance.
- Verifies all applicable certification, endorsements, and waivers have been granted.

AF validation also approves release of the document to the Joint Staff to begin joint validation if required. To expedite the validation process, AF documents may be submitted to the Joint Staff for validation review by the responsible FCB Working Group or FCB following eAFROC and AF/A5D approval. Formal decisions are documented in writing via an Air Force Requirements Decision Memorandum (AFRDM).

If Joint validation is required, the sponsor will collaborate with the AF/A5DR Joint Integration Team, the AF/A5/7 SME, and the Joint Staff to build and present the briefing products to the FCB WG, FCB, JCB and JROC. Normally, no briefing is required for AF validation.

Completion. A copy of the final document with the validation page posted in IRSS and submitted to the Joint Staff for archiving in KM/DS.

2.3.2.2. SW-ICD. Figure 2.3 and the following text describes the SW-ICD process. The SW-ICD is intended to allow rapid software development so the document development and validation processes are accelerated. The AF employs Rapid Staffing, detailed below.

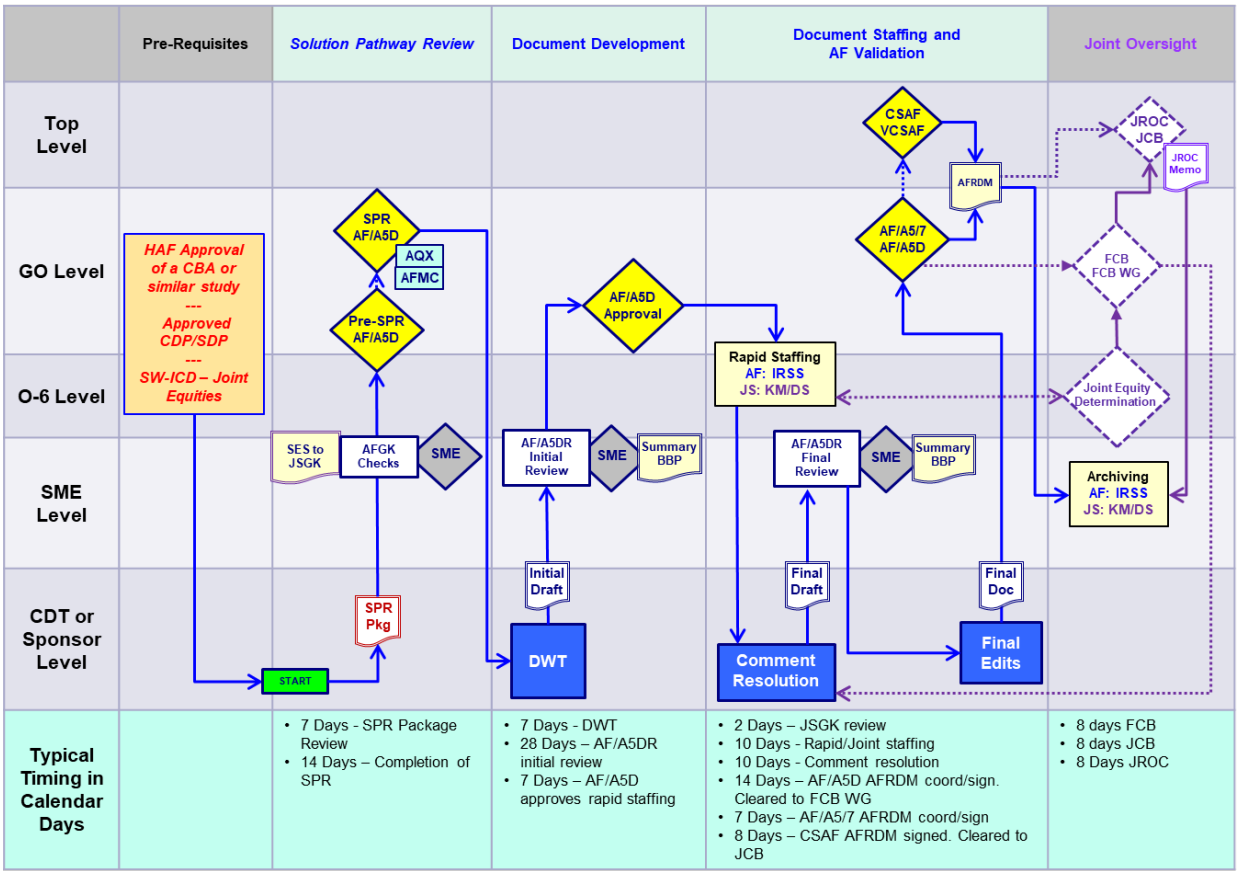

Figure 2.3. The Software-ICD Process

Entry Criteria. Identical to Deliberate ICD.

Solution Pathway Review. Identical to Deliberate ICD except the SPR notification must be sent not later than 10 days prior to the start of the proposed document writing event.

Prior to the SPR, the sponsor will develop the SES and the IRSS POC will load it into IRSS. AF/A5DR will forward the SES to the JSGK and the AFGK for a preliminary review of joint equities. The final determination of Joint equities and the need for Joint staffing will be made when the JSGK reviews the final SW-ICD.

The SPR package must address:

- Justification for use of a SW-ICD rather than an alternative agile/rapid process such as Middle Tier of Acquisition, AF Form 1067 Modification Proposal, etc.
- Ensure entry criteria are met as described above.
- Proposed nomenclature that reflects the proposed type of approach associated with the core mission or gap area being addressed. For example:
    - *TAC-P Software Modernization* describes a SW-ICD recommending a modernization approach.
    - *Tanker Recapitalization Software* describes a SW-ICD recommending a Software-only solution as part of a larger recapitalization approach.
- Potential interdependencies with other AF or joint systems/solutions or other enablers.
- Proposed DWT members, location, and dates, including any issues/concerns with support, funding, security, etc. TBDs are not permitted.
- Training status and experience of Team Leadership and Acquisition POC(s).
- Proposed POAM with a timeline for completion of the CNS and the UA.
- Proposed first software release date and follow-on releases.
- Any requested waivers to mandatory document content.
- When required, projected follow-on requirements oversight/reviews, and interaction with stakeholders from the Joint Staff, other Services and Office of the Secretary of Defense organizations.
- Proposed AF Requirements DA and proposed Acquisition DA.
- The SES with AF and JS Gatekeeper preliminary coordination. A preliminary Joint Staff assessment of no Joint Equities may not require a SW-ICD.

Any changes to the above after SPR approval to proceed must be submitted to AF/A5DR for approval.

Document Writing Event. Identical to Deliberate ICD.

Initial Review. See Section 3.

Rapid Staffing. Unlike traditional staffing, rapid staffing allows comments in addition to final certifications, endorsements, and attestations. The AF/A5DR Team will forward the document, regardless of potential Acquisition Category or proposed requirements validation authority, to the JSGK for review and joint equities assessment. If joint equities exist, the JSGK will assign a Joint Staffing Designator and staff the SW-ICD through the Joint Staff.

IRSS POCs for each tasked organization should forward the document to appropriate individuals in their organization for review. AFROC principal endorsement certifies that the Stakeholders agree that required certifications, endorsements, attestations, or waivers have been obtained prior to validation.

Validation. Identical to a Deliberate ICD.

Completion. Identical to a Deliberate ICD.

2.3.3. CDD and Variants Process. Although the content varies between the CDD variants, the process for each is identical for the most part. Differences will be noted in the text. Figure 2.4, the general guidelines in Section 3.2, and the following text describes the process.

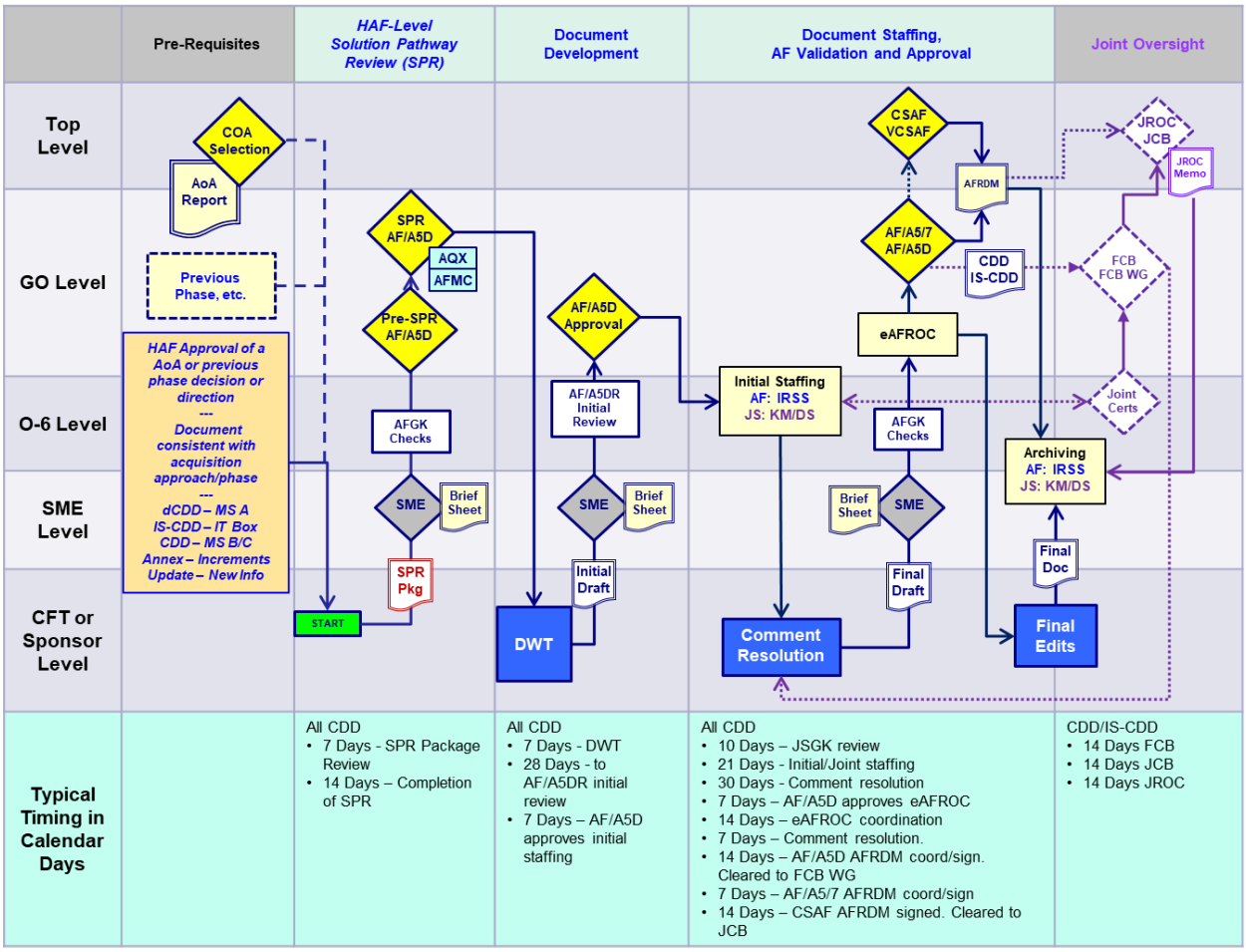

Figure 2.4 The CDD Process

2.3.3.1. Capability Development Document.

Entry Criteria. There are several possible entry points for a CDD.

- An approved AoA Final Report with a signed Capability Guidance Decision Memorandum directing the way forward.
    - In cases where a Sponsor proposes to use a Non-AF ICD, a Non-AF AoA, or other alternative analysis, the documents must be reviewed and approved for use by AFGK prior to submitting the CDD SPR package.
- A previously validated dCDD.

- The acquisition MDA may direct transition from an alternate acquisition pathway such as MTA or a UON. With AF/A5D coordination, the MDA may accept non-JCIDS documentation as the requirements basis for the CDD.

Solution Pathway Review. The SPR will ensure the Sponsor is on the correct pathway for development of the right document at the right time, with the right people involved. Refer to AF/A5/7 Capability Development Guidebook, Vol 2A for details on SPR conduct and expectations.

Sponsors, in collaboration with the AF/A5D SME, will complete a SPR Worksheet, a POA&M that reflects the anticipated approval and validation date of the document, and any additional supporting material. The Sponsor's IRSS POC will create a Document Record in IRSS, change the Status to "Solution Pathway Review", and send AF/A5DR a "Solution Pathway Review Request" task, followed by an email notification from their Requirements Policy Shop's O-6 to the AFGK. The email can be sent via NIPRNET or SIPRNET and must include the completed SPR Worksheet and POA&M.

The SPR package must address:

- Justification for use of a CDD rather than a CDD variant or an alternative process such as MTA, Section 800 Software Pathway, AF Form 1067 Modification Proposal, etc.
- Ensure entry criteria are met as described above.
- Proposed CDD title that reflects the system or solution. For example:
    - *B-2 EHF SATCOM and Computer Upgrade CDD,* for a modernization program.
    - *T-X CDD, KC-X CDD,* for a recapitalization or replacement program.
    - *JATM CDD Update,* for an update to capabilities and acquisition strategy.
- Results of the AoA, or similar study, and the preferred solution concept.
- The scope for the proposed strategy/solution (e.g., single increment, multiple increments), and which gaps are to be mitigated in the CDD/increment.
- Potential interdependencies with other AF or joint systems/solutions or other enablers.
- Current/projected Technology Readiness and Manufacturing Readiness levels.
- Projected IOC and FOC, and how the capability will be sustained.
- Intelligence supportability requirements and CIPs.
- RAI considerations for AI enabled capabilities.
- Proposed DWT members, location, dates, and format (live or virtual), including any issues/concerns with support, funding, security, etc. TBDs are not permitted. Sponsors are expected to establish effective dialog with key stakeholders to fully develop the requirements document strategy and DWT membership. Ideally, the CDD Team evolves from the ICD Team and the AoA Study Team membership.
    - DWT should include organizations responsible for feasibility and testability attestations and AF certifications and endorsements.
    - It is advisable to contact outside organizations such as OSD, the Functional Capability Boards, or the Defense Intelligence Enterprise (DIE) for guidance in obtaining the certifications and endorsements required for JROC or JCB Interest documents.
- RMCT status and experience of Team Leaders and Acquisition POC(s).

- Proposed POA&M for completion of the document.
- Expected date when the Sponsor expects to submit the document for initial staffing.
- Any requested waivers to mandatory JCIDS Manual content to include mandatory performance attributes and special interest items.
- Consider the impact of mandatory performance attributes and special interest items on quantitative parameters and metrics.
- Projected follow-on requirements oversight/reviews and interaction with stakeholders from the Joint Staff, other Services and OSD.
- Proposed AF Validation Authority, proposed JPRs when applicable, and proposed JSD when applicable.
- The sponsor must show evidence that acquisition activities such as technology development and preliminary design are sufficient to enable the DWT to accurately develop requirements attributes.

Any changes to the above after SPR approval to proceed must be submitted to AF/A5DR for approval.

Document Writing Event. An AF/A5D SPR Decision Memorandum documents the approval of the SPR package and directs the sponsor to convene a DWT. The document sponsor will assemble the DWT as planned and write the initial draft of the document. If the SPR directed document delivery date is exceeded by 30 days, the document sponsor must notify the AFGK and request an extension.

Initial Review. See Section 3.1.

Initial Staffing. See Section 3.2. At this point the sponsor should remind AFMC and the Lead Operational Test Organization DWT members that feasibility and testability attestations will be due with eAFROC endorsement. The sponsor should also remind AF Certification/Endorsement Organization DWT members that their certifications/endorsements will be due with their eAFROC endorsement.

eAFROC. See Section 3.2.

USAF has the authority to certify or endorse all performance attributes that are not designated and approved as JPRs regardless of JSD assignment. This includes the threat assessment/intelligence certification and DOTmLPF-P endorsement for JCIDS documents assigned a JSD of Joint Information.

AF Organizations responsible for certifications and endorsements review JCIDS documents and provide comments if changes to the document are required prior to providing the certification or endorsement. AF certifications and endorsements, or waivers, may be submitted via memorandum to the AFGK, or submitted as a comment during eAFROC Review. USAF Attestations, Certifications, and Endorsements are listed below.

- Testability Attestation. The Sponsor ensures that the Lead Operational Test Organization provides evidence, via official memorandum to AF/A5D, that the capability requirements and proposed system level performance attributes have been reviewed and determined to be testable and measurable.
- Feasibility Attestation. The Sponsor works with the appropriate acquisition program representative to provide written evidence indicating the capability requirements and proposed system level performance attributes have been reviewed by the acquisition community and determined to be technically achievable and executable within the estimated schedule and cost.

- Feasibility presents the viewpoint of the Program Manager who will execute the program. Dissenting viewpoints of the Program Manager or Program Executive Officer must be included and explained. Any adverse comments regarding feasibility must be adjudicated prior to submitting the document for final validation.
- After the feasibility review, any changes or revisions to the substance of the final document such as changes approved during eAFROC, or JCB/JROC review that alter the substance of the system attributes, cost, schedule, or quantity require an updated feasibility review prior to final validation.

The eAFROC concludes with AF/A5D approval to:

- Forward the package to the designated AF RDA for AF approval or validation staffing.
- Forward the document to the FCB to begin joint validation, if required.

To expedite the validation process, FCB review may be concurrent with AF validation staffing to the AF RDA. AF documents may be submitted to the Joint Staff for review by the FCB Working Group(s) and FCB immediately following the eAFROC and AF/A5D approval.

Validation. See Section 3.2.

In validating a CDD or variant, the validation authority:

- Validates the proposed capability solution fulfills a gap in joint military capabilities or is otherwise necessary to meet applicable requirements in the NDS.
- Approves the document and supporting data, including the performance attributes and when applicable, the JROC approves the designated performance attributes to JPRs.
- Assesses the risks in meeting those performance attributes in terms of lifecycle cost, schedule, and technological maturity.
- Assesses the affordability of the capability solution being delivered to mitigate the established and approved capability gap(s). Other alternatives to the proposed solution may be considered.
- Approves the IOC and FOC schedules and procurement quantities.
- Verifies all applicable certification, endorsements, and waivers have been granted.

AF validation also approves release of the document to the Joint Staff to begin joint validation if required. To expedite the validation process, AF documents may be submitted to the Joint Staff for validation review by the responsible FCB Working Group or FCB immediately following the eAFROC and AF/A5D approval. Formal decisions are documented in writing via an AFRDM. Normally, no briefing is required for AF validation.

Sponsors will work with the AF/A5DR Joint Integration Team and the Joint Staff to build and present the briefing products to the FCB WG, FCB, JCB and JROC as required.

Completion. A copy of the final document with the validation page posted in IRSS and submitted to the Joint Staff for archiving in KM/DS.

2.3.3.2. draft Capability Development Document.

The dCDD outlines the minimum essential information for technology maturation and preliminary design for development of a materiel solution, or capability increment. A validated dCDD is an entrance criterion for development of the RFP for the TMRR phase of acquisition and for the Milestone A acquisition decision. This is not to be confused with a draft version of a complete CDD.

A dCDD Annex may be developed for an incremental program as a precursor to a CDD Annex to a previously validated CDD. This strategy might be appropriate to support a Milestone A decision for entry into the TMRR phase of activity for a follow-on increment, block upgrade, or other subsequent development/production based on a previously validated CDD.

Entry Criteria. Identical to CDD in 2.3.3.1.

Solution Pathway Review. The SPR process is identical to the CDD process in 2.3.3.1, but the content is different. The SPR package must address:

- Justification for use of a dCDD rather than an alternative process such as MTA, Section 800 Software Pathway, AF Form 1067 Modification Proposal, etc.
- Ensure entry criteria (pre-requisites) are met as described for a CDD in 2.3.1.
- Proposed title of a dCDD should reflect the system/solution approach.
- Results of the AoA or similar study and the preferred solution concepts and alternative(s).
- Specific gaps which are to be addressed in the dCDD.
- Status of technology readiness for identified critical technology elements.
- Potential interdependencies with other AF or joint systems/solutions or other enablers.
- Intelligence supportability requirements and CIPs.
- RAI considerations for AI enabled capabilities.
- Affordability and schedule goals for the technology maturation phase of acquisition.
- Proposed DWT members, location, dates, and format (live or virtual), including any issues/concerns with support, funding, security, etc. TBDs are not permitted. Sponsors are expected to establish effective dialog with key stakeholders to fully develop the requirements document strategy and DWT membership. Ideally, the CDD Team evolves from the ICD Team and the AoA Study Team membership.
- RMCT status and experience of Team Leaders and Acquisition POC(s).
- POA&M for the document.
- Expected date when the Sponsor expects to submit the document for initial staffing.
- Projected follow-on requirements oversight/reviews and interaction with stakeholders from the Joint Staff, other Services and OSD.
- Proposed AF Validation Authority, proposed JPRs when applicable, and proposed JSD when applicable.

Any changes to the above after SPR approval to proceed must be submitted to AF/A5DR for approval.

Document Writing Event. Identical to CDD in 2.3.3.1.

Initial Staffing. Document review and staffing is identical to the CDD in 2.3.3.1. with the following exceptions:

- The document does not go to the Joint Staff for review.
- The feasibility and testability attestations, and certifications are not required. However, the responsible organizations should begin work on those items in preparation for the full CDD.

The eAFROC. eAFROC and validation staffing is identical to the CDD in 2.3.3.1. with the following exceptions:

- The document does not go to the Joint Staff for review.
- The feasibility and testability attestations, and certifications are not required.

eAFROC review concludes with package presentation to AF/A5D for validation if so delegated or approval to forward the package to the appropriate RDA for AF validation.

Validation. In validating a dCDD, the validation authority:

- Validates the proposed capability solution fulfills a gap in joint military capabilities or is otherwise necessary to meet applicable requirements in the NDS.
- Approves the document and supporting data, including the performance attributes.
- Assesses the risks in meeting those performance attributes in terms of lifecycle cost, schedule, and technological maturity.
- Assesses the affordability of the capability solution being delivered to mitigate the established and approved capability gap(s).

Completion. A copy of the final document with the validation page is posted in IRSS.

2.3.3.3. CDD Update. There are several circumstances where a CDD Update is required. Two of the most common scenarios are below:

- Program Changes and Trades, “Tripwire”, etc. A CDD update/revalidation is required if a change to KPP(s) is necessary after validation, the program experiences a 10% or greater growth over their current baseline or 25% over their original baseline as defined in the Acquisition Program Baseline (APB), a 10% or greater reduction in operational inventory quantities from the previously stated CDD procurement numbers, or a 12-month or greater schedule slip of IOC or FOC from the previously stated CDD schedule (IOC or FOC) date.
- Program Updates for Milestone C, Production Phase. A previously validated CDD or an updated and revalidated CDD is an entrance criterion necessary for the RFP release in support of the production phase of acquisition and the Milestone C decision. If changes to a previously validated CDD are necessary to support the Milestone C decision and entry into the production phase, an updated CDD may be developed and staffed to obtain re-validation of refined requirements and system level attributes (KPPs, KSAs, APAs and other attributes).

Entry Criteria. A previously validated CDD is the basis for the update. The analysis leading to the update must be available and presented with the SPR package. Proposed changes to KPPs, KSAs, APAs and/or other attributes must be accompanied by a funding strategy and schedule that have been coordinated with the appropriate program office.

Solution Pathway Review. Identical to CDD in section 2.3.3.1. In most cases, only the changed sections of the document require an update. The SPR will advise if a partial or full document update is required.

Document Writing Event. Identical to CDD in section 2.3.3.1. An update to the feasibility and testability attestations, and certifications may be required. The OPRs for the attestations and certifications will provide an updated attestation or memorandum stating the existing attestation is satisfactory.

Initial Review. See Section 3.1.

Initial Staffing. See Section 3.2. Only comments to the changes are permitted.

eAFROC. See Section 3.2. Only the changes are endorsed.

Validation. See Section 3.2. Only the changes are validated.

Completion/Exit Criteria. See Section 3.2.

2.3.3.4. CDD Annex. A CDD Annex is used to define capabilities in addition to the capabilities in FoS, SoS, or increments of base CDDs.

- FoS Annexes or Increments provide the Sponsor flexibility to redefine capabilities from a base document. The Annex is not intended to be a document of only changes but is derived from the parent CDD. In some cases, it may also be necessary to update Sections of the base document to ensure traceability and remain consistent with the more current Annex. Each Annex must remain in context with the base CDD and meets the approved military capabilities as specified in an ICD.
- The Incremental Path provides the Sponsor flexibility to define capabilities from a base CDD to address an incremental development approach.

Each individual annex will include the same Sections as a CDD. Sections with no change to the base document must be present but can state "No Change." Individual annexes are not to exceed 20 pages in length.

Entry Criteria. A previously validated CDD is the basis for the annex. The analysis supporting the annex must be available and presented with the SPR package.

Solution Pathway Review. Identical to CDD in section 2.3.3.1. The SPR will ensure the annex is within the scope of the base document.

Document Writing Event. Identical to CDD in section 2.3.3.1. An update to the feasibility and testability attestations may be required. The OPRs for the attestations will provide an updated attestation or memorandum stating the existing attestation is satisfactory.

Initial Staffing. See Section 3.2. The annex is submitted accompanied by the base CDD.

eAFROC. See Section 3.2.

Validation. See Section 3.2. The annex must be validated by the same validation authority as the base CDD.

Completion/Exit Criteria. See Section 3.2.

2.4. Information Systems Variants of JCIDS Documents

This pathway is meant to streamline applicable requirements processes and provide Sponsors the flexibility to manage IS requirements with alternate documents and validation processes if development efforts remain within the approved boundaries of the validated IT Box. However, the Sponsor must still ensure that they are compliant with acquisition policy and processes and Information Support Plan policy and processes. Sponsors should consider the IS-ICD or IS-CDD for IS solutions, software development, and off-the-shelf hardware. For software only solutions, sponsors may use the SW-ICD described in section 2.5, or the software acquisition pathway using a CNS and UA described in Section 1.2.4.6. and detailed in Guidebook Volume 2I.

The IS-ICD and IS-CDD are variants of the regular ICD and CDD implementing the IT Box used to document capability requirements and associated capability gaps where the intended capability solution approach involves research, development, and acquisition of applications system software, and the projected lifecycle costs exceed $15M. The IS variants allowed by the IT Box are narrowly focused on software

development efforts and are not appropriate for hardware development or for capturing overarching capability requirements.

IS variants require revalidation if any new capability requirements must be added beyond the scope of the previously validated document, or if program development and integration or sustainment funding increases by 10% or more than what is identified in the document, per the original validation memo.

2.4.1. The IT Box. The IT Box construct, Figure 2.4, allows for fewer iterations JCIDS documents, such as CDD Updates or Annexes, 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 validation authority. The IT Box uses initial minimum values in place of initial objective values so that the baseline capability, or Minimum Viable Product, is clearly specified, and the delegated oversight body has flexibility to further develop capabilities without revalidation of the baseline JCIDS document.

Successor documents, such as Requirements Definition Packages (RDP) and Capability Drops (CD) must be provided to IRSS and KM/DS for archiving for information purposes and visibility in the capability portfolios.

The details of the operation of the IT Box and RDP and Capability Drop use can be found in the JCIDS Manual.

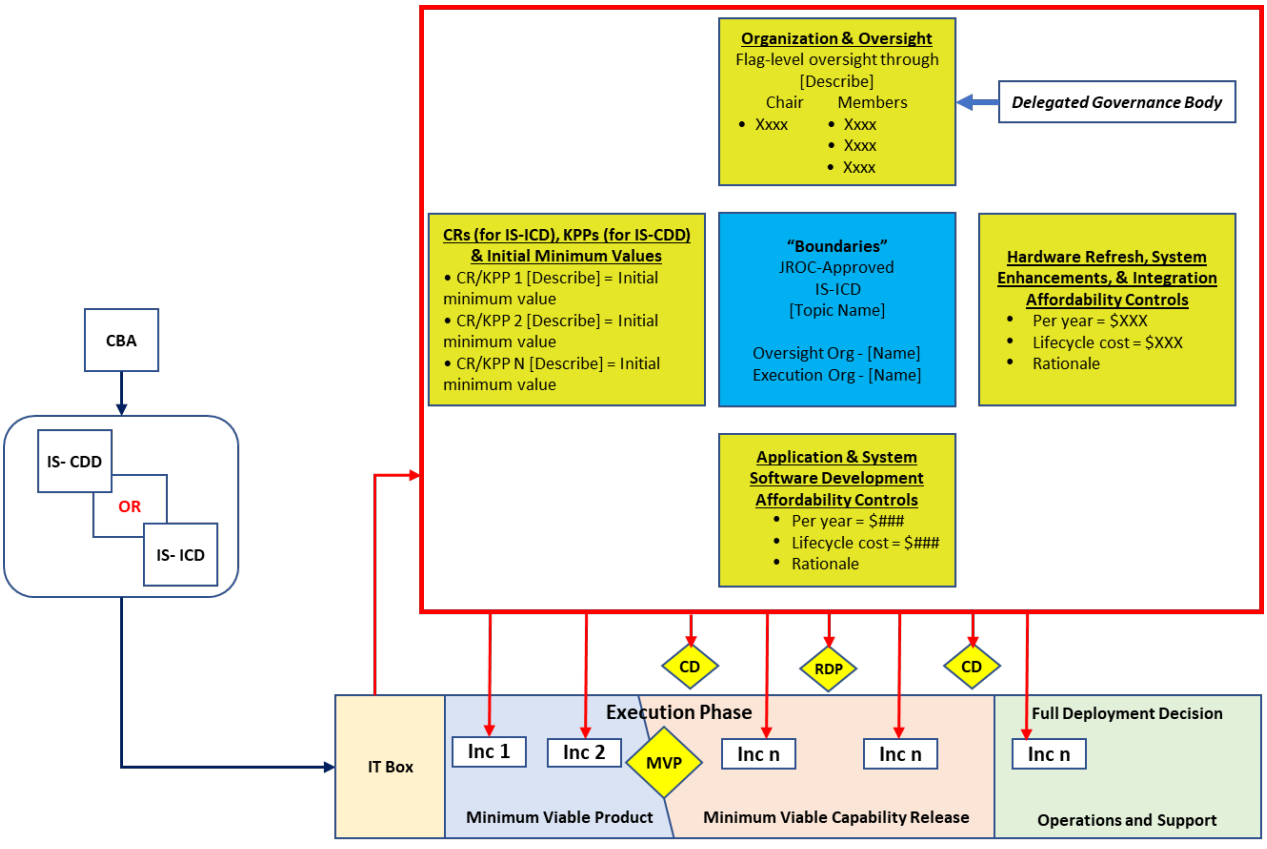

Figure 2.5 The IT Box

2.4.2. IS-ICD. IS-ICDs may be used when:

- It is clear from the CBA that an IS solution is the only viable approach. The AoA, or similar study, though not required, may be conducted after delegating authorities under the IT Box and will therefore only consider IS solutions.
- All hardware associated with the IT Box must be Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS) and hardware modification is restricted to that necessary for system integration and enhancements to meet requirements specified in the IS-ICD or IS-CDD or for hardware refresh due to obsolescence.
- The capability solution involves research, development, and/or acquisition of applications systems software, and the projected lifecycle costs exceed $15 million. IS-ICDs with lifecycle costs less than $15 million may be submitted for review and validation if validated requirements are needed to support budgetary requests or other purposes.

IS-ICDs are not appropriate when:

- Software embedded in a capability solution developed under other validated JCIDS documents.
- Software requiring a host platform, such as a manned or unmanned vehicle, which does not yet have validated JCIDS documents.
- Defense Business Systems are not weapons systems, are not subject to JCIDS, and therefore are not reviewed by AF/A5D.

Sponsors are encouraged to use the IT Box for all programs that meet the criteria. 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.

Entry Criteria. Identical to the ICD process in 2.3.2. The CBA/analysis must provide the rational and analysis to justify gap mitigation using an IS solution.

Solution Pathway Review. Identical to the ICD process in 2.3.2., except IT systems supporting AI enabled capabilities will address RAI considerations.

Document Writing Event. Identical to the ICD process in 2.3.2.

Initial Staffing. See Section 3.

The eAFROC. See Section 3.

Completion. See Section 3.

2.4.3. IS-CDD. IS-CDDs are used in the same circumstances as an IS-ICD except when an IS solution is identified in an AoA as a follow-on to a traditional ICD.

The IS-CDD development, staffing, and validation process is identical to the IS-ICD process in 2.4.2. with the following exceptions.

- The primary entry criteria is an approved AoA or similar analysis rather than a CBA.
- For IT systems supporting AI enabled capabilities, RAI considerations will be addressed.

2.5. Software Variant of JCIDS Documents

The key to agile software development is to form a collaborative cross-functional team focused on the involvement from the customer/end-user of the system. Software development necessitates a unique approach, drastically different from traditional materiel solution development for hardware systems.

While hardware development requires explicit requirements up front to drive the system design and development, software development should not. Agile software development works best with flexible requirements up front, without the rigid specificity and detailed documentation that is typical of the material solution requirements process.

The focus of software development is on solution development; end users over process. An emphasis on early delivery of capability followed by iterative and evolutionary updates for continual improvement to the product based on user needs and continuous feedback that is responsive to user needs, rather than adhering to plans and milestones. The primary metric is delivery of useable solutions, not documentation. The team should encourage the evolution of requirements to avoid obsolescence.

Agile Software Development requires a team of competent, dynamic, and effective participants and stakeholders. The team needs to work as one toward a shared vision. A project plan is useful, but it must not be seen as rigid milestones or limitations – the metric of success is not simply to lay out a plan and follow it. The metric is to produce value for the warfighter. Traditional or linear approaches to program plans cannot replace the need for flexibility and adaptability to get things done, which may include abandoning the previous plan. This type of approach requires close and continuous collaboration and trust relationships between all the team members in both the Planning and Execution Phases.

The Sponsor and the AF/A5/7 SME must engage with the appropriate Acquisition Program Office, SAF/AQX, SAF/FMB, AF/A8P, and AF/A8X to determine the timing and scale of resources required for the Document Writing Team (DWT) and overall software development effort. The Sponsor and the AF/A5/7 SME must also engage with SAF/AQR, SAF/AQX, and other relevant acquisition stakeholders to build consensus on the appropriate software acquisition pathway.

2.5.1. The Software-ICD. JCIDS includes a software pathway to capture requirements for software development using a SW-ICD. The SW-ICD is not to be confused with the Information Systems JCIDS documents. The Information Systems documents are governed by the Information Technology (IT)-Box and include hardware components. The SW-ICD is a separate and distinct process, will not include hardware, and is not governed by the IT-Box.

The SW-ICD facilitates efficient and timely software development efforts by using an expedited process within the JCIDS structure to enable modern software development practices and rapidly deliver mission impactful software. It is not appropriate for hardware development efforts or for capturing capability requirements that span a broad scope of hardware, software, and/or Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P) efforts. SW-ICDs may be used to document embedded software requirements for a capability solution developed under other validated JCIDS documents. In this case, since the software requirements were validated as part of the overall capability solution, the SW-ICD does not require further staffing.

The SW-ICD is the preferred method for software programs that the Joint Staff J8 believes warrant their oversight. Software capability requirements that the Joint Staff determines to have Joint Equities must use the SW-ICD format and validation procedures. Following AF review and validation, AF/A5DR will send the SW-ICD to the Joint Staff Gatekeeper (JSGK) for expedited staffing and validation. Programs that do not have Joint equities may use the Software Acquisition Pathway described in AF/A5/7 Capability Development Guidebook Vol 2I.

Software acquisition from a validated SW-ICD is governed by the overarching acquisition policies and management principles of the Defense Acquisition System as described in DoD Directive 5000.01 and DoD Instruction 5000.02. Acquisition governance is outside the scope of this Guidebook, but requirement sponsors should be familiar with the acquisition system being pursued. The document development process is identical to the ICD detailed in section 2.3.2.

SECTION 3. STAFFING PROCEDURES

This section provides a general description of the document staffing procedures and guidance common to all JCIDS documents. Air Force procedures implement, but do not replace, the over-arching JCIDS process guidance. Document-specific details are in Section 2 of this Guidebook.

3.1. Initial Review

Upon document receipt from the DWT, the Sponsor's IRSS POC will use the Document Review Checklist to ensure the document meets JCIDS criteria for entering initial staffing, check the spelling and grammar, and verify proper classification and portion markings. The document must comply with JCIDS Manual format/content guidance unless waived by the AF or Joint Staff Gatekeeper. An AF-only document may be permitted more flexibility; variances will have been approved during the SPR. The sponsor IRSS POC will then import the draft version of the document and supporting materials, create an Initial Staffing Request task to AF/A5DR, followed by a notification email from their Requirements Policy shop's O-6 to the AFGK. The IRSS POC will then update the Document Record Status to "Initial Staffing – AFGK Review."

Denial of entry into initial staffing is based primarily on the failure to meet the Joint Staff Gatekeeper initial review criteria, as described in the JCIDS Manual. The most common include:

- CBA, Studies, or other supporting data missing or not provided in IRSS and KM/DS.
    - Resolution: IRSS POCs link to the supporting documents via IRSS or upload the supporting files to the document record.
- Predecessor document missing or not provided in IRSS and KM/DS
    - Resolution: IRSS POCs should link to the predecessor documents via IRSS or upload the supporting files to the document record.
- Exceeding the allowable page count – or achieving page count by not using 12 pitch Times New Roman font and 1" margins.
    - Resolution: Reformat and reduce page count.
- Missing or incomplete DoDAF Architecture Views
    - Resolution: The appropriate AF and Joint Staff document reviewers need to be granted access to ALL architecture views.
- Incomplete or unclear representation of capability gaps.
    - Resolution: 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, along with the operational impact or risk.
- Values specified as "TBD" or unquantified descriptions in the definition of operational attributes in the ICD or KPPs/KSAs/APAs in the CDD variants).
    - Resolution: Provide sufficient analysis to support all proposed initial objective values in ICDs and proposed threshold/objective values in CDDs/CDD Annexes.
- Omission of any of the mandatory KPPs without appropriate justification.
    - Resolution: Include mandatory KPPs or justify their omission.

- Incomplete or missing life cycle cost data
    - Resolution: Include lifecycle cost data.
- Unclear or omitted discussion of interdependencies between the proposed capability and enabling capabilities, or other capabilities within SoS approach.
    - Clarify or include interdependency discussion.

Following AFGK initial document review, the Sponsor will update the document as directed and imports a staffing-ready draft version of the document to IRSS to initiate formal staffing. The Sponsor will create an Initial Staffing Request Task to AF/A5DR and send a notification email from their Requirement Policy O-6 to the AFGK.

The AF/A5D will approve initiation of Initial Staffing after review and recommendation by the AF/A5DR team and the AF/A5D SME.

3.2. Formal Staffing

The document process charts in Section 2 show the typical timing for staffing for each document. Timing for each stage may be altered with approval from the AFGK and the JSGK.

Initial Staffing. Initial staffing provides AF and Joint stakeholders the opportunity to review the document and provide O-6-level comments. Critical comments must be approved by a GO/SES.

The AF/A5DR Team will create an Initial Staffing task to organizations on the Air Staff and MAJCOM Distribution Lists in IRSS and update the Document Record Status to “Initial Staffing”. The AF/A5DR Team will forward the document, regardless of potential Acquisition Category (ACAT) or proposed requirements validation authority, to the Joint Staff Gatekeeper for review, JSD assignment, and formal JCIDS staffing if required.

IRSS POCs for each tasked organization should forward the document to individuals within their organization for review and comment. After consolidating all comments, IRSS POCs will verify the Comment Resolution Matrix (CRM) has proper classification and portion markings, upload the CRM into IRSS, and close their IRSS Initial Staffing task. Critical comments must be approved by a GO/SES; the name and rank will be in the remarks section of the CRM.

Document Commenting Phase. AF reviewers submit comments per the IRSS tasking instructions. Comments are identified as critical, substantive, or administrative as described below. Proper justification for critical or substantive comments must be provided in the CRM. For comments to upload properly, they must be submitted using the provided CRM template; no alterations permitted. Critical comments must be signed out at the Senior Executive Service or General Officer level.

- Critical. A critical comment indicates a non-concur position on the document until the comment is satisfactorily resolved. Critical comments should be restricted to critical issues regarding KPPs and KSAs, concepts of operations, violation of policies and directives, and other fundamental issues concerning cost, schedule, or performance that would bring into question the rationale for the document to be approved. Critical comments may also address text or issues which would otherwise be considered Substantive, but if not corrected would prevent the document from serving its intended purpose, lead to the withholding of a mandatory certification or endorsement, or result in disapproval by the validation authority.
- Substantive. A substantive comment indicates a concur, with comment response. A substantive comment addresses minor or moderate changes to correct or clarify minor factual inaccuracies, information that is incorrect, misleading, confusing, or inconsistent with other sections. The scope

and quantity of several substantive comments may also lead to a non-concur response to the staffing until satisfactorily adjudicated.

- Administrative. An administrative comment addresses typographical, formatting, or grammatical errors or changes to writing style to make the document easier to read and understand without substantively changing the content of the document.

At the conclusion of Initial Staffing, AF/A5DR closes the Initial Staffing task in IRSS, creates an AF CRM, and retrieves JS comments from KM/DS. AF/A5DR then uploads the AF and JS CRMs to IRSS and creates a Comment Resolution task to the Sponsoring organization.

Comment Resolution.

Sponsors must use the CRMs to record adjudication action taken in response to each comment. The Sponsor must show the rationale for not fully accepting a critical or substantive comment. Change recommendations must be properly coordinated with the Joint and AF commenters to ensure the changes do not adversely affect other areas of the document.

Comments against AF-sponsored documents designated as JROC interest or JCB Interest must be adjudicated to the final satisfaction of the FCB Chair on behalf of the JCB/JROC, and the Joint Staff certifying or endorsing organizations. Comments against AF-sponsored documents designated as Joint Information must be adjudicated to the final satisfaction of the validation authority.

Document Sponsor Internal Approval. Following completion of comment resolution, Sponsors will conduct an internal review of the document before it goes forward for the eAFROC and validation staffing. Documents submitted for formal approval and validation will be accompanied by a transmittal memorandum signed by the Commander for documents designated for CSAF approval or the Sponsor's Director of Requirements (5/8/9) for all other documents.

Upon document and CRM receipt, the Sponsor IRSS POC will use the Document Review Checklist to ensure the document meets JCIDS criteria, check the spelling and grammar, and verify proper classification and portion markings. The IRSS POC then imports the updated version of the document, adjudicated AF and Joint Staff CRMs, and supporting materials to IRSS. The IRSS POC will create an eAFROC Review Request task to AF/A5D, followed by a notification email from their Requirements Policy shop's O-6 to the AFGK, to include the signed transmittal memorandum. The IRSS POC will update the Document Record Status to "eAFROC Review – AFGK Review".

To expedite the staffing process, Sponsors may submit documents to AF/A5DR and request initiation of the eAFROC concurrently with staffing required to obtain the transmittal memorandum. The transmittal memorandum must be obtained prior to initiating AF validation.

eAFROC. The eAFROC is not an additional commenting phase. The purpose is to route the document for final certifications, endorsements, and attestations.

After review by the AF/A5DR team and the AF/A5D SME, AF/A5D approves initiation of the eAFROC Review. The AF/A5DR Team creates an eAFROC Review task in IRSS to organizations on the AFROC Principal Distribution List and updates the Document Record Status to "eAFROC Review".

IRSS POCs for each tasked organization should forward the document to appropriate individuals in their organization for review. AFROC endorsement certifies that the Stakeholders:

- Agree that comments have been properly adjudicated, or proper justification exists to proceed with unresolved comments.

- Agree that comment adjudication has not created secondary issues that would preclude validation.
- Agree that required certifications, endorsements, attestations, or waivers are obtained prior to validation. JCIDS requires documents designated as JCB or JROC Interest obtain Joint Staff certifications, endorsements, and or waivers prior to AF approval. This includes proper adjudication of comments made by Joint Staff certifiers and endorsers during staffing.

Any recommendations to not endorse validation of the document will be accompanied by a rationale. IRSS POCs will consolidate endorsement recommendations and present the document and recommendations to their AFROC Principal for a document validation recommendation. IRSS POCs will email their principal-approved recommendation and rational if necessary to AF/A5DR and close the eAFROC Review task in IRSS. The full name and rank of the AFROC Principal must be in the Approval Authority section of the Task Details.

The eAFROC review concludes with AF/A5D approval to:

- Forward the package to the designated AF RDA for AF approval or validation staffing.
- Forward the document to the FCB to begin joint validation, if required.

To expedite the validation process, FCB review may be concurrent with AF validation staffing to the AF RDA. AF documents may be submitted to the Joint Staff for review by the FCB Working Group(s) and FCB immediately following the eAFROC and AF/A5D approval.

Validation. Validation criteria are tailored to support the type of document. See Section 2 for further details.

Formal decisions are documented in an AFRDM and signed by the CSAF for documents associated with any program designated as a Major Defense Acquisition Program or the AF/A5D designated RDA. The AFRDM will validate a Joint Interest document or approve forwarding the document to the JCB. A signed AFRDM is required prior to releasing the document beyond the FCB level for final joint validation.

If Joint validation is required, the sponsor will collaborate with the AF/A5DR Joint Integration Team, the AF/A5D SME, and the Joint Staff to build and present the briefing products to the FCB WG, FCB, JCB and JROC. Normally, no briefing is required for AF validation.

Completion. After AF or Joint validation, the Sponsor will import a copy of the final document to IRSS. AF/A5DR will ensure the final document contains the signed validation memorandum and all supporting materials are posted in IRSS. AF/A5DR will forward the package to the Joint Staff Gatekeeper for archiving in KM/DS. The document is the official document of record and must be updated to reflect any changes made during formal validation and review.

3.3. Rapid Staffing. Rapid staffing is used when expedited approval is required in support of rapid capability development. Rapid staffing is not for use in all circumstances and must be approved by the AFGK.

Rapid staffing is the same as formal staffing except it uses compressed timelines and combines the formal staffing phases of initial staffing and the eAFROC. Unlike traditional staffing, rapid staffing allows eAFROC comments in addition to final certifications, endorsements, and attestations. IRSS POCs for each tasked organization will forward the document to appropriate individuals in their organization for review. AFROC principal endorsement certifies that the Stakeholders agree that required certifications, endorsements, attestations, or waivers have been obtained prior to validation.

When the AF employs rapid staffing, the JSGK will likely also expedite Joint staffing.

APPENDIX 1 – ACRONYMS, GLOSSARY, AND REFERENCES

Acronyms

AFGK—Air Force Gatekeeper

AFRDM – Air Force Requirements Decision Memorandum

AFROC – Air Force Requirements Oversight Council

AI – Artificial Intelligence

AoA—Analysis of Alternatives

APA – Additional Performance Attribute

CBA—Capabilities-Based Assessment

CDD—Capability Development Document

CDP - Capability Development Plan

CIP – Critical Intelligence Parameter

CNS – Capability Needs Statement

CONOPS - Concept of Operations

CRM—Comment Resolution Matrix

dCDD – draft CDD

DCR—DOTmLPF-P Change Recommendation

DIE – Defense Intelligence Enterprise

DoDAF – DoD Architecture Framework

DOTmLPF-P - Doctrine, Organization, Training, materiel, Leadership, Personnel, Facilities, and Policy

DWT – Document Writing Team

eAFROC – electronic AFROC

FCB—Functional Capabilities Board

FOC – Full Operational Capability

FoS – Family of Systems

FPO – Functional Process Owner

ICD—Initial Capabilities Document

IOC – Initial Operational Capability

IRSS—Information and Resource Support System

IS – Information System

JCB—Joint Capabilities Board

JCIDS – Joint Capabilities Integration and Development System

JPR – Joint Performance Requirement

JROC—Joint Requirements Oversight Council

JROCM—JROC Memorandum

JSD—Joint Staffing Designator

JEON - Joint Emergent Operational Need

JUON - Joint Urgent Operational Need

KM/DS—Knowledge Management & Decision Support System

KPP—Key Performance Parameter

KSA—Key System Attribute

MDA—Milestone Decision Authority

MTA - Middle Tier Acquisition

NDS – National Defense Strategy

OPR – Office of Primary Responsibility

POA&M - Plan of Action and Milestones

POC – Point of Contact

RAI – Responsible Artificial Intelligence

RDA – Requirements Decision Authority

RDP – Requirements Definition Package

RFP—Request for Proposal

RMCT - Requirements Management Certification Training

SDP – System Development Plan

SME – Subject Matter Expert

SoS – System of Systems

SPR—Solution Pathway Review

SW - Software

TMRR – Technology maturation and Risk Reduction

UON - Urgent Operational Need

Glossary

Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this manual only.

Affordability – The degree to which the life-cycle cost of an acquisition program is in consonance with the long-range modernization, force structure, and manpower plans of the individual DoD Components (military departments and defense agencies), as well as for the Department as a whole. Affordability constrains prioritization of requirements, drives performance and cost trades, and ensures that unaffordable programs do not enter the acquisition process.

Artificial Intelligence - The theory and development of the set of technologies that enable machines to sense, comprehend, act, learn and perform tasks that normally require human intelligence, such as visual perception, speech recognition, and decision-making.

Capability - The ability to complete a task or execute a course of action under specified conditions and level of performance through combinations of means and ways across the DOTmLPF-P to perform a set of tasks to execute a specified course of action. (Source: DoD Dictionary of Military and Associated Terms)

Capability Drop - This describes the performance characteristics of a relatively small increment of a capability solution included in a software build necessary for partial deployment of the overall 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 Capability Drop (or equivalent) could be developed directly from the definitions in the IS-CDD in the event of a timelier need for the capability solution. More commonly, multiple CDs (or equivalents) would be derived from an RDP (or equivalent) or IS-CDD to deliver the overall capability solution defined in the RDP (or equivalent) or IS-CDD. (Source: JCIDS Manual)

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. (Source: CJCSI 5123.01)

Capability Need - See "Requirement."

Capability Requirement – Capability Requirements are Measures of Effectiveness in the form of mission focused task statements that are best written in "task, condition and standard" format. They are described in relation to tasks, conditions, and standards IAW the Universal Joint Task List or equivalent DoD Component Task List and are thought of as "what needs to be done (the metric), and to what level (the initial value)". If a Capability Requirement is not satisfied by a capability solution, then there is an associated capability gap. A requirement is considered 'draft' or 'proposed' until validated by the appropriate authority. (Source: JCIDS Manual)

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. (Source: CJCSI 5123.01)

Critical Intelligence Parameter – A threat capability or threshold established collaboratively by the requirements sponsor and the capability developer, changes to which could critically impact the effectiveness and survivability of the proposed system. (Source: DIA 5000.200)

Document Sponsor - The organization submitting a requirements document. The Document Sponsor is responsible for format compliance of staffing and final closeout of validated documents for archiving. Solution Sponsors for successor documents - CDDs and Joint DCRs - may be different from the Requirement Sponsors for initial documents - ICDs, UONs, JUONs, and 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 validated document generated by a different Sponsor. (Source: JCIDS Manual)

Energy - Energy is an enabler of joint military capabilities, and ensuring the availability of sufficient energy supplies will grow in importance with the development of new energy intensive capabilities designed to sustain and enhance warfighting capability. The DoD's capability development activities, from requirements to acquisition to sustainment, must increase energy supportability and must reduce energy demand across all capability solutions. The joint capacity to meet the demand for energy needed to employ and sustain a capability in projected scenarios and threat environments should inform the energy performance requirements of all DoD systems. The DepSecDef provided guidance in an April 2022 memorandum requiring an increased emphasis on the statutorily required energy KPP and directed, "… assessments of energy supportability and demand reduction are conducted and standardized, as appropriate, for all capability development activities within JCIDS, the defense acquisition process, and upgrades to current systems."

Exportability - The process to identify, develop and integrate technology protection features into U.S. defense systems early in the acquisition process to protect Critical Program Information (CPI) and other critical technologies / capabilities and thus enables a system's export to partners. Technology protection primarily involves two tools: Anti-Tamper (AT) and differential capability modifications.

Family of Systems - A set of systems that provide similar interdependent capabilities through different approaches to achieve similar or complementary effects for example, the warfighter may need the capability to track moving targets. The FoS that provides this capability could include manned or unmanned aerial vehicles (UAVs) with the appropriate sensors, a space-based platform or special operations capability. Each can provide the ability to track moving targets, but with differing characteristics of persistence, accuracy, timeliness, etc. (Source: DoD, 2018, DAU Glossary)

Feasible – A requirement that is technically achievable and executable within the estimated schedule and budgeted life cycle cost.

Full Operational Capability – Full attainment of the capability to effectively employ a weapon, item of equipment, or system of approved specific characteristics, which is manned and operated by a trained, equipped, and supported military force or unit. The specifics are defined in the CDD.

Initial Operational Capability – That first attainment of the capability to effectively employ a weapon, item of equipment, or system of approved specific characteristics with the appropriate number, type, and mix of trained and equipped personnel necessary to operate, maintain, and support the system. It is normally defined in the CDD.

Information Systems - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: Title 44 U.S.C. § 3502)

Information Technology -

- With respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in that automatic acquisition storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency

that requires the use - (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

- Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
- Does not include any equipment acquired by a federal contractor incidental to a federal contract. (Source: Title 40 U.S.C. § 3502)
- Does not include national security systems as defined in 40 U.S.C. § 3502.

Intelligence Interoperability - The ability to receive, produce, store and/or share intelligence data, products, services, and/or processes with similarly compatible systems; and, to render that data, product, service, and/or process to other applicable systems in a readily available format. Intelligence interoperability includes both the technical exchange of information (data) and the operational effectiveness of that exchanged information (service and processes). Intelligence interoperability is more than just information exchange; it includes the harmonization of intelligence systems, processes, procedures, organizations, and missions. (Source: JP 2.0, DoDI 8330.01).

Interoperability -

- The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (Source: JP 3-0)
- The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (Source: JP 6-0)
- The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity (formerly IA). (Source: DoDI 8330.01)

Joint - Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. Note that this definition of "joint" is applicable to JCIDS documents and capability solutions which apply to more than one DoD Component. See "joint matters" definition derived from Title 10 U.S.C. § 668 and "joint military capability" for the definition applicable to Title 10 U.S.C. § 181 JROC responsibilities. (Source: DoD Dictionary of Military and Associated Terms)

Joint Concepts - Identifies a current or future military challenge and proposes a solution to improve the ability of the joint force to address that military challenge. A joint concept may also propose new ways to employ the joint force based on future technology. (Source: DoD Dictionary of Military and Associated Terms, CJCSI 3010.02).

Joint Military Capabilities - Means the collective capabilities across the joint force, including both joint and force-specific capabilities that are available to conduct military operations. (Source: Title 10 U.S.C. § 181)

Joint Performance Requirement - A performance requirement that is critical or essential to ensure interoperability or fulfill a capability gap of more than one armed force, Defense Agency, or other entity of the Department of Defense, or impacts the joint force in other ways such as logistics. (Source: Title 10 U.S.C. § 181)

Materiel (Capability Solution, aka Big 'M') - 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. (Source: DoD Dictionary of Military and Associated Terms, JP 4-0)

materiel (Capability Solution, aka little 'm') - The letter "m" in the acronym is usually lower case since Joint DCRs do not advocate new materiel development, but rather advocate the identification of materiel items, systems, or equipment needed to support the required capability increased quantities, modifications, improvements, or alternate applications of existing materiel or the purchase of Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), or Non-Development Items (NDI). Sometimes referred to as "little m" materiel, the materiel DOTmLPF-P consideration is everything necessary to equip DoD forces to operate effectively. Materiel includes ships, tanks, self-propelled weapons, aircraft, related spares, repair parts, and support equipment, but excludes real property, installations, and utilities.

Mandatory KPPs – These are the Force Protection (FP), System Survivability (SS), Sustainment, and Energy attributes that are designated as mandatory KPPs IAW the applicable provisions of federal law under Title 10 U.S.C.

Mandatory Performance Attributes - These consist of the four mandatory KPPs as well as the Interoperability Performance Attribute and Exportability.

Materiel Capability Solution - Correction of a deficiency, satisfaction of a capability gap, or incorporation of new technology that results in the development, acquisition, procurement, or fielding of a new item (including ships, tanks, self-propelled weapons, aircraft, and related software and data, spares, repair parts, and support equipment, but excluding real property, installations, and utilities). In the case of FoS and SoS approaches, an individual materiel solution may not fully satisfy a necessary capability gap on its own. [CJCSI 5123]

Materiel Development Decision - The formal entry point into the acquisition management system and is mandatory for all programs. It is based on a validated requirements document (an ICD or equivalent requirements document) and the completion of the Analysis of Alternatives Study Guidance and Study Plan. This decision directs execution of the Analysis of Alternatives and authorizes entry into the Materiel Solution Analysis Phase of acquisition.

Middle Tier Acquisition - A rapid acquisition approach within the Adaptive Acquisition Framework that focuses on rapidly delivering capability to fill a mission capability gap. Also known as Section 804 authorities, the MTA process is detailed in DoD Instruction 5000.80 which provides authorities to rapidly prototype and/or rapidly field capabilities requiring minimal capability development effort and able to deliver to the warfighter in 2 – 5 years. DoDI 5000.80 allows for an acquisition process distinct from the traditional acquisition system and exempt from JCIDS and the processes in DoD Directive 5000.01, *The Defense Acquisition System*. Each DoD Component has developed processes to implement MTA.

Need - See "Requirement."

Net-Ready – Net Ready is addressed as part of the Mandatory Interoperability Attribute. DoD IT that meets required information needs, information timeliness requirements, has a cybersecurity

accreditation, and meets the required attributes to support military operations, to be entered and managed on the network, and to effectively exchange information for both the technical exchange of information and the operational effectiveness of that exchange. DoD IT that is net ready enables warfighters and DoD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all participants. Net readiness requires that IT operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure communications within and across diverse media; information is in a common format with a common meaning; common human-computer interfaces for users and effective means to protect the information exist. Net readiness is critical to achieving the envisioned objective of a cost-effective integrated environment. Achieving and maintaining this vision requires interoperability:

- Within a joint task force or CCMD area of responsibility (AOR).
- Across CCMD AOR boundaries.
- Between strategic and tactical systems.
- Within and across Military Services and agencies.
- From the battlefield to the sustaining base.
- Among U.S., allied, and coalition forces.
- Across current and future systems. (Source: JCIDS Manual)

Non-Materiel Capability Solution - Changes to DOTmLPF-P, 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. (Source: DoD Dictionary of Military and Associated Terms, JP 4-0)

Objective Value - The objective value is only applicable when a higher level of performance (above the threshold value) represents a 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 must be feasible and achievable but may involve higher risk in life cycle cost, schedule, or technology. Performance above the objective value does not warrant additional expenditure. [JCIDS Manual]

Performance Attribute – A characteristic or inherent part of a required system that is needed by the system to achieve satisfactory performance.

Performance Requirement – Consists of performance attributes (KPPs, KSAs, and APAs) of a system that is critical or essential to the development of an effective military capability that does not meet the criteria of a JPR. The Service Chiefs are responsible for all performance requirements for their respective Service. (Source: Title 10 U.S.C. § 181)

Program Costs (IAW Title 10 U.S.C. § 2448a) - The procurement unit cost and sustainment cost (referred to in this Section as “program cost targets”). Sustainment cost targets are calculated in accordance with the “Operational” cost metric.

Requirement - A capability which is needed to meet an organization’s roles, functions, and missions in current or future operations to the greatest extent possible. A requirement is considered ‘draft’ or ‘proposed’ until validated by the appropriate validation authority. (Source: CJCSI 5123.01)

Requirements Definition Package - 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, KSAs, and APAs necessary to scope and cost implementation of a capability solution. The RDP (or equivalent) may also identify non-materiel changes that need to be implemented to fully realize the IS capability solution. The RDP (or equivalent) is approved by the delegated oversight authority listed in the IS-ICD or IS-CDD. (Source: JCIDS Manual)

Requirement Sponsor - See "Document Sponsor."

Responsible Artificial Intelligence – The AF must integrate AI enabled capabilities responsibly. Responsible AI is governed by five DoD AI Ethical Principles: Responsible, Equitable, Traceable, Reliable, and Governable. These five Ethical Principles apply to all DoD AI capabilities at any scale, used in warfighting and business applications, to include AI-enabled autonomous systems. Implementation of RAI guards against AI-enabled capabilities that may be applied unethically or irresponsibly. See Appendix 3 for definitions of the five AI Ethical Principles, recommendations on how to document RAI efforts early in the development process, and a list of additional items for consideration.

Shall Statement – For the purposes of JCIDS documents, the word "shall" be used as "mandatory". A shall-statement indicates a mandatory requirement. A mandatory requirement requires justification of why not to follow the requirement. In a CDD, only one attribute will equal one shall statement. Shall equals the legal terms of "will" or "must".

Solution - See "Capability Solution."

Solution Sponsor - See "Document Sponsor."

Sponsor - See "Document Sponsor."

System of Systems - A set or arrangement that results when independent and useful systems are integrated into a larger system that delivers unique capabilities. A SoS may deliver capabilities by combining multiple collaborative and independent-yet-interacting systems. The mix of systems may include existing, partially developed, and yet-to-be designed independent systems. (Source: DoD, 2018, DAU Glossary)

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. (Source: CJCSI 5123.01)

Threshold Value - A minimum acceptable operationally effective or suitable value below which the utility of the system becomes questionable. The threshold value for a performance attribute (KPP, KSA or APA) must also be considered achievable within the projected life cycle cost, schedule, and technology at low to moderate risk. [JCIDS Manual]

Urgent Capability Acquisitions - Acquisition programs that provide capabilities to fulfill urgent operational needs and other quick reaction capabilities that can be fielded in less than 2 years. (Source: DoDI 5000.81)

Urgent Operational Need - Capability requirements identified as impacting an ongoing or anticipated contingency operation. If left unfulfilled, Urgent Operational Needs result in capability gaps potentially resulting in loss of life or critical mission failure. (Source: CJCSI 5123.01)

Validation – The review and approval of capability requirements documents by a designated validation authority. The JROC is the ultimate validation authority for capability requirements unless otherwise delegated to a subordinate board or in the case where the independent validation authority is a Service, CCMD, or another DoD Component. (Source: CJCSI 5123.01)

References

AFI 63-101/20-101, *Integrated Life Cycle Management, 23 Nov 2021*

AF/A5/7 Capability Development Guidebook Vol 2A, *Capability Development Overview. Requirements Oversight & Governance*

AF/A5/7 Capability Development Guidebook Vol 2B, *Capability/System Development Plans*

AF/A5/7 Capability Development Guidebook Vol 2C, *Capability-Based Assessment (CBA)*

AF/A5/7 Capability Development Guidebook Vol 2D, *JCIDS/MCA Documents*

AF/A5/7 Capability Development Guidebook Vol 2D, *Annex A, Analysis of Alternatives (AoA)*

AF/A5/7 Capability Development Guidebook Vol 2E, *Strategic Requirements Document*

AF/A5/7 Capability Development Guidebook Vol 2F, *MTA - Rapid Requirements*

AF/A5/7 Capability Development Guidebook Vol 2G, *Urgent Needs*

AF/A5/7 Capability Development Guidebook Vol 2H, *Modifications*

AF/A5/7 Capability Development Guidebook Vol 2I, *Software Development*

CJCSI 5123.01I, Charter of the JROC and Implementation of JCIDS, 30 Oct 2021

DAFPD 10-9, *Lead Command Designation and Responsibilities for Weapon Systems, 25 May 2021*

DepSecDef Memo, *Energy Supportability and Demand Reduction, 26 May 2021*

DepSecDef Memo, *Implementing Responsible Artificial Intelligence in the Department of Defense, 26 May 2021*

DoDI 4650.01, *Policy and Procedures for Management & Use of Electromagnetic Spectrum*, *17 Oct 2017*

DoDI 5000.02, *Operation of the Adaptive Acquisition Framework, 08 Jun 2022*

DoDI 5000.69, *DoD Joint Services Weapon and Laser System Safety Review Processes, 15 Oct 2018*

DoDI 5000.73, *Cost Analysis Guidance and Procedures, 13 Mar 2020*

DoDI 5000.80, *Operation of the Middle Tier of Acquisition, 30 Dec 2019*

DoDI 5000.81, *Urgent Capability Acquisition, 31 Dec 2019*

DoDI 5000.85, *Major Capability Acquisition, 4 Nov 2021*

DoDI 5000.87, *Operation of the Software Acquisition Pathway, 2 Oct 2020*

DoDM 5200.01 Volume 2, *DoD Information Security Program: Marking Information, 28 Jul 2020*

HAF MD 1-57, *Deputy Chief of Staff, Air Force Futures (AF/A5/7)*

Manual for the Operation of Joint Capabilities Integration and Development System, 30 Oct 2021

Manual for the Operation of Joint Capabilities Integration and Development System, 8 Feb 2023 (draft)

APPENDIX 2. DOCUMENT CHECKLISTS

These checklists are an abbreviated version of the guidelines in the 2023 JCIDS Manual, Enclosure B and are intended for use in screening and review of document content. It is not a definitive guide to required content. DWT members must use the JCIDS Manual for detailed content guidance. Any deviations from the JCIDS Manual must be approved by the AF Gatekeeper. All sections reference the appropriate pages in the JCIDS Manual.

APPENDIX 2A. DCR Checklist. Pages B-E-1 through B-E-10.

Format

□ Complies with JCIDS formatting (font, style, spacing, etc.) pages B-1, B-2.

□ Complies with DCR formatting, page B-E-1 and B-E-2.

□ Classification markings IAW DoDM 5200.01 V2

Validation Page. Page B-E-2 and B-C-3. Must contain validation statement appropriate to assigned JSD.

Waivers. Page B-E-3. Include signed waiver or reference to Joint Staff Gatekeeper's KM/DS approval note.

Executive Summary. Page B-E-3. No more than 1 page

Body. Pages B-E-3 through B-E-10. 5 sections, no more than 30 pages.

□ Section 1. Ops Context. Pages B-E-3 and B-E-4. **Describe** how recommendations address or enable solutions to validated requirements and contribute to the missions/activities of the joint force.

- □ Narrative **consistent** with DoDAF OVs from prior analysis.
- □ Provide **only** OV-1 here. Include URL of DoDAF repository.
- □ **Describe** the addressed ROMO and **traceability** to UCP assigned mission, OPLANs/CONPLANs, supporting scenario products. Service and Joint Concepts, CONOPS, and other relevant factors to the capability requirements identified in the DCR.
- □ If the DCR is a successor document to one or more validated JCIDS documents:
  - □ Cite **validated** source documents. Post to KM/DS, IRSS, or provide to JSGK and AFGK.
  - □ Note any **changes** to context from that in the ICD or other source document.
  - □ **Ensure** key intelligence support capabilities affected by the changes to DOTmLPF-P are addressed within the operational context.
- □ If the DCR is not based on a validated JCIDS document, provide ops context as outlined for Section 1 of an ICD.

□ Section 2. Threat Summary. Pages B-E-4 through B-E-6. Provides context for the capability requirements addressed or enabled by the DCR. Provides traceability to approved threat products from DIE. May not be applicable. Coordinate with the proponent for the intel certificate, as outlined in Annex G to Appendix G of this enclosure to determine need.

- □ If the DCR is a successor document to one or more validated requirement documents:
  - □ **Cite** latest applicable DIE or Service-approved threat products. DCRs enabling or associated with Major Defense Acquisition Programs must use current DIA-approved threat products.
  - □ **Outline** threat summary(ies) associated with the validated requirements addressed or enabled.

- □ If the DCR is not based on a validated document, **provide** a threat summary as in Sec 2 of an ICD.

□ Section 3. Capability Requirement Discussion. Pages B-E-6 and B-E-7. Identifies the validated capability requirements addressed or enabled by the DCR, and outlines the results of related studies, lessons learned, or analysis performed to define the change recommendations.

- □ Clearly and succinctly **describe** the capability gap.
- □ Narrative must be **consistent** with DoDAFs from prior analysis.
- □ **Provide** an overview of supporting validated requirements addressed or enabled by the DCR.
- □ If the DCR is not based on a validated document, **provide** the capability requirements and gaps as in an ICD, Sec 3.
- □ Summarize **all** analyses and studies conducted to develop change recommendations. Ensure availability on IRSS and KM/DS.
- □ Key intelligence support capabilities affected by the changes are **addressed**.

□ Section 4. Change Recommendations. Pages B-E-6 and B-E-7. Outlines recommendations that provide or enable capability solutions. Identifies related interdependencies. Provide the following:

- □ **Describe** the recommended change.
  - □ TTP changes and **implications** on the safe use of the solution in the proposed environment.
  - □ Forces and systems **affected**, and any **impact** on interoperability.
  - □ If future technology is needed, **discuss** the maturity and a risk assessment of the approach.
  - □ **Cite** DoD policies or issues that would prevent implementation of the changes and the reason for non-compliance. **Propose** changes to the policy or issue and identify other implications.
  - □ **Update** applicable DoDAF OVs and CVs to show how the solutions address requirements and mitigate portfolio gaps without introducing unnecessary redundancy in capability or capacity.

□ Section 5. Implementation Plans. Pages B-E-7 through B-E-9. Outline implementation plans for the recommended changes and task OPR(s) and affected Joint DOTmLPF-P FPOs. For each recommendation, provide the following:

- □ Proposed **POA&M** with start times, major milestones, and completion dates.
- □ **Discuss** relationships between recommendations and implementation timing.
- □ Fielded or new key intelligence support capabilities are **identified** and addressed in the plan.
- □ **Propose** a specific OPR for each action and provide rationale. **Socialize** OPR nomination.
- □ **Provide** rough-order-of-magnitude total required resources needed in Table form.

Appendices. Pages B-E-9 and B-E-10. Only A-D are permitted as defined. D counts for page limit. Submit additional information IAW JCIDS Manual, Enclosure B.

- □ Appendix A. References. **First entry** - Ensure architectures are discoverable.
- □ Appendix B. Acronym List. All acronyms in the document in **alphabetical** order

- □ Appendix C. Glossary. **Consistent** with AV-2.
  - □ Add **statement** "Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this document only."
- □ Appendix D. (Optional) Classified Appendix. Provided to the J8 SAPCO
  - □ If the document is not useful without this appendix, **classify** higher.
  - □ Indexed to **align** with the baseline document sections.

DoDAF Architecture Views. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B Figure B-26 and if the Net-Ready certification is applicable, additional views listed in Table B-29.

APPENDIX 2B. ICD and Variants Checklists

ICD Checklist. Pages B-A-1 through B-A-12.

Format

□ Complies with JCIDS formatting (font, style, spacing, etc.) pages B-1, B-2.

□ Complies with ICD formatting, page B-A-1 and B-A-2.

□ Classification markings IAW DoDM 5200.01 V2

Validation Page. Page B-A-2. Must contain validation statement appropriate to assigned JSD.

Waivers. Pages B-A-2 and B-A-3. If applicable, list any waivers granted by the Joint Staff or AF Gatekeeper. Include the signed waiver or reference to the Joint Staff Gatekeeper's KM/DS approval note.

Executive Summary. Page B-A-3. No more than 1 page

Body. Pages B-A-3 through B-A-12. 4 sections, no more than 10 pages. Appendix D (SAP) counts toward page limit. Each section augmented by the classified appendix will refer to the classified appendix.

□ Section 1. Operational Context. Pages B-A-3 and B-A-4. Describe how the capability, being concept based and threat informed, contributes to the missions and activities of the joint force.

- □ **Describe** the addressed ROMO and **traceability** to UCP assigned mission, OPLANs/CONPLANs, supporting scenario products. Service and Joint Concepts, CONOPS, and other relevant factors to the capability requirements identified.
- □ **Discuss** the impact of a loss of the capability and if the loss would lead to critical mission failure.
- □ Sponsors shall **address** Exportability "Allied/Partner Interoperability and Coalition Use."
- □ **Proposed** IOC and FOC consistent with DoDAF CV-3 and capability phasing from ICD Section 3.
- □ **Identify** required measurable operational outcomes; desired effects to achieve those outcomes; how they complement the integrated joint/multinational warfighting force; and required enabling capabilities.
- □ Provide **only** OV-1 here.
- □ Narrative **consistent** with DoDAF OVs generated during prior analysis. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B Figure B-26 and if the Net-Ready is applicable, additional views listed in Table B-29.

□ Section 2. Threat Summary. Pages B-A-4 and B-A-5. Gaps are consistent with threat.

- □ **Cite** DIE threat products.
- □ **Identify** anticipated adversary capabilities from the supporting DIE element. Address capability and associated capability gaps **related** to the conduct of operational tasks and missions.
- □ **Describe** all threat capabilities, tactics, and doctrine, in the expected environment and the nature of threats which are a factor in setting the capability and initial objective values.
- □ **Include** any CBRN, space, cyber, or kinetic threats and/or threats to a future system's use of the electromagnetic spectrum if the operational context requires operation in such environments.
- □ **Consider** threats to follow-on RDT&E, production, and (O&M) resulting from technology transfer, espionage, and other adversarial collection efforts.

- □ **Consider** threats that are likely to evolve or change to ensure flexibility in requirements.
- □ **Cite** either approved or proposed CIPs for review and approval in conjunction with ICD validation.

□ Section 3. Capability Gaps and Overlaps. Pages B-A-5 through B-A-9. Specify capability requirements and assess associated capability gaps in terms of a comparison between the capability requirements and current capability solutions.

- □ **Define** capability requirements as follows: "The ability to [perform a task (UJT or Service Task) Operational Activity]] against/given a [Threat] in order to achieve [Effect] in a/under [Environmental Conditions] in the [Standard Timeframe]." capability requirements must be general enough to not support a predetermined capability solution or approach but specific enough to evaluate alternatives.
- □ **Specify** the required operational attributes with appropriate quantitative parameters and metrics. See Annex A to Appendix B of Enclosure C to the JCIDS Manual for examples.
  - □ Consider the impact of mandatory performance attributes and special interest items.
- □ The narrative, attributes, and values in the capability requirements and capability gap Section must be **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.
- □ **Describe** the intelligence support requirements and resources needed to enable each capability requirements. Refer to JCIDS Manual Annex G of Appendix G.
- □ Survivability Considerations
  - □ Consider the **cybersecurity threat** when determining initial objective values and include the appropriate CSRC. Refer to JCIDS manual, Annex C to Appendix G and the Cyber Survivability Endorsement Implementation Guide which can be found on KM/DS. Additionally, identify the system categorization for IS and Platform IT systems as a required capability - the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability if a security breach occurs. This is required by DoD's Risk Management Framework for Information Technology Systems.
  - □ Consider **EMS** threats when determining initial objective values and include exemplar statement in the ICD for the appropriate EMS Survivability Risk Category. Refer to JCIDS Manual Annex C to Appendix G and the DoD Guidebook for Electromagnetic Spectrum Survivability on KM/DS.
  - □ **State** whether the proposed solution will be required to operate in CBRN (including EMP) environments and ensure required CBRN operations are addressed in any follow-on AoA(s). CBRN Mission Critical systems must consider all relevant CBRN environments (as indicated in the threat Section).
- □ **Describe** the capability gaps or overlaps in terms of the difference between the initial objective values and the performance levels of capability solutions currently available or in development.
- □ **Identify** how each capability gap impacts the operational context in Section 1 in terms of inability to execute part or all of an operational plan and/or unacceptable levels of operational risk. **Identify** the workarounds and operational risk(s) associated with them.
- □ **Provide** a summary table.

- □ Section 4. Final Recommendations. Pages B-A-9 and B-A-11. Identify paths to satisfy the capability requirements and mitigate gaps.
  - □ **Identify** DOTmLPF-P recommendations to be considered as part of a materiel solution and independent of a materiel solution.
  - □ **Specify** the preferred type of materiel approach such as:
    - □ Evolution of a fielded capability solution(s) with significant capability improvement.
    - □ Replace or recapitalization of a fielded capability with significant capability improvement.
    - □ Introduction of a transformational capability solution that differs significantly in form, function, and/or operation from fielded solutions.
  - □ Identify key factors that may be, or may become, significant cost drivers.

Appendices. Pages B-A-11 through B-A-12. Only A-F are permitted as defined. D counts for page limit. Submit additional information IAW JCIDS Manual, Enclosure A.

- □ Appendix A. References. **First entry** - Ensure architectures are discoverable.
- □ Appendix B. Acronym List. All acronyms in the document in **alphabetical** order
- □ Appendix C. Glossary. **Consistent** with AV-2.
  - □ Add **statement** "Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this document only."
- □ Appendix D. (Optional) Classified Appendix. Provided to the J8 SAPCO
  - □ If the document is not useful without this appendix, **classify** higher.
  - □ Indexed to **align** with the baseline document sections.
- □ Appendix E (Optional). If not in main document, **describe** Cyber Survivability Attribute requirements. **Reference** the Cyber Survivability Endorsement (CSE) Implementation Guide.
- □ Appendix F (Optional). If not in the main document, **describe** EMS Survivability Risk Category. **Describe** IAW page B-G-C-1, EMS section.

DoDAF Architecture Views. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B Figure B-26 and if the Net-Ready certification is applicable, additional views listed in Table B-29.

IS-ICD Checklist. Pages B-B-1 through B-B-6.

The IS-ICD is identical to the ICD with the following exceptions:

- □ Section 3. **Must include** a Net-Ready Performance Attribute table, JCIDS Manual, Figure B-2.
  - □ **Describe** each attribute in terms of initial minimum values, rather than threshold/objective.
  - □ **Include** Responsible AI principles into AI requirements IAW DepSecDef Memo, 26 May 2021.
- □ Section 4.
  - □ **Must include** the "IT Box," JCIDS Manual, Figure B-3
  - □ **Must include** estimated lifecycle costs for the program, JCIDS Manual, Figure B-4

DoDAF Architecture Views. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B Figure B-26 and if the Net-Ready certification is applicable, additional views listed in Table B-29.

Software-ICD Checklist. Pages B-B-A-1 through B-B-A-12.

The SW-ICD is identical to the ICD with the following exceptions:

Executive Summary. Not required.

Body. Pages B-B-A-3 through B-B-A-12. 5 sections, no more than 10 pages, including classified index.

Sections 1-3, no changes from basic ICD.

Section 4. Interoperability.

- □ Describe **governance process** for interfaces and data for the program and the major systems, services, and networks with which the software must interoperate.
- □ Describe internal and externally accessible **data management**.
- □ Reference any **Digital Engineering** strategy, frameworks, or models.
- □ Include **Net Ready KPP table**, JCIDS manual Figure B-6, page B-B-A-9.
- □ Include **Responsible AI** principles into AI requirements IAW DepSecDef Memo, 26 May 2021.

Section 5. Final Recommendations.

- □ Outline the plan to capture, prioritize, and continuously refine the **lower-level needs** that will guide the software development.
- □ Include alignment with **legacy** systems, **related** systems, software, and platforms.
- □ Identify **UAs** to provide active, continuous engagement during development.
- □ Identify **DOTmLPF-P recommendations** to be considered as part of a materiel solution and independent of a materiel solution.
- □ Include how the **evolution of software requirements**, development, and operations align and evolve with DOTmLPF-P efforts.
- □ Consider and address **affordability** in the development of an SW-ICD.

DoDAF Views. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B, Figure B-26 and if Net-Ready certification is applicable, additional views listed in Table B-29.

APPENDIX 2C. CDD and Variants Checklists

CDD Checklist. Pages B-C-1 through B-C-28

Format

□ Complies with JCIDS formatting (font, style, spacing, etc.) pages B-1, B-2.

□ Complies with CDD formatting, page B-C-2.

□ Classification markings IAW DoDM 5200.01 V2

Validation Page. Page B-C-2 and B-C-3. Must contain validation statement appropriate to assigned JSD.

Waivers. Pages B-C-3. If applicable, list any waivers granted by the Joint Staff or AF Gatekeeper. Include the signed waiver or reference to the Joint Staff Gatekeeper's KM/DS approval note. For waivers to format, the Sponsor will include a crosswalk of the format Sections/content and where that content can be found in the waived document format. This does not contribute to page count limits.

Executive Summary. Page B-C-3. No more than 1 page

Body. Pages B-C-3 through B-C-28. 13 sections, no more than 45 pages. Appendix D (SAP) counts toward page limit. Each section augmented by the classified appendix will refer to the classified appendix.

□ Section 1. Operational Context. Pages B-C-3 and B-C-4. **Describe** ICD capabilities being addressed by the CDD and their contributions to Joint Force.

- □ Narrative **consistent** with DoDAFs generated during prior analysis or to support this CDD. Required views are in JCIDS Manual, Appendix H to Enclosure B, Figure B-26. If Net-Ready applies, include views in Table B-29.
- □ Provide **only** OV-1 here. Include any intel connectivity and interoperability.
- □ Cite **validated** source documents. Make available in KM/DS, IRSS, or provide to JSGK and AFGK.
- □ **Summarize** the operational context associated with the CDD requirements. Note **changes** to context from that in the ICD or other source document.
- □ If not based on a validated JCIDS document, **provide** the operational context and initial DoDAF OVs as outlined for Section 1 of an ICD.

□ Section 2. Threat Summary. Pages B-C-4 and B-C-5. Solutions are consistent with threat.

- □ Develop using the most **current** DIE threat products.
- □ **Cite** threat products.
- □ Describe **new** threats since ICD as outlined for ICD Section 2.
- □ If not based on a validated JCIDS document, **provide** the threat summary as in ICD, Section 2.
- □ Summarize CIPs and **link** to KPPs and KSAs. Cite **COLISEUM** number, CIP number, and topic.
- □ Summarize **all** threats cited in the System Survivability KPP.

□ Section 3. Capability Discussion. Pages B-C-5 through B-C-7. Identifies capability requirements and gaps addressed by the CDD. Outline studies or analysis performed since ICD validation.

- □ If not based on a validated requirements document, **outline** the requirements and associated gaps in the format of Section 3 of an ICD in addition to the below content.
- □ Narrative must be **consistent** with DoDAF SV-8, especially the discussion of dependencies.

- □ Provide **updated** DoDAF CVs consistent with CDD.
- □ Summarize **all** analyses and studies conducted to derive attributes and ensure availability.
- □ Capability Requirement to Attribute Traceability, Page B-C-6, **Figure B-7**.
- □ Provide **traceability** between capability requirements and performance attributes in Section 5
- □ Describe **dependencies** between CDD solutions and other fielded/planned solutions.
  - □ Include **interactions** with intel capabilities, dependencies, and enablers over the planned lifecycle of the solution. Discuss **critical** dependencies and known risks.
- □ Identify SoS **compatibility and synchronization** of related solutions.
- □ Address if solution needs **undeveloped** intel tech or fielded intel tech planned for **deactivation.**

□ Section 4. Program Summary. Pages B-C-7 and B-C-8. Development method and interdependencies.

- □ Strategy for reaching **FOC** and, if applicable, relationship between **increments** defined in CDD.
  - □ **Define** IOC and FOC of current increment, dates, types, and quantities of **required assets**.
  - □ Required **integration** and timing related to IOC and FOC.
  - □ Identify the lead and following **platforms** for IOC and FOC.
  - □ **All** employing units and **quantities** for ops, training, spares, attrition, etc., consistent with OV-4.
  - □ Describe plans to use a **MOSA** including future capabilities to be added, removed, or replaced.

□ Section 5. Performance Attributes. Pages B-C-8 through B-C-15.

- □ Consistent with CV-3, SV-7, and SV-8.
- □ Do not over specify or include technical specifications.
- □ **Correlate** each attribute (KPP, KSA, APA) to ICD attributes to the lowest possible JCA tier.
- □ Parameters most **critical to mission** effectiveness should be KPPs.
- □ Performance attributes are measures of **system performance**, not mission effectiveness.
- □ Parameters **are** technically achievable, quantifiable, measurable, testable, and unambiguous.
- □ If an incremental CDD, identify threshold/objective values by increment.
- □ If a FoS CDD, provide attributes for the FoS as well as those unique to each system.
- □ Identify and attributes requiring intelligence supportability or are threat sensitive.
- □ Thresholds are **minimums** for military utility; objectives are **significant** increase in utility.
- □ **Mandatory** attributes - Energy, System Survivability, Force Protection, Sustainment KPPs; Interoperability JPR/KPP/KSA, APA, and Exportability KSA.
  - □ All **Interoperability** attributes are in appropriate Section 5 tables.
  - □ Provide threshold and objective for each mandatory KPP.
  - □ **Provide** rational and **coordinate** exclusion of mandatory KPPs with the **certifying** authority.
  - □ Include any **special interest** items.

- □ Provide **Figures B-8 and B-9.**

□ Section 6. Other System Attributes. Pages B-C-16 and B-C-17. Attributes not directly quantified and traceable to operational performance, and not identified elsewhere in the document. Examples:

- □ **Future** integration platforms.
- □ Human Systems Integration considerations that have a **major** impact.
- □ **Natural** environmental factors, such as climate, terrain, meteorological factors, etc., including weather, oceanographic and astro-geophysical impacts, and effects.
- □ Weather, oceanographic and astro-geophysical support needs throughout the lifecycle. Describe supportability needed for operational use to include atmospheric sensors/data/products/etc., to optimize combat effectiveness of the system.
- □ **Transportability** and deployability considerations.
- □ Space, Weight, & Power, and Cooling **margin** requirements and open system attributes.
- □ Cybersecurity **Risk** Management.

□ Section 7. Interoperability. Pages B-C-17 through B-C-19. Discuss all aspects of interoperability.

- □ Factors that may affect a **future** system or subsystem's interoperability with the base system.
- □ Intel interoperability **consistent** with JCIDS Manual, Annex G, Appendix G, Enclosure B.
- □ MOSA use **consistent** with CDD Section 4 and the Program Manager's acquisition strategy.
- □ Physical aspects that may **impact** the solution. **Consistent** with the OV-2 and SV-1.
- □ Describe Net-Ready **IAW** JCIDS Manual, Annex A, Appendix G, Enclosure B.
- □ **Ensure** Net Ready Attributes are in CDD Section 5, Figure B-9. Figure B-10 is in Section 7.
- □ Describe how training, exercises, and/or mission rehearsal systems will interoperate in the Joint Synthetic Training Environment and are designed to those standards.
- □ Incorporate responsible AI principles into AI requirements IAW DepSecDef Memo, 26 May 2021.

□ Section 8. Spectrum and E3 Control Requirements. Pages B-C-20 and B-C-21. EMS and E3 control.

- □ **Comply** with E3 direction. Address/summarize Host Nation coordination/approval, and Spectrum Supportability Risk Assessment (SSRA)
- □ Summarize the requirements to **ensure** mutual electromagnetic compatibility and effective E3 control. Comply with DoDI 3222.03. Ensure E3 controls consider all E3 disciplines.
- □ Consider all potential **friendly and neutral** background EMI.
- □ Preclude EA effects. Ensure threats are **consistent** with CDD Section 2.
- □ Ensure inclusion of all spectrum related requirements in **DoDI 4650.01**.

□ Section 9. Intelligence Supportability. Page B-C-21.

- □ **Reference** the Threat and Intell Supportability Guide in JCIDS Manual, Annex G to Appendix G.
- □ Identify **all** intelligence support requirements throughout the projected lifecycle.
- □ **Obtain** Intelligence certification.

□ Section 10. Weapon Safety Assurance. Pages B-C-22.

- □ **Obtain** Joint Weapons Safety Review and Weapon Safety Endorsement IAW JROCM 102-06 and DoDI 5000.69. Reference the Weapons Safety Guide in JCIDS Manual, Enclosure B, Appendix G, Annex H.

□ Section 11. Technology Readiness. Page B-C-22. Tech challenges that may impart program risk.

- □ **Identify** technology risk areas that require attention during Engineering, Management, and Development.
- □ For multiple increments, **describe** tech to be matured for each increment.
- □ For each CTE with a TRL less than 6, discuss potential **workarounds**, decision points and criteria.
- □ Address **Exportability** "Allied/Partner Interoperability and Coalition Use"

□ Section 12. DOTmLPF-P Considerations. Pages B-C-23 through B-C-24. Reference JCIDS Manual, Enclosure B, Appendix G, Annex F.

- □ **Outline** DOTmLPF-P changes required to implement the materiel capability solution.
- □ **Obtain** DOTmLPF-P endorsement.
- □ Address **all** DOTmLPF-P considerations in a CDD or state N/A.
- □ **Coordinate** with organizations to ensure endorsement is not withheld by missing information.
- □ **All** DOTmLPF-P considerations that are increment dependent must be clearly identified.
- □ Discuss DOTmLPF-P changes **enabling** implementing, ops, and support of the system.
- □ Discuss DOTmLPF-P changes required to **integrate** the system with fielded solutions.
- □ Cite **DCRs** that apply and provide status.
- □ Provide **details** of the recommended DOTmLPF-P changes and implementation plans.

□ Section 13. Program Cost. Pages B-C-24 and B-C-26.

- □ Identify the **overall** resources required including materiel and non-materiel lifecycle costs.
- □ **Cite** the cost caps from the APB for unit production and sustainment costs.
- □ Include Lifecycle cost data for **all increments** described in the CDD.
- □ Cite lifecycle cost analyses, conducted IAW **DoDI 5000.73**, including other cost models.
- □ **Include** Required Resources Table, Figure B-11. Include DOTmLPF-P and intel support.
- □ Describe **affordability** under expected 30-year TOA, including elimination of legacy capability.
- □ Generate **30-year "sand chart**" data IAW DoDI 5000.02. Provide in CDD or in KM/DS.

Appendices. Pages B-C-26 through B-C-28. Only A-F are permitted as defined. D counts for page limit. Submit additional information IAW JCIDS Manual, Enclosure A.

- □ Appendix A. References. **First entry** - Ensure architectures are discoverable.
- □ Appendix B. Acronym List. All acronyms in the document in **alphabetical** order
- □ Appendix C. Glossary. **Consistent** with AV-2.
  - □ Add **statement** "Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this document only."

- □ Appendix D. (Optional) Classified Appendix. Provided to the J8 SAPCO
  - □ If the document is not useful without this appendix, **classify** higher.
  - □ Indexed to **align** with the baseline document sections.
- □ Appendix E. **Reference** the Cyber Survivability Endorsement (CSE) Implementation Guide.
  - □ **Provide** Cyber Survivability Attribute (CSA) Table, Figure B-12
- □ Appendix F. If not in Section 5, **provide** EMS Survivability Risk Category, narrative, and attributes with thresholds and objectives. **Describe** IAW JCIDS Manual, Enclosure B, Appendix G, Annex C.
- □ Annexes A – Z. (Optional) Incremental Approach or FoS.

DoDAF Architecture Views. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B Figure B-26 and if the Net-Ready certification is applicable, additional views listed in Table B-29.

draft CDD.

There is no mandatory content for the dCDD in the JCIDS Manual; the MDA will determine the required content and will be directed by the SPR. The required sections will follow the format guidance for a full CDD.

CDD Update Checklist.

Pages A-A-16 and A-A-17. A CDD Update document is developed in the same format as the original validated CDD, unless there is an excessive period of time between documents requiring Certifications and Endorsements to be updated due to capability, threat, or mission changes, JPR/KPP attribute additions/deletions, or the current JCIDS Manual has mandatory requirements that shall be addressed. In this case, the original validated document will be updated to the most current JCIDS Manual for format and content and reviewed in its entirety.

A CDD Update is a stand-alone document. All changes/revisions to the CDD Update will be made in red font. If the updates are not significant as noted above, only the “red” font changes/revisions to the current version of the document will be commented on during the staffing process. The final version of the document will retain “red” text, to identify the changes. For subsequent updates, the document sponsor will change the font color of the previous update to black before making new updates." A “Summary of Change” page will be incorporated after the Executive Summary page to note all changes as in the example Figure A-15, page A-A-41. The Title Page content remains the same except for changing CDD to “CDD Update.”

CDD Annexes and Increments Checklist.

Pages B-C-A-2 and B-C-A-3. Each individual annex will include the same Sections as a CDD. Sections with no change to base document must be present but can state "No Change." Individual annexes are not to exceed 20 pages in length. Changes are noted below.

Body.

- □ Section 1. Operational Context. Provide updates.
- □ Section 2. Threat Summary. Provide updates.
- □ Section 3. Capability Discussion. Specify capabilities developed for the individual annex.
- □ Section 4. Program Summary. Provide updates. If an incremental approach is taken, describe the strategy taken to deliver the incremental capability.
- □ Section 5. Performance Attributes. Specify performance attributes specific to the increment or the individual system within the family. The capability solution specified by the annex will be a subset of what is required to meet the performance attributes of the overall system as identified in the base document.
- □ Section 6. Other System Attributes. Specify other system attributes specific to the increment or the individual system within the family. The capability solution specified by the annex inherits the attributes of the base document.
- □ Section 7. Interoperability. In the incremental approach, ensure the incremental capability meets the current standards at the time of validation. It is likely a new Net-Ready summary table will be required for each increment or individual system in an FoS. If applicable, update the intelligence interoperability requirements consistent with JCIDS Manual Enclosure B, Appendix G, Annex G.
- □ Section 8. Spectrum and E3 Control Requirements. Capture any additional spectrum and E3 control requirements for the increment or individual system.
- □ Section 9. Intelligence Supportability. Provide changes to the requirements or additional supportability requirements from the base document.
- □ Section 10. Weapon Safety Assurance. Provide changes from the base document.
- □ Section 11. Technology & Manufacturing Readiness. Specify the technology readiness and manufacturing readiness of the capability for the increment or individual system.
- □ Section 12. DOTmLPF-P Considerations. Describe additional DOTmLPF-P considerations.
- □ Section 13. Program Cost. Specify any updates to the base document.

DoDAF Architecture Views. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B Figure B-26 and if the Net-Ready certification is applicable, additional views listed in Table B-29.

IS-CDD Checklist.

Pages B-D-1 through B-D-8. Exceptions to CDD format and content are noted below.

Format.

- □ Cover. Identical to CDD except title reads, "Information Systems Capability Development Document for …"
- □ Validation, Waivers, Executive Summary. Identical to CDD.

Body. Six sections, with one being optional. No more than 45 pages long including a classified Annex, if used. See the regular CDD Section for content of the unchanged Sections.

- □ Section 1. Operational Context. No change.
- □ Section 2. Threat Summary. No change. Strongly **consider** cyber threats.
- □ Section 3. Capability Discussion. No change except:
  - □ **Provide** a table that describes the contribution this IS-CDD makes to the fulfillment of capability requirements described in the applicable ICDs or analysis as illustrated in Figure B-13.
  - □ **Consider** Responsible AI in capability descriptions.
- □ Section 4. Program Summary. No changes except **include** the IT Box.
- □ Section 5. Performance Attributes. No change except:
  - □ Performance attributes may be initial minimum values rather than threshold/objective values.
  - □ SS and Sustainment KPPs are **required**. **Address** Interoperability and Exportability.
- □ Section 6. Other System Attributes. Optional. But **consider** identifying the system categorization for IS and platform IT systems as a required capability.
- □ Section 7. Interoperability. No change except:
  - □ Summary table uses **initial minimum values** rather than threshold/objective as in Figure B-15.
- □ Section 8. Spectrum and E3 Control Requirements. No change.
- □ Section 9. Intelligence Supportability. No change.
- □ Section 10. Weapons Safety Assurance. Not required.
- □ Section 11. Technology and Manufacturing Readiness. **Verify** the planned capability is aligned with current IT and manufacturing levels, and not dependent on technology development.
- □ Section 12. DOTmLPF-P Considerations. No change.
- □ Section 13. Program Cost. No change except:
  - □ Required Resources Table contains programmed funding by year for software development and sustainment and for hardware refresh and integration, as shown in Figure B-16.
- □ Appendices. No change.

DoDAF Architecture Views. Required DoDAF views are listed in JCIDS Manual Appendix H to Enclosure B Figure B-26 and if the Net-Ready certification is applicable, additional views listed in Table B-29.

APPENDIX 3. RESPONSIBLE ARTIFICIAL INTELLIGENCE PRIMER

Artificial Intelligence enabled capabilities are changing the nature of warfare. They can significantly enhance warfighting capability and deliver performance improvements to existing and future Air Force systems. However, AI is evolving rapidly, has unique characteristics, creates new ethical challenges, and increases the risk of unintended consequences if not properly implemented. To address these concerns, DepSecDef issued a memorandum in May 2021 that established the DoD's holistic, integrated, and disciplined approach to RAI.[1] The memo introduced five DoD AI Ethical Principles (Responsible, Equitable, Traceable, Reliable and Governable). It is important to note that the DoD AI Ethical Principles apply to all DoD AI capabilities, of any scale, including AI-enabled autonomous systems, for warfighting and business applications. Sponsors will consider the AI Ethical Principles in all acquisition pathways as soon as an AI-enabled capability has been identified as a potential solution.

The DepSecDef memo also presented six tenets to guide the implementation of RAI across DoD. The RAI Requirements Validation tenet is of particular interest to AFF and is the driver for including RAI information in our guidebooks. The RAI Requirements Validation tenet is defined as:

- Incorporate RAI into all applicable AI requirements, including joint performance requirements established and approved by the Joint Requirements Oversight Council, to ensure RAI inclusion in appropriate DoD AI capabilities.

To support RAI implementation across the Air Force, we anticipate more specific policy guidance and digital tools will be provided by DoD Chief Digital and AI Office (CDAO) in the coming years.[3] In the absence of explicit policy guidance and digital tools, prior to Solution Pathway Review, if possible, sponsors should attempt to document any efforts to comply with the RAI Requirements Validation tenet and each of the DoD RAI Ethical Principles. We encourage interested parties to consult SAF/CND subject matter experts for guidance on the other five tenets.

AI-enabled capabilities continue to mature and offer unique solutions to military capability gaps that have previously been unattainable. The Air Force must integrate these offerings responsibly. RAI allows us to guard against AI-enabled capabilities that are applied unethically or irresponsibly. With this approach developers and users will have appropriate levels of trust in AI systems thus enabling rapid adoption and operationalization to strengthen our competitive edge.

An RAI checklist is provided below with additional items to consider when AI offers a viable solution to your military problem. For questions and/or assistance regarding RAI and AI-enabled capabilities please contact AF/A5DQ (AI CDT):

- Responsible: DoD personnel will exercise appropriate levels of judgement and care, while remaining responsible for the development, deployment, and use of AI capabilities.

  Recommendation: Ensure an accurate and data-informed description of why AI is an appropriate solution for the problem is captured. Clearly document relevant design choices and considerations. Thoroughly describe the intended system functions and the conditions they can expect to be met, with consideration for level of human interaction and reliance on machines.

- Equitable: The Department will take deliberate steps to minimize unintended bias in AI capabilities.

  Recommendation: Ensure an equitable approach to AI-enabled capabilities is described. Stakeholders should ensure a broad and diverse group of data is considered to prevent cognitive bias. Ensure training data represents ALL options and is distributed fairly, the system is tested in

a variety of contexts and evaluate whether the system disproportionally weights input to optimize for specific scenarios that may unjustly skew the outcome.

- Traceable: The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of technology, development processes, and operational methods applicable to AI capabilities, including transparent and auditable methodologies, data sources, and design procedures and documentation.

  Recommendation: Document efforts to trace AI-enabled system performance to design decisions and specifications. The system should log sufficient activity for audits, produce outputs for justification, provide confidence levels for decisions, leverage integration testing to show causal relationships, and deliver clear functionality without degrading performance.

- Reliable: The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across AI capabilities' entire life-cycle.

  Recommendation: Risk analysis of the intended system tasks should be performed. This should be well documented to ensure both common and edge cases[2] are evaluated, and the system is designed to work well in both scenarios. Tests of the algorithms, system functions, and overall system under a variety of scenarios should be planned to characterize issues as they are discovered. Most importantly for AI-enabled systems, data processes must be completed in a disciplined manner and aligned with best practices.

- Governable: The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.

  Recommendation: Ensure intended functions of the AI-enabled capability are clearly documented. Describe how the behaviors of the system will be explained and mechanisms for de-activation if undesired or harmful behavior is observed. Include test plans designed to detect anomalies, ensure the system is working as planned, and allow testing of edge cases.

For questions and/or assistance regarding RAI and AI-enabled capabilities please contact AF/A5DQ (AI CDT).

RAI Checklists

The below are recommended items to consider for AI-enabled capability development. The ability to answer yes to these questions does not guarantee but increases the likelihood that the program will comply with anticipated RAI policy, governance, and oversight constraints.

Item #	Responsible	Yes/No
1	Have other alternatives to AI as a capability enabler been considered?	
2	Are there designated roles/persons with the power to make and certify necessary changes to AI-enabled capability?	
3	Are there clearly delineated organizations or entities responsible for overseeing AI system's phases: Data management, Model development, Model deployment, User employment, Post-deployment?	
4	Has the sponsor identified the intended range of tasks the AI system will perform autonomously and associated risk?	
5	Are there clearly defined tasks to be performed by the AI vs. the human?	
6	Will the AI system replace human decision-making?	
7	Will AI system make ethical, legal, or moral decisions that a human would make?	
8	Will the AI system be used in coordination with Allies & partners (A&P)?	
9	Is the AI system to be used in coordination with A&P consistent with their norms and shared values?	
10	Have the system functions, data needs, and operational conditions been defined?	
11	Is there a plan for disciplined AI/ML DevSecOps?	
12	Is there a plan to prevent the intentional or unintentional manipulation of the data or trained model?	
13	Has the entity responsible for the plan specified in item # 12 been identified?	
14	Has DODI 3000.09 approval process been considered if involving lethal effect?	
15	Is the AI solution registered in DoD Chief Digital and AI Office (CDAO) repository? *Note:* currently not available, in development with anticipated deliver ~2 years.	N/A

Item #	Equitable	Yes/No
1	Have domain experts been consulted to articulate potential biases in the domain where the AI system will be used?	
2	Have a variety of historical and cultural contexts been considered?	
3	Have data analytics been used to fully understand the dataset distribution?	
4	Is there a plan to assess AI system likelihood and magnitude of potential harm from unintended bias?	
5	Does the dataset perpetuate an unreasoned and unfair distortion of judgment in favor of or against a person or a thing?	
6	Is the dataset specific information from item # 5 understood and available to decision makers?	
7	Has it been considered to what extent the AI system may disproportionately weigh input features that unjustly skew outcomes? i.e., take the step to ensure you didn't start with a biased dataset that results in an unjust outcome.	

Item #	Traceable	Yes/No
1	Are the qualities and limitations of training data (including synthetic dataset) well-understood and appropriate for expected operating conditions?	
2	Is it possible to determine the causal chain between inputs and outputs of the AI system i.e., is it an explainable system or a "black box" system?	
3	Is the AI system able to explain causal relationships for outcomes to end users?	
4	Is the AI system able to provide the end user with the perceived confidence of the output?	
5	Is there a plan for the AI system to log sufficient activity in the right format to perform an audit?	
6	Is there a plan to leverage a simpler model architecture for the AI system, a more explainable trained model while still providing the needed capability?	
7	Is there an appropriate plan/interface to verify individual outputs of the system?	

Item #	Reliable	Yes/No
1	Has the sponsor identified the intended range of tasks the AI system will perform?	
2	Has the sponsor adequately conveyed to the end user the limitations of AI system's reliability?	
3	Is there a plan to assess data inputs qualitatively and quantitatively to protect against interference/manipulation?	
4	Is there a plan to document procedures and reporting processes of AI system's performance and post deployment monitoring?	
5	Has the responsible entity been identified for the plan specified in item #5?	
6	Have potential edge cases been identified?	
7	Has the risk of operations outside of the intended environment been adequately defined?	
8	Has the end user established clear performance metrics needed to deploy the AI system for the intended purpose?	
9	Is there a plan to align application of model with origin of models/packages, domain deployment, performance, and breadth of deployment?	
10	Is there a Test, Evaluation, Verification, and Validation (TEVV) plan for the AI system's intended functions under specified operating conditions?	
11	Is there a plan to validate the AI system's ability to detect unintended consequences?	

Item #	Governable	Yes/No
1	Is there a plan to monitor whether the AI system is being used for its intended function, and under the specified operating conditions?	
2	Is there a plan to rollback AI system malfunctions?	
3	Is there a plan to deactivate AI system as required?	
4	Is there a plan for AI system to identify performance deviation and present it to appropriate decision makers for correction?	
5	Will the decisions or actions made by AI system be apparent and provide sufficient explanation to end user(s)?	
6	Is there a plan to provide an account of how the AI system will resolve edge cases?	
7	Is there a plan to develop appropriate training and documentation to help end user understand AI system's function, risks, performance expectations, and potential harms?	
8	Is there a plan to document and clearly communicate data policies, risks, and testing results to the sponsor and end user?	
9	Is there a plan to catalogue sensitivity of training/deployment data?	
10	Is there a strategy in place to protect sensitive data?	

References:

1. Deputy Secretary of Defense Memorandum, 26 May 2021, Implementing Responsible Artificial Intelligence in the Department of Defense.

2. Edge case – in AI terms refers to rare events or extreme situations that may only be identified in real world situations.

3. Chief Digital and Artificial Intelligence Office. "U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway." Chief Digital and Artificial Intelligence Office, Department of Defense, June 2022, www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf.