

#### 4. ICD

##### a. Background

(1) The purpose of an ICD is to document capability requirements and traceability to the UCP-assigned missions, OPLANs/CONPLANs, Support for Strategic Analysis (SSA) Products, CONOPS, and other driving factors for the capability requirements, quantify capability gaps and operational risk across the Joint force based upon the identified capability requirements, and propose materiel and/or non-materiel approaches to closing or mitigating the identified capability gaps. The document serves as the basis for validation by the appropriate validation authority identified in Enclosure D of this Manual.

(2) An ICD supports the acquisition process at several points, including the MDD; the AoA or other analysis, as required; update of the DOD Enterprise Architecture, development of the solution architecture; the Technology Development Strategy (TDS); and the Milestone (MS) A acquisition decision.

(3) An ICD is not always required before creating successor documents – CDDs, CPDs, or Joint DCRs – if alternative studies or documentation sources make the ICD redundant. In cases where the Sponsor proposes to proceed directly to a successor document, the general content of the ICD, including capability requirement and capability gap tables, will be provided in the successor document.

(4) For capability requirements likely to be addressed by IS solutions – software development, and off-the-shelf hardware if required, should consider the IS-ICD variant detailed in the next section of this Enclosure. For capability requirements likely to be addressed by a mix of IS and non-IS solutions, the regular ICD format should be used and an IS-CDD considered after ICD validation to streamline the IS portion of solution development.

##### b. Format

(1) Cover Page. The cover page of an ICD shall include the following information.

(a) Classification.

(b) Title, starting with the phrase “Initial Capabilities Document for...”

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New ICDs, and modifications to previously validated ICDs, must be endorsed by the Service, CCMD, or other DOD Component J8 equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of Requirements Management Certification Training (RMCT) in accordance with Enclosure H.

(f) Proposed validation authority.

(g) Proposed MDA.

(h) Proposed JSD.

(2) Executive Summary. An executive summary, not to exceed 1 page, shall follow the cover page and precede the body of the ICD.

c. Document body. The body of the ICD shall have the following five sections, and shall be no more than 10 pages long.

(1) Operational Context

(a) The purpose of this section is to provide context for the capability requirements identified in the ICD, and to provide appropriate traceability to the UCP-assigned missions, OPLANs/CONPLANs, SSA Products, CONOPS, and other driving factors for the capability requirements. This information facilitates review and validation of the ICD from the standpoint of how the capability requirements contribute to the overarching missions and activities of the Joint force.

(b) Describe the range of military operations being addressed and the relevant parts of SSA Products, Joint Concepts, CONOPS, Unified Command Plan (UCP)-assigned mission and/or other driving factors to which the capability requirements identified in the ICD contribute. If operations in, or after exposure to, Chemical, Biological, Radiological, or Nuclear (CBRN) environments are required, discuss how and where this fits in the operational context.

(c) Identify the timeframe under consideration for IOC and FOC based on input from supported/supporting CCMDs and the acquisition community.

(d) Identify what operational outcomes are required; what effects must be produced to achieve those outcomes; how they complement the integrated joint/multinational warfighting force; and what enabling capabilities are required to achieve the desired operational outcomes.

(e) Include the High-Level Operational Concept Graphic (OV-1). Other than the OV-1, do not include other architecture data in this section unless specifically referenced for illustration purposes elsewhere in the body of the ICD.

## (2) Threat Summary

(a) The purpose of this section is to provide context for the capability requirements identified in the ICD, and to provide appropriate traceability to the threat assessments used during the development of the capability requirements and identification of associated capability gaps. This information also enables threat validation as part of the intelligence certification provided during ICD review and validation, and facilitates more rapid review and updating of successor documents when/if threat assessments are updated.

(b) Cite the threat assessments used during the development of the capability requirements identified in the ICD.

1. For ICDs likely to result in Acquisition Category (ACAT) ID programs, ensure the most current DIA-validated threat analysis and findings are used to develop the ICD and any associated studies or analysis.

2. For all other ICDs, ensure the most current DIA- or Service-validated threat documents are used to develop the ICD and any associated studies or analysis.

(c) Provide a general description of the expected operational environment, including specific threat capabilities, the nature of existing and anticipated threats (both lethal and non-lethal), and threat tactics, if available. Include CBRN threats if applicable to the operational context. Ensure judgments or extrapolations regarding adversarial capabilities are appropriate, logical, and consistent with existing DIA- and Service-validated assessments. Also consider threats to follow-on research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts. Note that threats are factors that an adversary can control and direct, or will be able to direct, and do not include environmental or natural factors such as weather or terrain.

(d) See Appendix I of this Enclosure for intelligence related considerations which are applicable to other sections of the ICD.

## (3) Capability Requirements and Gaps/Overlaps

(a) The purpose of this section is to both identify the specific capability requirements, with associated JCAs and operational attributes, and to assess capability gaps and/or redundancies in terms of a comparison between capability requirements and current/projected force capabilities.

(b) In separate paragraphs, describe the capability requirements as identified during the CBA or other study. Explain why the capability requirements are essential to the Sponsor in order to achieve assigned goals and objectives. This discussion should relate capability requirements to the Operational Context outlined in Section (1) of the ICD. Address compliance with any applicable DOD, joint, national, and international policies and regulations.

1. Define capability requirements in the lexicon established for the JCAs, the tasks, standards, and conditions from the applicable Universal Joint Tasks or DOD Component equivalents, the relevant range of military operations, and the timeframe under consideration.

2. Describe capability requirements in terms of the required operational attributes with appropriate quantitative parameters and metrics, e.g., outcomes, time, distance, effect (including scale), obstacles to be overcome, and supportability. Indicate the minimum value below which the capability will no longer be effective. "TBD" values are not allowed. Appendix A to this Enclosure provides examples of appropriate attributes which should be used where applicable, although other attributes may be identified and used when those in Appendix A to this Enclosure are not appropriate.

3. Capability requirements should be general enough so as not to prejudice decisions in favor of a particular capability solution but specific enough to evaluate alternative approaches to achieve the capability.

4. Capability requirements shown in this section need only be those requirements which have associated gaps or overlaps/redundancies. This does not preclude the inclusion of capability requirements which are currently satisfied by capability solutions and do not have associated capability gaps, if inclusion of such capability requirements provides necessary context or serves other purposes. (i.e. – a capability requirement might be satisfied by a fielded capability solution, but the Sponsor proposes a much more cost effective capability solution or a consolidation of multiple independent solutions into a single common capability solution.)

(c) For each capability requirement identified, describe the capability gaps or overlaps in terms of the difference between the capability requirements enumerated above and the performance levels of current and projected force capabilities. Identify those capability requirements for which there exist overlaps or redundancies. Include considerations of capabilities in

other DOD Components, Interagency, and Allied/Partner nations. Assess whether the overlap is advisable for operational redundancy, or if the overlap should be evaluated as potential tradeoffs to satisfy identified capability gaps.

1. When describing "current capabilities" in the narrative paragraphs in order to assess the gap between the proposed capability requirements and current state of the art, one must consider all programs of record and rapidly fielded capability solutions in the joint force. One cannot exclude viable capability solutions from the comparison because they are not the preferred solution of the authoring organization, or because they are developed and operated by another DOD Component.

2. When describing a recapitalization (or "next generation") situation, the "current capabilities" must consider the capability solution being replaced, as well as other viable solutions as noted above, even though the plan may be to retire the older solution as the new solution becomes available. Life extension or continuing/restarting production of the existing capability solution, or possibly leveraging portions of existing capability solutions, may be part of tradeoff discussions and/or follow-on AoA activities.

(d) Clearly identify how each capability gap identified impacts the operational context in section (1) of the ICD, in terms of inability to execute part of all of an operational plan and/or unacceptable levels of operational risk. Where workarounds are feasible until the requirements proposed in the ICD are satisfied by capability solutions, identify the workarounds and operational risk(s) associated with them.

(e) Summary table. Provide a summary table for the relationship between capability requirements in each JCA and relevant attributes, and associated gaps/overlaps with respect to current or programmed force capabilities in a table as shown in Table B-1. The example table shown is intended to be illustrative, and may be tailored as long as it still clearly articulates both the capability requirements and the difference between those requirements and the current/programmed Joint force.

Capability Requirements			Current Capabilities (documents basis for gap/overlap)	
Capability Requirements	Attribute/ Metric	Minimum Value	Source/ System	Value
(for example) JCA 2.1: Battlespace Awareness / ISR				
Capability 1			Description	
	Attribute 1.1	Value (no TBDs)		Value (no TBDs)
	Attribute 1.n	Value (no TBDs)		Value (no TBDs)
(for example) JCA 3.1: Force Application / Maneuver				
Capability 2			Description	
	Attribute 2.1	Value (no TBDs)		Value (no TBDs)
	Attribute 2.n	Value (no TBDs)		Value (no TBDs)
(for example) JCA 3.2: Force Application / Engagement				
Capability 3			Description	
	Attribute 3.1	Value (no TBDs)		Value (no TBDs)
	Attribute 3.n	Value (no TBDs)		Value (no TBDs)
JCA X.x: TBD / tbd				
Capability n			Description	
	Attribute n.n	Value (no TBDs)		Value (no TBDs)

Table B-1. Example Capability Requirement and Gap/Overlap Table

(4) Assessment of Non-Materiel Approaches

(a) The purpose of this section is to identify what non-materiel approaches have been considered to close or mitigate capability gaps identified in Section (3) of the ICD, and what capability gaps may require a materiel solution. This information also informs the DOTmLPF-P review and endorsement conducted during staffing of the document.

(b) Summarize the changes to DOTmLPF-P considered during the CBA or other analysis that would satisfy the capability gaps in part or in whole. Include consideration of capabilities in Allied/partner nations, the interagency, and other DOD Components.

(c) If there is an issue of sufficiency in existing or projected capability (not enough units of capability to be effective) without requiring increased proficiency in existing or projected capability (not enough performance in each unit of capability), capture the assessment of “little-m” quantity changes in this section.

(5) Final Recommendations

(a) The purpose of this section is to identify one or more paths forward to satisfy the capability requirements and close or mitigate associated capability gaps identified in the document.

(b) Identify DOTmLPF-P recommendations to be considered as part of a materiel solution.

(c) Identify DOTmLPF-P recommendations to be considered independent of a materiel solution.

(d) For all capability requirements that cannot be met using non-materiel approaches, make specific recommendations on the type of materiel approach preferred to close each capability gap, which may be used by the MDA to adjust the scope of the AoA:

1. Enhancement of an existing capability solution. Enhancing an existing system includes development and fielding of IS, development of similar technologies to address high obsolescence rates, or evolution of the system through significant capability improvements.

2. Replacement or recapitalization of an existing capability solution. ICDs will describe a plan to retire (sunset) an existing system as the new capability or version of legacy system is brought into service, and whether quantities should be reduced based on the increase in capability for the new system.

3. Development of a new capability solution. New capability solutions differ significantly in form, function, and operation from existing capability solutions. They may address gaps associated with a new mission, or describe breakout capabilities that offer significant improvement over current capabilities, possibly transforming the ways of accomplishing an existing mission.

(e) As appropriate for each recommendation, provide a uniform resource locator (URL) for required architecture data identified in Table B-F-3 in accordance with references j, ss, and qq.

d. Appendices

- (1) Appendix A: References.
- (2) Appendix B: Acronym List.
- (3) Appendix C: Glossary.

(INTENTIONALLY BLANK)

## 5. IS-ICD

### a. Background

(1) The purpose of an IS-ICD is the same as for a regular ICD, but implements the “IT Box” model, outlined in this section, to provide IS programs greater flexibility to incorporate evolving technologies, and achieve faster responses from requirement validation processes than is typical for other kinds of materiel or non-materiel solutions. The document serves as the basis for validation by the appropriate validation authority identified in Enclosure D of this Manual.

(2) The “IT Box” model calls for fewer iterations of validating documents through the JCIDS process by describing the overall IS program in the IS-ICD, and delegating validation of detailed follow-on requirement and solution oversight to a flag-level organization other than the JROC or JCB.

(a) Using identified measures of effectiveness (MOEs), initial minimums are used instead of thresholds/objectives, allowing for rapid capability development within specified funding limits.

(b) CDDs and CPDs are generally not required as successor documents to an IS-ICD, and the delegated authority may prescribe alternative document formats most appropriate to the follow-on efforts.

1. Alternative documents must be provided to the KM/DS system for information purposes and visibility in the Joint portfolios. An example of Sponsor documents used for managing follow-on efforts is provided later in this section, but is not intended to limit potential flexibilities provided by the IS-ICD, or a previously validated ICD or CDD which the validation authority has approved for transition to the IT Box model.

2. IS programs that are designated as MDAPs must have a validated CDD even if authority to use alternate document formats has been delegated by a preceding IS-ICD.

(3) IS-ICDs are used to document capability requirements and associated capability gaps where the intended solution approach involves research, development, and acquisition of applications system software, and the projected software development costs exceed \$15 million. IS with development costs less than \$15 million are not required to use the JCIDS process.

(a) It is not intended to be used for software embedded as a subset of a capability solution developed under other validated documents.

(b) All hardware associated with an IS-ICD is COTS/GOTS, and hardware development is restricted to that necessary for system integration, system enhancements, and hardware refresh due to obsolescence.

(4) Efforts in an IS-ICD may include:

(a) The procurement or modification of commercially available products and technologies from domestic or international sources, or the development of dual-use technologies.

1. COTS/GOTS software, and associated hardware, without modification.

2. Commercial capability solutions with integrated, DOD-specific performance characteristics/standards.

(b) The additional production or modification of previously-developed U.S. and/or Allied military or Interagency systems or equipment. Increases in quantities of unmodified existing systems which remain within the scope of the validated IT Box may be accomplished without validation of new documents.

(c) Development, integration, and acquisition of customized application software.

(5) Sponsors shall use the IS-ICD format when applicable for JROC Interest and JCB Interest documents drafted after the effective date of this Manual. Sponsors are encouraged to use and validate IS-ICDs for situations where the Sponsor is the validation authority.

(a) For existing programs that have validated ICDs or CDDs, but want to transition to the IT Box model, an amendment to the existing document and revalidation, documented in a new JROC Memorandum (JROCM), is necessary to delegate JROC or JCB requirements oversight authority.

(b) Defense Business Systems capabilities which are defined and acquired in accordance with reference dd, are not required to use the IT Box model or IS-ICD document format.

(6) Revalidation. IS-ICDs require revalidation if the Sponsor proposes to:

(a) Add new capability requirements beyond the scope of the validated IS-ICD.

(b) Increase programmed development and integration funding for a MAIS program by 10% or more compared with the desired level of funding identified in the IS-ICD.

(7) Biennial FCB Review. For all IS programs with a valid IS-ICD, the lead FCB shall receive a brief every second year following the validation. The lead FCB will determine if the JROC or JCB should review the following briefing items, and will make appropriate recommendations for action.

(a) Progress in delivering capability solutions within the required timeframe and available funding.

(b) Compliance with applicable enterprise architecture and data standards.

(c) Other items identified by the IS-ICD validation

b. Format

(1) Cover Page. The cover page for an IS-ICD shall be the same as for a regular ICD except that the title will begin with the phrase “Information Systems Initial Capabilities Document for...”

(2) Executive Summary. The executive summary for an IS-ICD is the same as for a regular ICD.

c. Document body. The body of an IS-ICD differs from a regular ICD in two sections, and shall be no more than 11 pages long. See the regular ICD section for content of the unchanged sections.

(1) Capability Requirements and Gaps/Overlaps – ICD Section (3). Define the proposed capability requirements and initial minimum levels in terms of measures of effectiveness (MOEs). Describe capability gaps in terms of the difference between the proposed capability requirements and similar existing capabilities, if any.

(2) Final Recommendations (ICD Section 5). With the capability requirements making up one side of the IT Box, briefly discuss the remaining sides of the IT Box, illustrated in Figure B-2.

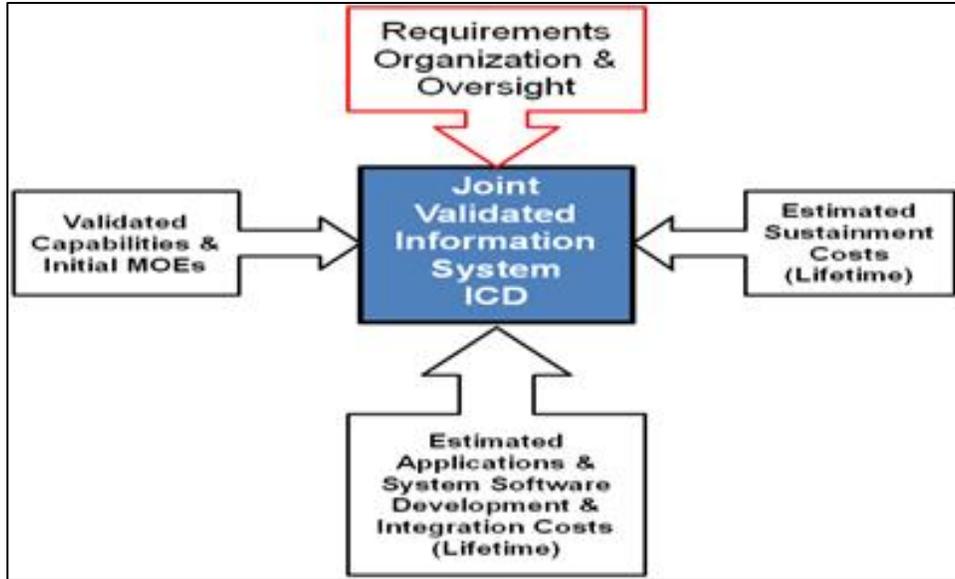


Figure B-2. Components of the “IT Box” model in IS-ICDs

(a) Identify the proposed flag-level oversight body, the chair of that body, and the organizations represented on the body to receive delegated requirements oversight duties.

(b) Show estimated development and integration as well as sustainment costs over the life cycle of the program. Break out costs into annual estimates as shown in Table B-2.

	<b>FY xx (e.g. 12)</b>	<b>FY xx (e.g. 13)</b>	<b>FY xx (e.g. 14)</b>	<b>FY xx (e.g. 15)</b>	<b>FY xx (e.g. 16)</b>	<b>FY xx (e.g. 17)</b>	<b>FYDP Total</b>	<b>Life Cycle Cost</b>
Development & Integration Costs								
Sustainment Costs								

Table B-2. Example Cost Summary Table for IS-ICDs

d. Appendices. The appendices for an IS-ICD are the same as for a regular ICD.

e. Example of managing an IS program using an IS-ICD

(1) As the standard CDD and CPD documents are not typically required, an IS-ICD provides Sponsors the flexibility manage IS programs with alternate documents and validation processes as necessary, as long as the program remains within the boundaries of the validated IS-ICD and any additional guidance provided by the delegated validation authority.

(2) The following example of documents used for managing follow-on efforts are intended to be illustrative, and are not intended to limit potential flexibilities provided by the IS-ICD, or a previously validated ICD or CDD which the validation authority has approved for transition to the IT Box model.

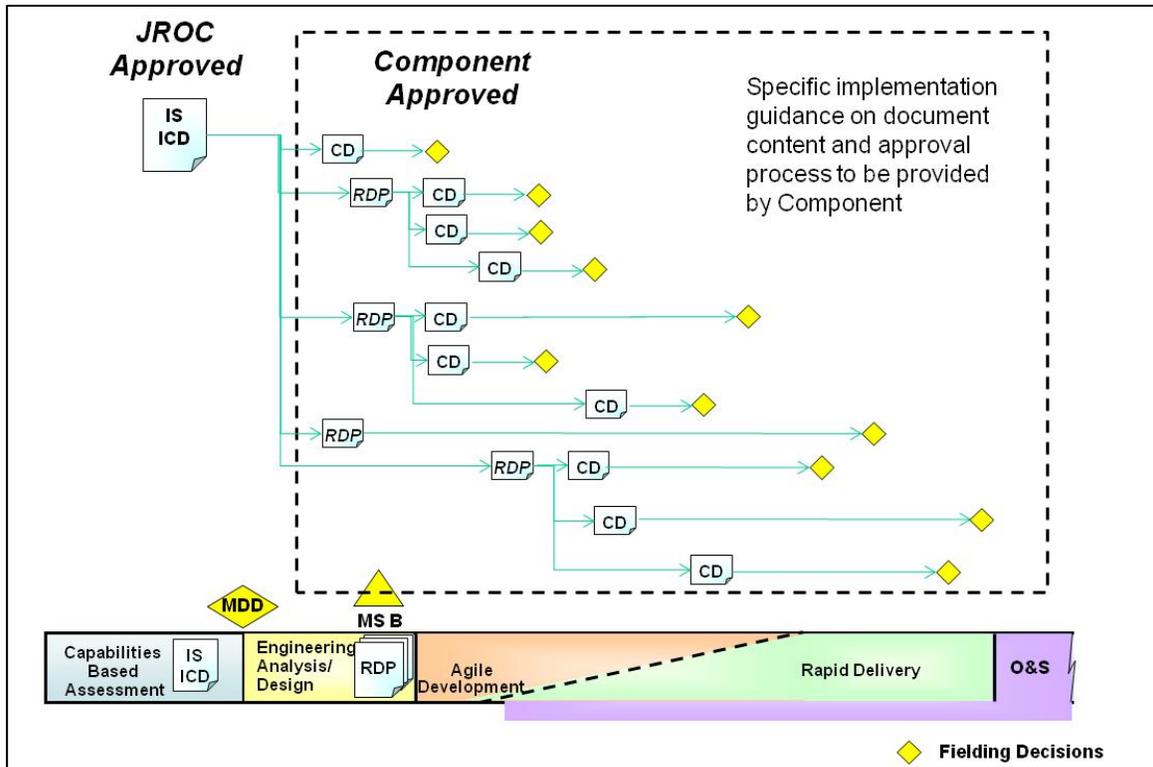


Figure B-3. Example of IS-ICD Follow-on Documents

(3) For the purpose of this example two document types have been created and illustrated in Figure B-3. The Requirements Definition Package (RDP) and the Capability Drop (CD). Actual names, content and approval process are to be determined by the delegated validation authority.

(4) The RDP is a first level decomposition of one or more capability requirements in the IS-ICD, and is co-developed between the operational user (or representative) and the program office. One or more RDPs together would represent the total set of capability solutions developed to satisfy the capability requirements in the IS-ICD.

(a) The RDP would identify the KPPs (including the NR-KPP), Key System Attributes (KSAs), and/or additional performance parameters as necessary to scope and cost a specific solution implementation. The RDP may also identify non-materiel changes that need to be implemented to fully realize the IS capability. The RDP would be supported by an Information Support Plan (ISP), submitted separately to DOD Chief Information Officer (DOD CIO) for certification purposes, in accordance with reference rr. This would be the

equivalent of a CDD as defined in the typical JCIDS process, and would be approved by the delegated validation authority identified in the IS-ICD.

(b) A draft RDP could be used before validation to support MS A decisions for IS technology/prototyping efforts. The RDP would be submitted to the delegated validation authority for validation ahead of a MS B decision. Following validation, the RDP would be posted to the KM/DS system for information purposes and for visibility into the appropriate FCB portfolio.

(c) The RDP can then be used in multiple ways. It can be used to initiate an IS program to develop, test, and deliver the full capability defined in the RDP. It can also be used as a basis for defining multiple drops of incremental capabilities such as “apps” or “widgets” which could be documented in something like a CD.

(d) If an IS program has a projected cost such that it is designated an MDAP, the requirements document must be written as a CDD and approved by the JROC to comply with statute.

(5) The CD could be a much lower level document to specify the detailed characteristics of a “widget” or “app” necessary for partial deployment of the capability solution. It could be developed through a rapid prototyping effort with the user to ensure it meets their needs. A CD could be developed directly from the definitions in the ICD in the event of a more urgent need for the capability. More commonly, multiple CDs would be derived from an RDP to deliver all of the capabilities defined in the RDP.

(a) The CD should include information such as a detailed technical description of the capabilities provided by a “widget” or “app” that can be developed and fielded within a short period of time, along with specific technical performance requirements. If not already covered by the ISP approved for the RDP, the CD is supported by a separately submitted ISP for certification purposes in accordance with reference rr.

(b) The approval of CDs would most likely be delegated to a lower level requirements authority as determined by the RDP authority to ensure timely decision making.

(6) Deployment decisions are made whenever the product - whether from an RDP or a CD - is ready for deployment to the user.

6. Joint DCR

a. Background

(1) The purpose of a Joint DCR is to provide traceability to predecessor documents, or identify capability requirements and gaps in cases where there are no predecessor documents, as well as to propose non-materiel capability solutions as an alternative to, or complement of, materiel capability solutions. The document serves as the basis for validation by the appropriate validation authority identified in Enclosure D of this Manual

(2) An ICD waiver is not required prior to generating a Joint DCR without a preceding ICD.

(3) Joint DOTmLPF-P Functional Process Owners (FPOs). FPOs are designated by the CJCS for each of the DOTmLPF-P areas, and are responsible for their respective joint functional processes and overseeing implementation of the recommended changes from Joint DCRs. FPOs provide advice to Sponsors of Joint DCRs and assessment of their specific functional process during their review of proposed Joint DCRs. They also support the GO/FO Integration Group and the JCB/JROC in executing their integration and implementation responsibilities for validated Joint DCRs. The FPOs are listed in Table B-3.

<b>DOTmLPF-P Area</b>	<b>Functional Process Owner</b>
Joint Doctrine	Joint Staff/J-7
Joint Organizations	Joint Staff/J-8 (with J-1 & J-5 support)
Joint Training	Joint Staff/J-7
Joint Materiel	Joint Staff/J-8
Joint Leadership and Education	Joint Staff/J-7
Joint Personnel	Joint Staff/J-1
Joint Facilities	Joint Staff/J-4
Joint Policy	Joint Staff/J-5

Table B-3. Joint DOTmLPF-P FPOs

b. Format

(1) Cover Page. The cover page of a Joint DCR shall include the following information.

(a) Classification.

(b) Title, starting with the phrase “Joint DOTmLPF-P Change Recommendation for...”.

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New Joint DCRs, and

modifications to previously validated Joint DCRs, must be endorsed by the Service, CCMD, or other DOD Component J8 equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure H.

(f) Proposed lead organization. Defines a single organization, which may be different from the document Sponsor, which will have responsibility for coordinating the proposed changes, and if applicable, the activities of other Office(s) of Primary Responsibility (OPR) assigned to specific recommendations within the Joint DCR.

(2) Executive Summary. An executive summary, not to exceed 1 page, shall follow the cover page and precede the body of the Joint DCR.

c. Document body. The body of the Joint DCR shall have the following five sections, and shall be no more than 30 pages long.

(1) Operational Context

(a) The purpose of this section is to provide context for the DOTmLPF-P change recommendations addressed by the Joint DCR, and to provide appropriate traceability to the UCP-assigned missions, OPLANs/CONPLANs, SSA Products, CONOPS, and other driving factors for the change recommendations. This information facilitates review and validation of the Joint DCR from the standpoint of how the change recommendations address or enable solutions to validated capability requirements and contribute to the overarching missions and activities of the Joint force.

(b) If the Joint DCR is a successor document to one or more previously validated requirements documents:

1. Cite the validated source documents which identified the capability requirements addressed or enabled by the Joint DCR, and ensure that any source documents not already present in the KM/DS system are provided to the Gatekeeper for reference purposes.

2. From the source document(s), summarize the operational context(s) associated with the validated capability requirements addressed or enabled by the Joint DCR. Ensure that any changes to operational context(s) which have occurred since the original validation of the capability requirements are addressed in this section.

3. If applicable to changes recommended in the Joint DCR, include the OV-1. Other than the OV-1, do not include other architecture data in this section unless specifically referenced for illustration purposes elsewhere in the body of the Joint DCR.

(c) If the Joint DCR is not based upon a previously validated requirements document, provide the operational context as outlined for Section (1) of an ICD. If applicable, ensure this section includes reference to relevant JROCMs, CCMD IPLs, joint monthly readiness reviews, quarterly reports to the Secretary of Defense, etc., that relate to the change recommendations.

(2) Threat Summary

(a) A threat summary is not applicable to all Joint DCRs, depending upon the nature of the change recommendations. When applicable, the purpose of this section is to provide context for the capability requirements addressed or enabled by the Joint DCR, to provide appropriate traceability to the threat assessments used during refinement of the capability requirements during development, and to describe any updates to threat assessments which have occurred since the original validation of the capability requirements. When applicable, this information also enables threat validation as part of the intelligence certification provided during Joint DCR review and validation, and facilitates more rapid review and updating of successor documents when/if threat assessments are updated.

(b) If the Joint DCR is a successor document to one or more previously validated requirements documents:

1. Cite the latest threat assessments applicable to the capability requirements addressed or enabled by the Joint DCR. Ensure the applicable threat information has been updated since the original validation of the capability requirements, considering evolving threats identified in the most current threat analysis and findings.

a. For Joint DCRs enabling or otherwise associated with ACAT ID programs, ensure the most current DIA-validated threat analysis and findings are used to develop the Joint DCR and any associated studies or analysis.

b. For all other Joint DCRs where threat assessments are applicable, ensure the most current DIA- or Service-validated threat analysis and findings are used to develop the Joint DCR and any associated studies or analysis.

2. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed or enabled by the Joint DCR.

(c) If the Joint DCR is not based upon a previously validated requirements document, provide the threat summary as outlined for Section (2) of an ICD.

(d) See Appendix I of this Enclosure for intelligence related considerations which are applicable to other sections of the Joint DCR.

### (3) Capability Discussion

(a) The purpose of this section is to identify the validated capability requirements addressed or enabled by the Joint DCR, and to outline the results of related studies or analysis performed to define the change recommendations.

(b) If the Joint DCR is a successor document to one or more previously validated requirements documents, provide an overview of the validated capability requirements addressed or enabled by the Joint DCR.

(c) If the Joint DCR is not based upon a previously validated requirements document, provide the capability requirement and capability gap information outlined for Section (3) of an ICD. Clearly state, in terms of major objectives, what the recommendation is intended to accomplish and how it could widen the qualitative superiority of joint forces over potential adversaries, or otherwise enhances joint and multinational warfighting capabilities.

(d) Summarize all related analyses and/or studies (i.e., AoA and/or other supporting analysis) conducted to develop the change recommendations. Include the alternatives, objective, criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in the KM/DS system are provided to the Gatekeeper for reference purposes.

### (4) Change Recommendations and Implementation Plans

(a) The purpose of this section is to outline the specific change recommendations and implementation plans in one or more DOTmLPP-P areas to address or enable capability solutions to satisfy the validated capability requirements and associated capability gaps, and to identify related interdependencies which must be satisfied to provide a successful capability solution.

(b) Use this section to describe change recommendations in terms of each applicable joint DOTmLPPF-P area.

(c) For each change recommendation to a DOTmLPPF-P area, outline the recommended change and proposed implementation plan, including:

1. Proposed OPR and rationale.
2. Changes to tactics, techniques, and procedures and/or implications on the safe use of the proposed non-materiel solution in the proposed operating environment.
3. Forces and systems affected and impact on interoperability. As appropriate for each recommendation, provide a URL for required architecture data identified in Table B-F-3 in accordance with references j, ss, and qq.
4. If recommendation includes incorporating future technology (materiel component), include brief discussion of the maturity of the science and technology area(s) or future systems involved and a risk assessment of the approach.
5. Discussion of relationships between recommendations and associated implementation timing (i.e., a joint organizational change has implications for a personnel change, which influences training plans).
6. Related support required to implement recommendations, including but not limited to: additional research, hardware, DOD manpower, test range time, contractor support, etc.
7. Cite any DOD policies or other issues (DOD treaties, protocols, agreements, legal issues, DOD roles, missions and functions, interagency, multinational, etc.) that would prevent the effective implementation of the recommended changes and the reason the proposed changes cannot comply with it. Provide proposed changes to the policy or other issue, and identify other potential implications from the proposed mitigation.

(d) Provide rough-order-of-magnitude total resources required to implement the proposed change as shown in Table B-4, including cost by FY and type of funding required. Note that cost data should represent only new costs or changes to previously funded efforts. For example, if a recommendation is to change an aspect of joint training, and sufficient resources are already programmed to cover the total cost of implementing the proposal, including course development, instructor staffing and/or billets,

instructor education, training facilities, reading materials, hardware, and mock-ups, etc., then do not include in this table.

<b>Resources Required</b>	<b>FY xx (e.g. 12)</b>	<b>FY xx (e.g. 13)</b>	<b>FY xx (e.g. 14)</b>	<b>FY xx (e.g. 15)</b>	<b>FY xx (e.g. 16)</b>	<b>FY xx (e.g. 17)</b>	<b>FYDP Total</b>
O&M							
RDT&E							
Procurement							
Personnel							
MILCON							
Total Funding							

Table B-4. Summary of Resources Required

(5) Alternatives. If applicable, outline alternative approaches and/or options to implement and resource change recommendations. Alternative approaches are particularly appropriate when comprehensive Joint DCRs are submitted with significant resource implications, but Joint DCRs without alternatives may be submitted when only one approach is appropriate or practical.

(a) As appropriate, alternatives will be tailored to the specific Joint DCRs and focused on optimizing, for example:

1. Scope
  - a. All forces and/or systems.
  - b. All forces and/or systems within a particular specialty.
  - c. Specific performance of a subset of forces within a specialty or system.
2. Implementation schedule
  - a. Maximum impact achieved at earliest practical date.
  - b. Impact achieved in phases.
3. Additional level of resources required (combined scope and schedule)
  - a. Comprehensive approach.
  - b. Moderate.
  - c. Limited.

(b) Include a brief discussion of advantages and risks and/or disadvantages of each alternative.

d. Appendices

- (1) Appendix A: References.
- (2) Appendix B: Acronym List.
- (3) Appendix C: Glossary.

DRAFT

(INTENTIONALLY BLANK)

## 7. CDD

### a. Background

(1) The purpose of a CDD is to provide traceability to predecessor documents, or identify capability requirements and gaps in cases where there are no predecessor documents, as well as to document proposed refinements of capability requirements, in the form of development KPPs, KSAs, and additional performance attributes, associated with a specific capability solution intended to wholly or partially satisfy validated capability requirements and close or mitigate associated capability gaps. The CDD also provides supporting data for various certifications and endorsements, identifies related DOTmLPP-P impacts of the proposed capability solution, and outlines life cycle costs which will result from pursuing the capability solution. The document serves as the basis for validation by the appropriate validation authority identified in Enclosure D of this Manual.

(2) For maximum flexibility, a CDD may be based upon a subset of an ICD and/or a consolidation of capability requirements and associated capability gaps from multiple ICDs.

(3) If sufficient information, from an AoA or other analyses, is available to define KPPs and KSAs for multiple capability increments, one validated CDD may support the MS B acquisition decisions of all the described increments. The CDD must clearly articulate if each increment has its own unique set of KPPs/KSAs, or if the KPPs/KSAs listed apply to all increments.

(4) Development of a CDD is guided by the ICD (or approved substitute), the reference architecture (i.e. – DOD Information Enterprise Architecture (IEA); IC; Joint Architecture Reference Model (JARM); Joint Information Environment Operational Reference Model (JIE ORA); Service, CCMD, or other DOD Component Enterprise Architecture; etc.) and the solution architecture; the AoA, the TDS, and the results of competitive prototyping and preliminary design.

(5) In certain cases, a CDD may be generated without a preceding ICD upon approval of an ICD waiver request in accordance with Enclosure C.

(6) Reference xx requires Sponsors to develop a draft CDD or similar documentation prior to MS A, not submitted to the Gatekeeper for staffing and validation, to inform the development of the Request for Proposals (RFP) performance specification in support of the Technology Development (TD) Phase. The draft CDD or similar documentation should contain at least the following CDD sections:

(a) Operational Context (CDD Section 1), with focus on the summary of the CONOPS.

(b) Program Summary (CDD Section 4), with focus on the synchronization of SoS efforts across other CDDs, CPDs, and Joint DCRs.

(c) Development KPPs, KSAs, and additional performance attributes (CDD Section 5), with focus on the initial/draft performance attributes resulting from the AoA or other studies/analyses.

(d) Other System Attributes (CDD Section 6), with focus on attributes which require significant TD Phase efforts.

(7) A validated CDD is a prerequisite to the pre-EMD review leading up to the MS B acquisition decision. IS programs that are designated as MDAPs must have a validated CDD even if authority to use alternate document formats has been delegated by a preceding IS-ICD.

(a) A CDD is not submitted for staffing and validation until the AoA or alternative supporting analysis is completed, provided to the studies repository, and reviewed by the validation authority. If an AoA has not been conducted, the sponsor will explain, in Section (3) of the CDD, why an AoA was not justified.

(b) A CDD will be validated prior to program initiation for shipbuilding programs.

(c) If a CDD describes a capability solution with a significant IS component, the validation of the CDD may permit alternate document formats and delegated approval authority for flexibility in managing IS capability development under the CDD, without having to revalidate an IS ICD. To use the IT Box construct in a CDD, see the IS-CDD section of this Enclosure.

(8) Sponsors of rapidly fielded capability solutions transitioning from the Urgent/Emergent to the Deliberate requirements and acquisition processes will submit a CDD for validation ahead of a MS B decision if additional development is necessary for the enduring capability solution. The supporting assessment of operational utility for the rapidly fielded capability solution will be provided to the studies repository prior to submitting the associated CDD for staffing and validation.

(9) Updates

(a) Updates to a CDD are required if changes to the KPPs are made after validation, or if changes are made in the Joint Concepts, CONOPS, or

DOD Enterprise Architecture and solution architecture, which affect the capability requirements and solution documented in the CDD.

(b) The CDD may be amended in lieu of a CPD to support MS C acquisition decisions for each successive capability increment so long as the amendments do not adversely affect the acquisition of the previously validated capability increments. To use a CDD in lieu of CPD, the Sponsor will resubmit the amended CDD in accordance with the normal staffing processes.

(c) The Sponsor will review the AoA for continuing relevance corresponding to each updated JCIDS document, and the AoA will be updated or a new AoA initiated if a CDD update invalidates the previous AoA.

(d) If the CDD describes more than one capability increment, it is refined/updated as needed before the MS B decision for each increment to incorporate the results of the activities during the acquisition phase (i.e., cost, schedule and performance tradeoffs, testing, and lessons learned from previously fielded capability increments).

(e) Updates to previously validated CDDs using the “IT Box” model are made to the CDD and revalidated as appropriate. Use of the IT Box model in a CDD does not require that predecessor ICD(s) also use the IT Box model. I.e. – conversion of a CDD to IS-CDD does not also require conversion of the related ICD to an IS-ICD.

(f) No additional changes or amendments will be made to previously validated Operational Requirements Documents (ORDs), unless minor changes are approved by the Gatekeeper and Lead FCB. To facilitate amendments or changes, Sponsors shall transcribe ORD content, and any previously validated changes or amendments, into applicable sections of a CDD or CPD for staffing and validation. The original ORD will be submitted as an attachment to the document in the KM/DS system, unless the ORD is already resident in the KM/DS system.

b. Format

(1) Cover Page. The cover page of a CDD shall include the following information.

(a) Classification.

(b) Title, starting with the phrase “Capability Development Document for...”.

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New CDDs, and

modifications to previously validated CDDs, must be endorsed by the Service, CCMD, or other DOD Component J8 equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure H.

(f) Proposed validation authority.

(g) Proposed MDA.

(h) Proposed JSD.

(i) Proposed ACAT.

(2) Executive Summary. An executive summary, not to exceed 1 page, shall follow the cover page and precede the body of the CDD.

c. Document body. The body of the CDD shall have the following 12 sections, and shall be no more than 45 pages long.

(1) Operational Context

(a) The purpose of this section is to provide context for the capability requirements addressed by the CDD, and to provide appropriate traceability to the UCP-assigned missions, OPLANs/CONPLANs, SSA Products, CONOPS, and other driving factors for the capability requirements. This information facilitates review and validation of the CDD from the standpoint of how the capability solutions contribute to the overarching missions and activities of the Joint force.

(b) If the CDD is a successor document to one or more previously validated requirements documents:

1. Cite the validated source documents which identified the capability requirements addressed by the CDD, and ensure that any source documents not already present in the KM/DS system are provided to the Gatekeeper for reference purposes.

2. From the source document(s), summarize the operational context(s) associated with the validated capability requirements addressed by the CDD. Ensure that any changes to operational context(s) which have

occurred since the original validation of the capability requirements are addressed in this section.

3. Include the OV-1. Other than the OV-1, do not include other architecture data in this section unless specifically referenced for illustration purposes elsewhere in the body of the CDD.

(c) If an ICD waiver has been granted and the CDD is not based upon a previously validated requirements document, provide the operational context as outlined for Section (1) of an ICD.

(2) Threat Summary

(a) The purpose of this section is to provide context for the capability requirements addressed by the CDD, to provide appropriate traceability to the threat assessments used during refinement of the capability requirements during development, and to describe any updates to threat assessments which have occurred since the original validation of the capability requirements. This information also enables threat validation as part of the intelligence certification provided during CDD review and validation, and facilitates more rapid review and updating of successor documents when/if threat assessments are updated.

(b) If the CDD is a successor document to one or more previously validated requirements documents:

1. Cite the latest threat assessments applicable to the capability requirements addressed by the CDD. Ensure the applicable threat information has been updated since the original validation of the capability requirements, considering evolving threats identified in the most current threat analysis and findings.

a. For CDDs associated with ACAT ID programs, ensure the most current DIA-validated threat analysis and findings are used to develop the CDD and any associated studies or analysis.

b. For all other CDDs, ensure the most current DIA- or Service-validated threat analysis and findings are used to develop the CDD and any associated studies or analysis.

2. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed by the CDD. Also consider evolving threats to on-going and follow-on research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts.

(c) If an ICD waiver has been granted and the CDD is not based upon a previously validated requirements document, provide the threat summary as outlined for Section (2) of an ICD.

(d) See Appendix I of this Enclosure for intelligence related considerations which are applicable to other sections of the CDD.

### (3) Capability Discussion

(a) The purpose of this section is to identify the validated capability requirements and associated capability gaps addressed by the CDD, and to outline the results of related studies or analysis performed since the original validation of the capability requirements.

(b) If the CDD is a successor document to one or more previously validated requirements documents:

1. Provide an overview of the validated capability requirements and associated capability gaps addressed by the CDD.

2. Summarize all related analyses and/or studies (i.e., AoA and/or other supporting analysis) conducted to determine the KPPs, KSAs, and other system attributes. Include the alternatives, objective, criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in the KM/DS system are provided to the Gatekeeper for reference purposes.

(c) If an ICD waiver has been granted and the CDD is not based upon a previously validated requirements document, provide the capability requirement and capability gap information outlined for Section (3) of an ICD.

### (4) Program Summary

(a) The purpose of this section is to outline the overall approach for developing and fielding one or more capability solutions to satisfy the validated capability requirements and associated capability gaps, and to identify related interdependencies which must be satisfied to provide a successful capability solution.

(b) Provide a summary of the overall program strategy for reaching full capability and, if applicable, the relationship between increments defined in the CDD. Carefully address the considerations (e.g., technologies to be developed, other systems in the FoS or SoS, inactivation of legacy systems) that are driving the incremental delivery plan. For follow-on increments, provide an update on the acquisition status of previous increments, and discuss any

updates to the program strategy to reflect lessons learned from previous increments, changes in Joint Concepts, CONOPS, or the DOD Information Enterprise Architecture and the solution architecture or other pertinent information.

(c) Describe the types and quantities of assets required to attain IOC and FOC. Identify the operational units, including other DOD Components or government agencies if applicable, that will employ the capability solution, and define the quantities required for each organization.

1. Total quantities must include both the required operational inventory, as well as quantities required for training, spares, accommodating a repair/overhaul pipeline, and anticipated attrition over the life cycle, so that the required operational inventory is maintained. Initial production planning should be based upon these quantities, and changes to these quantities may trigger a tripwire review in accordance with Enclosure F of this Manual.

2. Changes to production quantities intended solely to accommodate unexpected attrition, or expenditure in the case of munitions, and maintain the required operational inventory, do not trigger tripwire reviews and do not require re-validation of the capability requirements.

3. Changes to, or absence of changes to, production quantities which result in changes to the operational inventory will trigger tripwire reviews, and require revalidation of required operational inventory quantities and/or acceptance of the altered operational risk.

(d) Define what actions, when complete, will constitute attainment of IOC and FOC of the current increment. Specify the target date for IOC and FOC attainment based on discussions and coordination between the requirement Sponsor and the acquisition community.

(e) Identify any known external dependencies between existing and planned capability solutions and associated risks, particularly if the CDD is part of a FoS or SoS solution set. Discuss dependencies on separate Joint DCRs in this section, and discuss any new/additional DOTmLPF-P changes or required synchronization for SoS solutions in Section (11).

(f) In SoS capability solutions, the Sponsor is responsible for ensuring that related capability solutions, identified in other CDDs, CPDs, and Joint DCRs, remain compatible and that the development is synchronized. These related capability solutions should tie to a common ICD, set of ICDs, or approved substitute(s). In cases where development of SoS capability solutions involves multiple solution Sponsors, a lead Sponsor should be identified to coordinate efforts across organizations.

1. Discuss the relationship of the system described in this CDD to other systems contributing to satisfying the capability requirements. Discuss any related DOTmLPF-P changes needed to make the SoS an effective military capability solution in Section (11).

2. Provide a table that briefly describes the contribution this CDD makes to the fulfillment of capability requirements and closing of capability gaps described in the applicable ICDs, and the relationships to other CDDs, CPDs, or Joint DCRs that also support these capability requirements, as illustrated in Table B-5. Also identify the primary JCAs (Tier 1 & 2) supported by this CDD.

Capability Requirement	CDD Contribution	Related CDDs	Related CPDs	Tier 1 & Tier 2 JCAs
Capability 1 from ICD 1	Brief description of the contribution	CDD Title	CPD Title	
Other Joint validated source document	Brief description of the contribution	CDD Title	CPD Title	

Table B-5. Supported ICDs and Related CDD/CPDs/Joint DCRs

(5) Development KPPs, KSAs, and additional performance attributes

(a) The purpose of this section is to outline the KPPs, KSAs, and other performance attributes which are essential to satisfy the validated capability requirements and associated capability gaps. Sponsors should avoid over specification of KPPs/KSAs, or inclusion of technical specifications as KPPs/KSAs, unless essential to addressing a specific capability requirement. CDD KPPs must be inserted verbatim into the performance section of the Acquisition Program Baseline (APB).

(b) In addition to KPPs essential to the capability requirements being addressed by the CDD, Sponsors must consider the six “required” KPPs detailed in Appendix A to this Enclosure.

1. Not all KPPs will be applicable to every capability requirement, so Sponsors may either use the listed KPPs or articulate why a particular KPP is not applicable.

2. For each applicable KPP, provide specific attributes related to the KPP which must be met rather than a generic statement that the endorsements for the KPPs will be obtained.

3. For the NR-KPP, provide a URL for other required architecture data identified in Table B-F-3 in accordance with references j, ss, and qq.

(c) Provide a description of each attribute and list each attribute in a separate numbered subparagraph. Correlate each KPP and KSA to the capability requirements defined in the ICD and the Tier 1 and 2 JCAs to which they contribute directly. Where applicable, also correlate to the UJTL tasks to which each contributes. Include rationale for each, in terms of SSA products supported or as being derived from other requirements, and cite any existing analytic references. When appropriate, the description should include any unique operating environments for the system. If the CDD is describing a SoS solution, it must describe the attributes for the SoS level of performance and any unique attributes for each of the constituent systems. If the CDD is describing multiple increments, clearly identify which attributes apply to each increment.

(d) Present each attribute in output-oriented, measurable, and testable terms. For each attribute, provide a development threshold value representing the value below which performance is unacceptable. Provide objective values for attributes when the increased performance level provides significant increases in operational utility. If the objective and the threshold values are the same, indicate this by including the statement “threshold = objective.” The PM may use this information to provide incentives for the developing contractor or to weigh capability tradeoffs between threshold and objective values. When there are multiple capability increments and the threshold changes between increments, clearly identify the threshold for each increment. For CDDs that describe IS and use the IT Box model, list the Initial Minimums in lieu of Threshold values and do not list Objective values.

(e) Provide tables summarizing specified KPPs, KSAs, and additional performance attributes in threshold/objective format, as illustrated in Tables B-6 through B-8.

<b>Tier 1 &amp; Tier 2 JCAs</b>	<b>Key Performance Parameter</b>	<b>Development Threshold</b>	<b>Development Objective</b>
	KPP 1	Value	Value
	KPP 2	Value	Value
	KPP 3	Value	Value

Table B-6. Example KPP Table

<b>Tier 1 &amp; Tier 2 JCAs</b>	<b>Key System Attribute</b>	<b>Development Threshold</b>	<b>Development Objective</b>
	KSA 1	Value	Value
	KSA 2	Value	Value
	KSA 3	Value	Value

Table B-7. Example KSA Table

<b>Additional Performance Attribute</b>	<b>Development Threshold</b>	<b>Development Objective</b>
Attribute 1	Value	Value
Attribute 2	Value	Value

Table B-8. Example Additional Performance Attribute Table

(6) Other System Attributes

(a) The purpose of this section is to identify any other attributes not previously identified, especially those that tend to be design, cost, or risk drivers.

(b) Other system attributes may include, but are not limited to, the following:

1. Anti-tamper, embedded instrumentation, electronic attack (EA), and wartime reserve mode (WARM) requirements.
2. Human Systems Integration (HSI) considerations that have a major impact on system effectiveness and suitability.
3. Natural environmental factors (climatic design type, terrain, meteorological and oceanographic factors, impacts and effects).
4. Expected level of capability provided in various mission environments, if degraded relative to KPPs, KSAs, and additional performance attributes articulated in Section (5) of the CDD. Include applicable safety parameters, such as those related to system, nuclear, explosive, and flight safety.
5. Physical and operational security needs.
6. Weather, oceanographic and astro-geophysical support needs throughout the program's expected life cycle, including data accuracy and forecast needs.
7. For systems that may be used in combined allied and coalition operations, issues relating to applicable US-ratified international standardization agreements which will be incorporated in the derived system requirements, in accordance with references ggg and hhh.
8. Transportability considerations, including how the capability solution and related materiel will be moved either to or within the theater, and identify any lift constraints.

(7) Spectrum Requirements

(a) The purpose of this section is to identify electromagnetic spectrum requirements and to ensure compliance with appropriate policy and guidance. This information also informs the Net-Ready KPP (NR KPP) review and certification conducted during staffing of the CDD.

(b) All IS must comply with the spectrum management and electromagnetic environment effects (E3) direction. The spectrum supportability process includes joint, DOD, national and international policies and procedures for the management and use of the electromagnetic spectrum. The spectrum supportability process is detailed in reference ss and details on compliance available at reference qq.

(8) Intelligence Supportability

(a) The purpose of this section is to identify intelligence support requirements and to ensure compliance with appropriate IC policy and guidance. This information also informs the Intelligence review and certification conducted during staffing of the CDD.

(b) Identify, as specifically as possible, all intelligence support requirements throughout the expected life cycle in accordance with Appendix I of this Enclosure.

(9) Weapon Safety Assurance

(a) The purpose of this section is to ensure compliance with appropriate weapon safety policy and guidance. This information also informs the weapon safety review and endorsement conducted during staffing of the CDD.

(b) In accordance with reference tt, all munitions capable of being handled, transported, used, or stored by any Service in joint warfighting environments are considered to be joint weapons and require a joint weapons safety review in accordance with Appendix A to Enclosure D of this Manual and references tt and uu.

(c) The joint or multinational mission environment attributes and performance parameters must be addressed as the basis for the weapon safety endorsement. Identify, as specifically as possible, everything necessary to provide for safe weapon storage, handling, transportation, or use by joint forces throughout the weapon lifecycle, to include performance and descriptive, qualitative, or quantitative attributes.

(d) The CDD will address the following:

1. System Safety. Confirm the establishment of a System Safety Program (SSP) for the life cycle of the weapon system in accordance with references mm and ww. Reference xx provides risk acceptance criteria for high, serious, medium, and low risks.

2. Insensitive Munitions. Confirm capability of resisting insensitive munitions (IM) threats per the established standardized IM protocols in accordance with references yy and zz. If munitions cannot meet all IM criteria, provide details of and rationale for proposed variances, for consideration during review for weapon safety endorsement.

3. Fuze Safety. Confirm compliance with the provisions of references aaa through ccc.

4. Explosive Ordnance Disposal. If munitions contain or deliver energetic material, confirm coordination with the Explosive Ordnance Disposal (EOD) research, development, test and evaluation (RDT&E) authority in accordance with reference ddd.

5. Demilitarization/Disposal. If the munitions contain or deliver energetic material, confirm that the weapon system has a Demilitarization and Disposal plan IAW with treaties, international agreements, Federal and state regulations and laws, and reference xx.

6. Laser Safety. If the munitions contain lasers, confirm that engineering design, protective equipment, administrative controls, or a combination thereof have been implemented in accordance with reference eee, to protect and mitigate the risk to personnel from laser radiation to an acceptable level.

#### (10) Technology Readiness Assessment

(a) The purpose of this section is to highlight technological challenges which may impact the ability to reach the level of performance identified in the KPPs, KSAs, or other performance attributes. This information may be used to inform cost, performance, and schedule tradeoff discussions.

(b) Discuss the program's critical technologies in accordance with reference fff, specifically identifying any critical technologies associated with the program's KPPs.

#### (11) DOTmLPF-P Considerations

(a) The purpose of this section is to outline DOTmLPF-P changes which are required to successfully implement the materiel capability solution.

This information also informs the DOTmLPF-P review and endorsement conducted during staffing of the CDD.

(b) Discuss any DOTmLPF-P changes associated with fielding the system, to include those approaches that would impact CONOPS or plans within a CCMD Area of Responsibility (AOR). Describe the implications for all recommended changes. DOTmLPF-P changes should be considered from two perspectives:

1. Enabling - changes that enable the implementation, operations and support of the specific system;

2. Integrating – changes that must be made to support integration of this system with existing capability solutions.

(c) Include each of the DOTmLPF-P areas if impacted by the capability solution addressed in the CDD. For DOTmLPF-P changes already addressed in separate Joint DCRs, cite the Joint DCR which applies and provide status. For DOTmLPF-P changes not already addressed in separate Joint DCRs, provide details of the recommended changes and implementation plans in the following areas:

1. Doctrine.

2. Organization.

3. Training. Include only the training issues not already covered under the Training KPP.

4. Existing materiel. Include “little-m” changes in quantities to other materiel capability solutions.

5. Leadership and Education.

6. Personnel. Identify changes to personnel quantities, types (officer, enlisted, civilian, and/or contractor), and skill sets required to fully implement the capability solution.

7. Facilities. Specify facility, shelter, supporting infrastructure, and ESOH asset requirements, and the associated costs, availability, and acquisition MS schedule(s) related to supporting the system. Detail any basing needs (forward and main operating bases, institutional training base, and depot requirements).

8. Policy.

(12) Program Affordability

(a) The purpose of this section is to identify the overall resources associated with pursuing the capability solution, including materiel and non-materiel costs over its anticipated lifecycle. This information may be used to inform cost, performance, and schedule tradeoff discussions.

(b) Cite applicable cost analyses conducted to date, and ensure that any final reports or other results documentation, not already present in the KM/DS system, are provided to the Gatekeeper for reference purposes.

(c) Show total cost as shown in Table B-9, including cost by FY and type of funding based upon threshold levels of performance. Show cost factors used to determine ACAT level, per reference xx. The affordability determination is made as part of the cost assessment in the analysis supporting the CDD development. Cost will be included in the CDD as life-cycle cost or, if available, total ownership cost, and will include all associated DOTmLPP-P costs.

(d) For IS, identify the programmed funding by year for the software development and sustainment and for hardware refresh and integration, and provide rationale for the level of funding required.

<b>Resources Required</b>	<b>FY xx (e.g. 12)</b>	<b>FY xx (e.g. 13)</b>	<b>FY xx (e.g. 14)</b>	<b>FY xx (e.g. 15)</b>	<b>FY xx (e.g. 16)</b>	<b>FY xx (e.g. 17)</b>	<b>FYDP Total</b>	<b>Life Cycle Cost</b>
O&M								
RDT&E								
Procurement								
Personnel								
MILCON								
Total Funding								

Table B-9. Summary of Resources Required

d. Appendices

- (1) Appendix A: References.
- (2) Appendix B: Acronym List.
- (3) Appendix C: Glossary.

## 8. IS-CDD

### a. Background

(1) The purpose of an IS-CDD is the same as for a regular CDD, but implements the “IT Box” model, outlined in the IS-ICD section of this Enclosure, to provide IS programs greater flexibility to incorporate evolving technologies, and achieve faster responses from requirement validation processes than is typical for other kinds of materiel or non-materiel solutions. The document serves as the basis for validation by the appropriate validation authority identified in Enclosure D of this Manual.

(2) IS-CDDs are appropriate for use in cases where:

(a) An IS program has a validated ICD or CDD and wants to transition to the IT Box construct. An amendment to the existing document and revalidation, documented in a new JROC Memorandum (JROCM), is necessary to delegate JROC or JCB requirements oversight authority.

(b) A validated ICD contains capability requirements which can be addressed by a combination of IS and non-IS capability solutions and the IT Box construct is applicable to the IS portion of the capability solution(s).

(c) All hardware associated with an IS-CDD is COTS/GOTS, and hardware development is restricted to that necessary for system integration, system enhancements, and hardware refresh due to obsolescence.

(d) The intended solution approach involves research, development, and acquisition of applications system software, and the projected software development costs exceed \$15 million. IS with development costs less than \$15 million are not subject to JCIDS process.

(3) IS-CDDs is not appropriate for use in cases where:

(a) Software is embedded as a subset of a capability solution developed under other validated documents.

(b) Defense Business Systems capabilities are defined and acquired in accordance with reference dd.

(4) Sponsors shall use the IS-CDD format when applicable for JROC Interest and JCB Interest documents drafted after the effective date of this Manual. Sponsors are encouraged to use and validate IS-CDDs for situations where the Sponsor is the validation authority.

(5) CPDs are not required as successor documents to an IS-CDD, and the delegated authority may prescribe alternative document formats most appropriate to the follow-on efforts. Alternative documents must be provided to the KM/DS system for information purposes and visibility in the Joint portfolios. See the IS-ICD section of this enclosure for an example of Sponsor documents used for managing follow-on efforts.

(6) Efforts in an IS-CDD may include:

(a) The procurement or modification of commercially available products and technologies from domestic or international sources, or the development of dual-use technologies.

1. COTS/GOTS software, and associated hardware, without modification.

2. Commercial capability solutions with integrated, DOD-specific performance characteristics/standards.

(b) The additional production or modification of previously-developed U.S. and/or Allied military or Interagency systems or equipment. Increases in quantities of unmodified existing systems which remain within the scope of the validated IT Box may be accomplished without validation of new documents.

(c) Development, integration, and acquisition of customized application software.

(7) Revalidation. IS-CDDs require revalidation if the Sponsor proposes to:

(a) Add new capability requirements beyond the scope of the validated IS-CDD.

(b) Increase programmed development and integration funding for a MAIS program by 10% or more compared with the desired level of funding identified in the IS-CDD.

(8) Biennial FCB Review. For all IS programs with a valid IS-CDD, the lead FCB shall receive a brief every second year following the validation. The lead FCB will determine if the JROC or JCB should review the following briefing items, and will make appropriate recommendations for action.

(a) Progress in delivering capability solutions within the required timeframe and available funding.

(b) Compliance with applicable enterprise architecture and data standards.

(c) Other items identified by the IS-CDD validation

b. Format

(1) Cover Page. The cover page for an IS-CDD shall be the same as for a regular CDD except that the title will begin with the phrase “Information Systems Capability Development Document for...”

(2) Executive Summary. The executive summary for an IS-CDD is the same as for a regular CDD.

c. Document body. The body of an IS CDD differs from a regular CDD in two sections, and shall be no more than 45 pages long. See the regular CDD section for content of the unchanged sections.

(1) Capability Discussion – CDD Section (3). Define the proposed capability requirements and initial minimum levels in terms of measures of effectiveness (MOEs). Describe capability gaps in terms of the difference between the proposed capability requirements and similar existing capabilities, if any.

(2) Program Summary – CDD Section (4). With the capability requirements making up one side of the IT Box, briefly discuss the remaining sides of the IT Box, illustrated in Figure B-11.

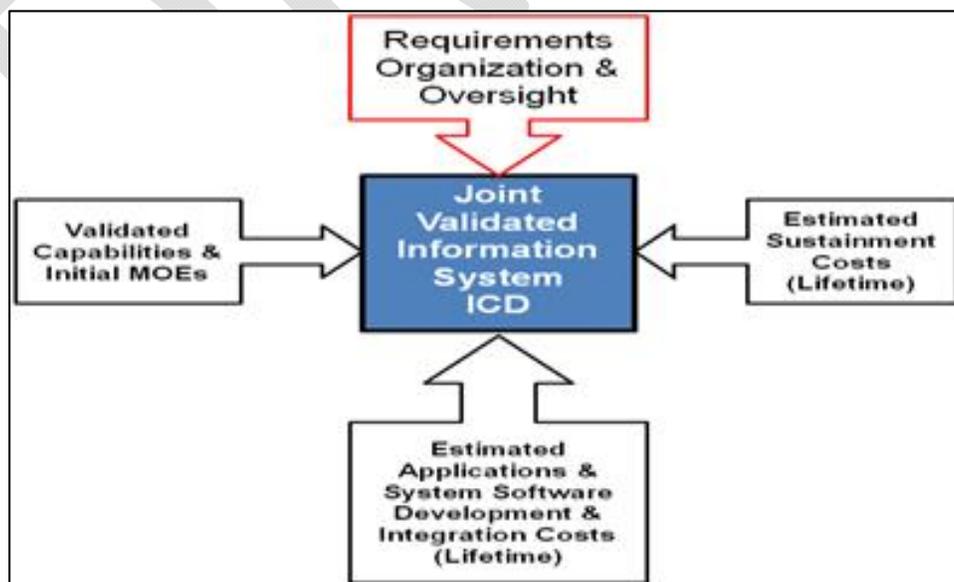


Figure B-11. Components of the “IT Box” model in IS-CDDs

(a) Identify the proposed flag-level oversight body, the chair of that body, and the organizations represented on the body being proposed to receive delegated requirements oversight duties.

(b) Summarize the estimated development and integration as well as sustainment costs over the life cycle of the program as shown in Section 12 – Program Affordability.

d. Appendices. The appendices for an IS-CDD are the same as for a regular CDD.

DRAFT

## 9. CPD

### a. Background

(1) The purpose of a CPD is to provide traceability to predecessor documents, or identify capability requirements and gaps in cases where there are no predecessor documents, as well as to document proposed refinements of capability requirements, in the form of production KPPs, KSAs, and additional performance attributes, associated with a specific capability solution intended to wholly or partially satisfy validated capability requirements and close or mitigate associated capability gaps. The CPD also provides supporting data for various certifications and endorsements, identifies related DOTmLPF-P impacts of the proposed capability solution, and outlines life cycle costs which will result from pursuing the capability solution. The document serves as the basis for validation by the appropriate validation authority identified in Enclosure D of this Manual.

(2) The CPD provides KPPs, KSAs, and additional performance attributes, at a system level necessary to guide the production and deployment of a single increment of a specific system. Each increment described by a CPD must provide a safe, operationally effective, suitable, and useful capability solution in the intended environment, commensurate with the investment.

(a) The most significant difference between the CDD and the CPD is the refinement of threshold and objective values for KSAs, KPPs, and additional performance attributes previously identified in the CDD or other source document. The Systems Engineering Plan (SEP) then documents Technical Performance Measures (TPMs) which are necessary to achieve the KPPs and KSAs. Metrics, criteria and desired test and evaluation strategy developed for the Test and Evaluation Master Plan (TEMP) and refined during the Engineering and Manufacturing Development (EMD) phase are updated as necessary to support MS C and initial operational test and evaluation. The metrics and criteria are based on validated performance criteria in the CPD. Each production threshold listed in the CPD depicts the minimum performance that the PM is expected to deliver for an increment's IOC or FOC based on the system design subsequent to the CDR.

(b) A Sponsor may resubmit a CDD for revalidation in lieu of a CPD in cases where the CDD accurately reflects the performance of the system to be delivered at low-rate initial production. To use a CDD in lieu of CPD, the Sponsor will resubmit the CDD in accordance with the steps outlined earlier in this Enclosure.

(c) Because a CPD is finalized after critical design review (CDR) and after the majority of capability development, it is normally not appropriate to introduce new capability requirements at this point. New capability

requirements should be included in the next increment in an evolutionary program or in a future modification or upgrade if no additional increments are planned.

(2) The development of the CPD is guided by applicable ICDs, the CDD; the reference architecture (i.e. – DOD IEA; IC; JARM; JIE ORA; Service, CCMD, or other DOD Component Enterprise Architecture; etc.) and the solution architecture; AoA and/or supporting analytical results; developmental and operational test results; and the CDR.

(3) In certain cases, a CPD may be generated without a preceding ICD and/or CDD upon approval of an ICD and/or CDD waiver request in accordance with Enclosure C.

#### (4) CPD Development and Documentation

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

(b) The CPD Sponsor will apply lessons learned during the EMD phase, lessons learned from previous increments, risk reduction activities, assessments (for JCTDs, qualified prototype projects, and quick-reaction technology projects), experimentation, test and evaluation, modeling and simulation, capability and schedule tradeoffs and affordability analysis in the delivery of the capability solution. The KPPs previously defined in a CDD may be refined (with a rationale provided) and should be tailored to the proposed system to be procured. (e.g., range, probability of kill, platform survivability, etc.)

(c) The CPD Sponsor, in coordination and collaboration with the appropriate DOD components, agencies, and FCB will prepare the CPD. Continuous collaboration with the systems acquisition PM is essential. The CPD Sponsor also will collaborate with Sponsors of related CDDs and/or CPDs that are required in FoS and SoS solutions, particularly those generated from a common ICD.

(5) Sponsors of rapidly fielded capability solutions transitioning from the Urgent/Emergent to the deliberate requirements and acquisition processes will submit a CPD for validation ahead of a MS C decision if additional development is not necessary for production and sustainment of the enduring

capability solution. The supporting assessment for the rapidly fielded capability solution will be provided to the studies repository prior to submitting the associated CPD for staffing and validation.

b. Format

(1) Cover Page. The cover page of a CPD shall include the following information.

(a) Classification.

(b) Title, starting with the phrase “Capability Production Document for...”.

(c) Sponsoring organization, and signature authority who authorized the submittal for review and validation. New CPDs, and modifications to previously validated CPDs, must be endorsed by the Service, CCMD, or other DOD Component J8 equivalent or higher.

(d) Date submitted by the Sponsoring organization.

(e) Primary and secondary POCs for the document Sponsor. Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure H.

(f) Proposed validation authority.

(g) Proposed MDA.

(h) Proposed JSD.

(i) Proposed ACAT.

(2) Executive Summary. An executive summary, not to exceed 1 page, shall follow the cover page and precede the body of the CPD.

c. Document body. The body of the CPD shall have the following 12 sections, and shall be no more than 40 pages long.

(1) Operational Context

(a) The purpose of this section is to provide context for the capability requirements addressed by the CPD, and to provide appropriate traceability to the UCP-assigned missions, OPLANs/CONPLANs, SSA Products, CONOPS, and other driving factors for the capability requirements. This

information facilitates review and validation of the CPD from the standpoint of how the capability solutions contribute to the overarching missions and activities of the Joint force.

(b) If the CPD is a successor document to one or more previously validated requirements documents:

1. Cite the validated source documents which identified the capability requirements addressed by the CPD, and ensure that any source documents not already present in the KM/DS system are provided to the Gatekeeper for reference purposes.

2. From the source document(s), summarize the operational context(s) associated with the validated capability requirements addressed by the CPD. Ensure that any changes to operational context(s) which have occurred since the original validation of the capability requirements are addressed in this section.

3. Include the OV-1. Other than the OV-1, do not include other architecture data in this section unless specifically referenced for illustration purposes elsewhere in the body of the CPD.

(c) If an ICD and CDD waiver has been granted and the CPD is not based upon a previously validated requirements document, provide the operational context as outlined for Section (1) of an ICD.

## (2) Threat Summary

(a) The purpose of this section is to provide context for the capability requirements addressed by the CPD, to provide appropriate traceability to the threat assessments used during refinement of the capability requirements during development, and to describe any updates to threat assessments which have occurred since the original validation of the capability requirements. This information also enables threat validation as part of the intelligence certification provided during CPD review and validation, and facilitates more rapid review and updating of successor documents when/if threat assessments are updated.

(b) If the CPD is a successor document to one or more previously validated requirements documents:

1. Cite the latest threat assessments applicable to the capability requirements addressed by the CPD. Ensure the applicable threat information has been updated since the original validation of the capability requirements, considering evolving threats identified in the most current threat analysis and findings.

a. For CPDs associated with ACAT ID programs, ensure the most current DIA-validated threat analysis and findings are used to develop the CPD and any associated studies or analysis.

b. For all other CPDs, ensure the most current DIA- or Service-validated threat analysis and findings are used to develop the CPD and any associated studies or analysis.

2. From the source document(s), outline the threat summary(ies) associated with the validated capability requirements addressed by the CPD. Also consider evolving threats to on-going and follow-on research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts.

(c) If an ICD and CDD waiver has been granted and the CPD is not based upon a previously validated requirements document, provide the threat summary as outlined for Section (2) of an ICD.

(d) See Appendix I of this Enclosure for intelligence related considerations which are applicable to other sections of the CPD.

### (3) Capability Discussion

(a) The purpose of this section is to identify the validated capability requirements and associated capability gaps addressed by the CPD, and to outline the results of related studies or analysis performed since the original validation of the capability requirements.

(b) If the CPD is a successor document to one or more previously validated requirements documents:

1. Provide an overview of the validated capability requirements and associated capability gaps addressed by the CPD.

2. Summarize all related analyses and/or studies conducted to refine the KPPs, KSAs, and other system attributes. Include the alternatives, objective, the criteria, assumptions, recommendations, and conclusion. Ensure that final reports, or other resulting products, of studies or analyses not already present in the KM/DS system are provided to the Gatekeeper for reference purposes.

(c) If an ICD and CDD waiver has been granted and the CPD is not based upon a previously validated requirements document, provide the

capability requirement and capability gap information outlined for Section (3) of an ICD.

(4) Program Summary

(a) The purpose of this section is to outline the overall approach for developing and fielding one or more capability solutions to satisfy the validated capability requirements and associated capability gaps, and to identify related interdependencies which must be satisfied to provide a successful capability solution.

(b) Provide a summary of the overall program strategy for reaching full capability and, if applicable, the relationship between the production increment addressed by this CPD and any other increments of the program. Carefully address the considerations (e.g., technologies to be developed, other systems in the FoS or SoS, inactivation of legacy systems) that are driving the incremental delivery plan. For follow-on increments, provide an update on the acquisition status of previous increments, and discuss any updates to the program strategy to reflect lessons learned from previous increments, changes in Joint Concepts, CONOPS, or the DOD Information Enterprise Architecture and the solution architecture or other pertinent information.

(c) Describe the types and quantities of assets required to attain IOC and FOC. Identify the operational units, including other DOD Components or government agencies if applicable, that will employ the capability solution, and define the quantities required for each organization.

1. Total quantities must include both the required operational inventory, as well as quantities required for training, spares, accommodating a repair/overhaul pipeline, and anticipated attrition over the life cycle, so that the required operational inventory is maintained. Initial production planning should be based upon these quantities, and changes to these quantities may trigger a tripwire review in accordance with Enclosure F of this Manual.

2. Changes to production quantities intended solely to accommodate unexpected attrition, or expenditure in the case of munitions, and maintain the required operational inventory, do not trigger tripwire reviews and do not require re-validation of the capability requirements.

3. Changes to, or absence of changes to, production quantities which result in changes to the operational inventory will trigger tripwire reviews, and require revalidation of required operational inventory quantities and/or acceptance of the altered operational risk.

(d) Define what actions, when complete, will constitute attainment of IOC and FOC of the current increment. Specify the target date for IOC and

FOC attainment based on discussions and coordination between the requirement Sponsor and the acquisition community.

(e) Identify any known external dependencies between existing and planned capability solutions and associated risks, particularly if the CPD is part of a FoS or SoS solution set. Discuss dependencies on separate Joint DCRs in this section, and discuss any new/additional DOTmLPF-P changes or required synchronization for SoS solutions in Section (11).

(f) In SoS capability solutions, the Sponsor is responsible for ensuring that related capability solutions, specified in other CDDs, CPDs, and Joint DCRs, remain compatible and that the development is synchronized. These related capability solutions should tie to a common ICD, set of ICDs, or approved substitute(s). In cases where development of SoS capability solutions involves multiple solution Sponsors, a lead Sponsor should be identified to coordinate efforts across organizations.

1. Discuss the relationship of the system described in this CPD to other systems contributing to satisfying the capability requirements. Discuss any related DOTmLPF-P changes needed to make the SoS an effective military capability solution in Section (11).

2. Provide a table that briefly describes the contribution this CPD makes to the fulfillment of capability requirements and closing of capability gaps described in the applicable ICDs, and the relationships to other CDDs, CPDs, and Joint DCRs that also support these capability requirements, as illustrated in Table B-10. Review all related ICDs, CDDs, and CPDs for applicability to the SoS addressed by this CPD. Also identify the primary JCAs (Tier 1 and 2) supported by this CPD. If the CPD is not based on validated capability requirements from an ICD, identify the validated source document.

<b>Capability Requirement</b>	<b>CPD Contribution</b>	<b>Related CDDs</b>	<b>Related CPDs</b>	<b>Tier 1 &amp; Tier 2 JCAs</b>
ICD Capability Description #1 (Source Doc)	Brief Description of the Contribution	CDD Title	CPD Title	
ICD Capability Description #2 (Source Doc)	Brief Description of the Contribution	CDD Title	CPD Title	
Other JROC validated source document	Brief Description of the Contribution	CDD Title	CPD Title	

Table B-10. Supported ICDs and Related CDDs/CPDs/Joint DCRs

(5) Production KPPs, KSAs, and additional performance attributes

(a) The purpose of this section is to outline the KPPs, KSAs, and other performance attributes which are essential to satisfy the validated capability requirements and associated capability gaps. Sponsors should avoid over specification of KPPs/KSAs, or inclusion of technical specifications as KPPs/KSAs, unless essential to addressing a specific capability requirement. CPD KPPs must be inserted verbatim into the performance section of the APB.

(b) In addition to KPPs essential to the capability requirements being addressed by the CPD, Sponsors must consider the six “required” KPPs detailed in Appendix A to this Enclosure.

1. Not all KPPs will be applicable to every capability requirement, so Sponsors may either use the listed KPPs or articulate why a particular KPP is not applicable.

2. For each applicable KPP, provide specific attributes related to the KPP which must be met rather than a generic statement that the endorsements for the KPPs will be obtained.

3. For the NR KPP, provide a URL for other required architecture data identified in Table B-F-3 in accordance with references j, ss, and qq.

(c) Provide a description for each attribute and list each attribute in a separately numbered subparagraph. Correlate each KPP and KSA to the capability requirements defined in the ICD and/or CDD, and the Tier 1 and 2 JCAs to which they contribute directly. Where applicable, also correlate to the UJTL tasks to which each contributes. Include rationale for each, in terms of SSA products supported or as being derived from other requirements, and cite any analytic references. When appropriate, the description should include any unique operating environments for the system. If the CPD is part of a SoS solution, it must describe the attributes for the SoS level of performance and any unique attributes for each of the constituent systems.

(d) Present each attribute in output-oriented, measurable, and testable terms. For each attribute, provide a production threshold value representing the value below which performance is unacceptable. Provide objective values for attributes when the increased performance level provides significant increases in operational utility. If the threshold and objective values are the same, indicate this by including the statement “threshold = objective.” The PM may use this information to provide incentives for the production contractor to enhance performance through production improvements or to weigh capability tradeoffs between threshold and objective values.

(e) Provide tables summarizing specified KPPs, KSAs and additional performance attributes in threshold/objective format, as illustrated in Tables B-11 through B-13.

<b>Tier 1 &amp; 2 JCA</b>	<b>Key Performance Parameter</b>	<b>Production Threshold</b>	<b>Production Objective</b>
	KPP 1	Value	Value
	KPP 2	Value	Value
	KPP 3	Value	Value

Table B-11. Example KPP Table

<b>Tier 1 &amp; 2 JCA</b>	<b>Key System Attributes</b>	<b>Production Threshold</b>	<b>Production Objective</b>
	KSA 1	Value	Value
	KSA 2	Value	Value
	KSA 3	Value	Value

Table B-12. Example KSA Table

<b>Additional Performance Attribute</b>	<b>Production Threshold</b>	<b>Production Objective</b>
Attribute 1	Value	Value
Attribute 2	Value	Value
Attribute 3	Value	Value

Table B-13. Example Additional Performance Attribute Table

(6) Other System Attributes

(a) The purpose of this section is to identify any other attributes not previously identified, especially those that tend to be design, cost, or risk drivers

(b) Other system attributes may include, but not limited to, the following:

1. Anti-tamper, embedded instrumentation, EA, and WARM requirements.

2. HSI considerations that have a major impact on system effectiveness, suitability, and affordability.

3. Natural environmental factors (climatic design type, terrain, meteorological and oceanographic factors, and impacts and effects).

4. Expected level of capability provided in various mission environments, if degraded relative to KPPs, KSAs, and additional performance attributes articulated in Section (5) of the CPD. Include applicable safety

parameters, such as those related to system, nuclear, explosive, and flight safety.

5. Physical and operational security needs.

6. Weather, oceanographic and astro-geophysical support needs throughout the program's expected life cycle, including data accuracy and forecast needs.

7. For systems that may be used in combined allied and coalition operations, issues relating to the potentially applicable US-ratified international standardization agreements. Provide an initial indication of which ones will be incorporated in the derived system requirements, in accordance with references ggg and hhh.

8. Transportability considerations, including how the capability solution and related materiel will be moved either to or within the theater, and identify any lift constraints.

#### (7) Spectrum Requirements

(a) The purpose of this section is to identify electromagnetic spectrum requirements and to ensure compliance with appropriate policy and guidance. This information also informs the NR KPP review and certification conducted during staffing of the CPD.

(b) All IS must comply with the spectrum management and E3 direction. The spectrum supportability process includes joint, DOD, national and international policies and procedures for the management and use of the electromagnetic spectrum. The spectrum supportability process is detailed in reference ss and details on compliance available at reference qq.

#### (8) Intelligence Supportability

(a) The purpose of this section is to identify intelligence support requirements and to ensure compliance with appropriate IC policy and guidance. This information also informs the Intelligence review and certification conducted during staffing of the CPD.

(b) Identify, as specifically as possible, all intelligence support requirements throughout the expected life cycle in accordance with Appendix I of this Enclosure.

#### (9) Weapon Safety Assurance

(a) The purpose of this section is to ensure compliance with appropriate weapon safety policy and guidance. This information also informs the weapon safety review and endorsement conducted during staffing of the CPD.

(b) In accordance with reference tt, all munitions capable of being handled, transported, used, or stored by any Service in joint warfighting environments are considered to be joint weapons and require a joint weapons safety review in accordance with Appendix A to Enclosure D of this Manual and references tt and uu.

(c) The joint or multinational mission environment attributes and performance parameters must be addressed as the basis for the weapon safety endorsement. Identify, as specifically as possible, everything necessary to provide for safe weapon storage, handling, transportation, or use by joint forces throughout the weapon lifecycle, to include performance and descriptive, qualitative, or quantitative attributes.

(d) The CPD will address the following:

1. System Safety. Confirm the establishment of a System Safety Program (SSP) for the life cycle of the weapon system in accordance with references mm and ww. Reference xx provides risk acceptance criteria for high, serious, medium, and low risks.

2. Insensitive Munitions. Confirm capability of resisting insensitive munitions (IM) threats per the established standardized IM protocols in accordance with references yy and zz. If munitions cannot meet all IM criteria, provide details of and rationale for proposed variances, for consideration during review for weapon safety endorsement.

3. Fuze Safety. Confirm compliance with the provisions of references aaa through ccc.

4. Explosive Ordnance Disposal. If munitions contain or deliver energetic material, confirm coordination with the Explosive Ordnance Disposal (EOD) research, development, test and evaluation (RDT&E) authority in accordance with reference ddd.

5. Demilitarization/Disposal. If the munitions contain or deliver energetic material, confirm that the weapon system has a Demilitarization and Disposal plan IAW with treaties, international agreements, Federal and state regulations and laws, and reference xx.

6. Laser Safety. If the munitions contain lasers, confirm that engineering design, protective equipment, administrative controls, or a

combination thereof have been implemented in accordance with reference eee, to protect and mitigate the risk to personnel from laser radiation to an acceptable level.

(10) Manufacturing Readiness Assessment

(a) The purpose of this section is to highlight manufacturing challenges which may impact the ability to produce the capability solution as designed to reach the level of performance identified in the KPPs, KSAs, or other performance attributes. This information may be used to inform cost, performance, and schedule tradeoff discussions.

(b) Discuss the program's critical manufacturing challenges in accordance with reference fff, specifically identifying any manufacturing readiness challenges associated with the program's KPPs.

(11) DOTmLPF-P Considerations

(a) The purpose of this section is to outline DOTmLPF-P changes which are required to successfully implement the materiel capability solution. This information also informs the DOTmLPF-P review and endorsement conducted during staffing of the CPD.

(b) Discuss any DOTmLPF-P changes associated with fielding the system, to include those approaches that would impact CONOPS or plans within a CCMD AOR. Describe the implications for all recommended changes. DOTmLPF-P changes should be considered from two perspectives:

1. Enabling – changes that enable the implementation, operations and support of the specific system;

2. Integrating – changes that must be made to support integration of this system with existing capability solutions.

(c) Include each of the DOTmLPF-P areas if impacted by the capability solution addressed in the CPD. For DOTmLPF-P changes already addressed in separate Joint DCRs, cite the Joint DCR which applies and provide status. For DOTmLPF-P changes not already addressed in separate Joint DCRs, provide details of the recommended changes and implementation plans in the following areas:

1. Doctrine.

2. Organization.

3. Training. Include only the training issues not already covered under the Training KPP.

4. Existing materiel. Include “little-m” changes in quantities to other materiel capability solutions.

5. Leadership and Education.

6. Personnel. Identify changes to personnel quantities, types (officer, enlisted, civilian, and/or contractor), and skill sets required to fully implement the capability solution.

7. Facilities. Specify facility, shelter, supporting infrastructure, and ESOH asset requirements, and the associated costs, availability, and acquisition MS schedule(s) related to supporting the system. Detail any basing needs (forward and main operating bases, institutional training base, and depot requirements).

8. Policy.

(12) Program Affordability

(a) The purpose of this section is to identify the overall resources associated with pursuing the capability solution, including materiel and non-materiel costs over its anticipated lifecycle. This information may be used to inform cost, performance, and schedule tradeoff discussions.

(b) Cite applicable cost analyses conducted to date, and ensure that any final reports or other results documentation, not already present in the KM/DS system, are provided to the Gatekeeper for reference purposes.

(c) Show total cost as shown in Table B-14, including cost by FY and type of funding based upon threshold levels of performance. Show cost factors used to determine ACAT level, per reference xx. The affordability determination is made as part of the cost assessment in the analysis supporting the CPD development, which may include updates to earlier cost analyses. Cost will be included in the CPD as life-cycle cost, or if available, total ownership cost, and will include all associated DOTmLFP-P costs.

<b>Resources Required</b>	<b>FY xx (e.g. 12)</b>	<b>FY xx (e.g. 13)</b>	<b>FY xx (e.g. 14)</b>	<b>FY xx (e.g. 15)</b>	<b>FY xx (e.g. 16)</b>	<b>FY xx (e.g. 17)</b>	<b>FYDP Total</b>	<b>Life Cycle Cost</b>
O&M								
RDT&E								
Procurement								
Personnel								
MILCON								
Total Funding								

Table B-14. Summary of Resources Required

d. Appendices

- (1) Appendix A: References.
- (2) Appendix B: Acronym List.
- (3) Appendix C: Glossary.

DRAFT

## 10. UON/JUON/JEON

### a. Background

(1) The purpose of UONs, JUONs, and JEONs is to facilitate expedited documentation of capability requirements and traceability to ongoing or anticipated contingency operations, quantify critical mission failure and/or unacceptable loss of life associated with not satisfying the capability requirements, and if known, propose potential approaches for rapid acquisition of a materiel capability solution. These documents are used ONLY when the deliberate requirement validation and deliberate acquisition processes are incapable of satisfying the capability requirement in the required timelines, and when other means of addressing the requirement such as the GFM process, Joint Manpower Validation Process (JMVP), etc., are not feasible. These documents serve as the basis for validation by the appropriate validation authority identified in Enclosure E of this Manual.

### (2) Types of UONs

(a) DOD Component UONs are applicable to only one DOD Component and are driven by ongoing or anticipated contingency operations. DOD Component UONs are submitted, staffed, and validated in accordance with references o through u. After validation, DOD Component UONs are uploaded to the KM/DS system for information and visibility in the FCB portfolios.

(b) JUONs are UONs affecting two or more DOD Components and are driven by ongoing contingency operations. JUONs are submitted by CCMDs in accordance with this enclosure, and reviewed and validated in accordance with Enclosure E.

(c) JEONs are UONs affecting two or more DOD Components and are driven by anticipated contingency operations. JEONs are submitted by CCMDs in accordance with this Enclosure, and reviewed and validated in accordance with Enclosure E.

(3) Capability requirements with anticipated development/fielding timeframes longer than 2 years for JUONs or 5 years for JEONs should not use a JUON or JEON to document and validate the capability requirement and associated gaps, but rather generate an ICD, CDD, or CPD for review and validation in the deliberate staffing process.

(4) Capability solutions for JUONs, JEONs, and DOD Component UONs do not require associated ICDs, CDDs, or CPDs for initial fielding, but may require appropriate CDDs or CPDs to support transition for sustainment

and/or further development of capability solutions for enduring use. See Enclosure F of this Manual for transition details for JUONs and JEONs.

b. Format

(1) Cover Page. JUONs and JEONs do not require a cover page.

(2) Executive Summary. JUONs and JEONs do not require an executive summary.

c. Document body. JUONs and JEONs will be in memo format and generally not exceed 3 pages.

(1) Administrative Data

(a) Title: (Unclassified version)

(b) CCMD Submitted by: (e.g., CENTCOM)

(c) Authorized by: Release authority's name, rank and title. New JUONs and JEONs, and modifications to the capability requirements in previously validated JUONs and JEONs, must be endorsed by the CCMD Commander, Deputy Commander, or Chief of Staff. Administrative modifications to previously validated JUONs or JEONs may be endorsed by the CCMD J8.

(d) Primary and secondary POCs for the document Sponsor: Include name, title/rank, phone, and both NIPRNET and SIPRNET email addresses. POCs must have completed the appropriate level of RMCT in accordance with Enclosure H.

(e) Date submitted by the CCMD.

(2) Operational Context and Threat Analysis. What is the target, threat, or operational deficiency? What cannot be done without a new or improved capability solution? Identify where the operational deficiency exists, describing the mission deficiency or capability gap. Describe in detail the nature of the urgency and the operational impact, if not immediately resolved, in terms of critical mission failure or loss of life. Provide a CONOPS for which the capabilities requested in the JUON/JEON contribute, including information regarding the coalition environment within which the capability solution will need to operate.

(3) Required Capability: Describe what capabilities are required, and whether they support a discrete operation, must be sustained for an extended period of time, or must be sustained until the end of the conflict. Include

threshold/objective performance requirements for any key attributes. This description must also specify the latest acceptable date to address the capability requirements and capability gaps.

(4) Flexibility. In the event of technological or other challenges, indicate whether receiving a partial solution on schedule is preferred to a delayed solution which satisfies a greater portion of the capability requirement. Estimate acceptable percentages of reduced performance and/or acceptable delay timeframes.

(5) Potential Non-Materiel Solutions: Describe any non-materiel options and alternatives that were considered or which provide partial mitigation of the capability requirement.

(6) Potential Materiel Solutions: If known, identify and discuss viable solutions – from US or Allied/Partner nation sources – that could improve operational capabilities or system performance. Discuss any impacts to safety, survivability, personnel, training, logistics, communications, etc. If applicable, discuss any market survey or similar related information developed by document Sponsor or during the validation process. If market research details are available, provide along with the JUON or JEON to facilitate reuse during rapid acquisition activities.

(7) Required Quantities. For materiel solutions, identify quantities required and distribution among applicable DoD Components.

(a) Total quantities must include both the required operational inventory, as well as quantities required for training, spares, accommodating a repair/overhaul pipeline, and anticipated attrition over the life cycle, so that the required operational inventory is maintained.

(b) Changes to quantities intended solely to accommodate unexpected attrition, or expenditure in the case of munitions, and maintain the required operational inventory, do not require re-validation of the capability requirements.

(c) Changes to, or absence of changes to, quantities which result in changes to the operational inventory will require revalidation of required operational inventory quantities and/or acceptance of the altered operational risk.

(8) Constraints: Identify any known constraints that could inhibit satisfying the need -- such as arms control treaties, logistics support, transportation, manpower, training or non-military barriers.

(INTENTIONALLY BLANK)

## APPENDIX I TO ENCLOSURE B

### CONTENT GUIDE FOR THREAT VALIDATION AND INTELLIGENCE SUPPORTABILITY

#### 1. Purpose

a. This guide provides general descriptions of intelligence support requirement categories, along with examples of quantitative and qualitative attributes, to assist Sponsors with identification of intelligence support requirements. The descriptions of intelligence support requirement categories are not all-inclusive; but rather serve as examples and must be tailored to satisfy each capability solution's unique intelligence support requirements.

b. This guide also provides paragraph-by-paragraph considerations for each of the JCIDS documents as well as ISPs, to ensure that intelligence related content is captured consistently throughout the documents, and facilitate DWO threat validation and Joint Staff Directorate for Intelligence (J-2) intelligence certification outlined in Appendix B to Enclosure D.

c. To ensure consistency with IC policies and procedures, any substantive changes to this Guide will be coordinated with and approved by the Director, Joint Staff J-2 Directorate for Intelligence (DJ-2).

2. Intelligence Support Requirement Category Descriptions. JCIDS documents must identify and explain known or anticipated intelligence support requirements, and potential shortfalls if applicable, that will result from the development and operation of the capability solution over its entire life cycle. This includes projected requirements for all intelligence information (collection requirements/ parameters, analytical products, etc.), infrastructure (intelligence systems, processes, etc.), and/or resources (intelligence funding, personnel, etc.).

a. Intelligence Manpower. This category should be addressed if the operational or support aspects of a capability solution will require intelligence personnel for any and all phases (to include development, testing, training, and operation) of the acquisition life cycle. Depending on the maturity of the capability solution, a Manpower Estimation Report (MER) may have been completed.

(1) Associated Generic Capabilities: Potentially all.

(2) Qualitative Attributes: Address whether existing skills and specialties suffice, or if specific skills are required for support. Address whether specialized training will be required.

(3) **Quantitative Attributes:** Address how existing intelligence or other support personnel/billet resources will meet the capability solution's intelligence support requirements or whether the capability solution will require additional, dedicated intelligence personnel/billets - either with additional organic support within the Sponsor's organization, by leveraging support from other organizations, or by training new personnel to fill the anticipated support requirements.

b. **Intelligence Resource Support.** This category should be addressed if either the capability solution itself, or required intelligence support capabilities will depend upon intelligence funding. In particular, these dependencies should be identified if the capability solution will rely upon intelligence capabilities that have not yet been provided dedicated funding, or involve capability solutions that have not received necessary approvals to begin operations or may not retain approval to remain operational,

(1) **Associated Generic Capabilities:** Potentially all.

(2) **Qualitative Attributes:** Not applicable.

(3) **Quantitative Attributes:** Address whether and to what extent the capability solution relies upon non-funded or underfunded programs (i.e., to what extent, if at all, is the capability solution reliant upon elements that are being planned, are awaiting development, or otherwise not yet in existence).

c. **Collection Management Support.** This category refers to both management of collection assets and identification and management of intelligence information requirements. The collection management process converts intelligence information requests into information requirements, validates the requirements by ensuring the information is not already available, and then tasks collection assets to collect the information. At the strategic and operational level, collection management support refers to the personnel, expertise, training, and systems required to ensure intelligence collection assets, including national, joint, Coalition, and multinational, are effectively employed to collect the information required. At the tactical level, collection management support refers to the personnel, expertise, training, and systems required to ensure intelligence information requests are submitted through the appropriate channels, and that collected information is disseminated to the requestor and any other end users.

(1) **Associated Generic Capabilities:** Intelligence collection assets; intelligence collection management assets; intelligence operations, tactics, techniques, and procedures (TTPs); assets involving strategic decision-making

functions; and, programs with intelligence information needs to support their operation(s).

(2) Qualitative Attributes: Level of training required for personnel, system knowledge required, level of national/Coalition interoperability to enable timely intelligence collection management, types of intelligence information needed (form and substance), and specific collection asset capabilities that will be needed to collect the requested information.

(3) Quantitative Attributes: Address what intelligence information needs the capability solution will require during its life cycle. Identify, if possible, what entities will provide the required collection management support and whether the entities will have the capacity to provide such support.

d. Signature Support. Signature support refers to either the collection and measurement of signature data – unique, detectable characteristics that describe or define specific equipment, events, or locations associated with a specific adversary capability, system, or other type of target – or the programs/algorithms required to make signature data useable. This data may be used by intelligence analysts, automated systems, and system design and development engineers to analyze and identify threats or the patterns of use of an adversary system.

(1) Associated Generic Capabilities: Assets required to detect, identify, classify, and/or characterize emitters (generally equipment and systems) in the battlespace/operational environment.

(2) Qualitative Attributes: Format; content; reliability; data fidelity; accuracy; timeliness; static versus dynamic data; frequency range required; specific target types to be detected, identified, or characterized; level of automation and data fusion required; and compliance with SSP standards.

(3) Quantitative Attributes: Volume of data required.

e. Geospatial Intelligence (GEOINT) Support

(1) GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth.

(a) GEOINT provides two critical components that contribute to the effectiveness of weapons and weapon systems:

1. A framework that renders other intelligence actionable by virtue of referencing it to a four-dimensional space-time context.

2. Critical qualitative and quantitative information to describe the physical and functional characteristics of the political, economic, military, social, informational, and infrastructure components of an adversary's capabilities.

(b) The fusion of imagery-based intelligence (to include imagery-based measurement and signals intelligence (MASINT)) with geospatial information to create GEOINT conveys understandings of enemy assets and actions that play a dominant role in determining weapon and weapon system effectiveness. The critical contribution of GEOINT to effectiveness spans all categories of capabilities, kinetic/non-kinetic and lethal/non-lethal, as well as the entire breadth of planning and execution, from the initial selection of potential target systems and targets down to the specific details of discrete target construction, functional attributes, and operating patterns, and into the three phases of combat assessment.

(c) GEOINT support refers to a capability solution's requirement for geospatial information, services, or products traditionally associated with the mapping, charting, and geodesy disciplines. To fulfill geospatial requirements for capability solutions, Sponsors must factor in significant lead times needed to accommodate the planning, allocation, and de-confliction of geospatial information and services (GI&S)-related collection, analytic, and dissemination resources that are consistently in high demand. Compliance with National Geospatial-Intelligence Agency (NGA) standards and dissemination policies is a mandatory requirement.

(d) Different missions require different types of GEOINT support and create different effects upon IC members providing geospatial intelligence, including impacts on collection assets, intelligence systems, and manpower (e.g., collection managers, analysts, etc.).

(e) Early and concise identification of GEOINT shortfalls for decision-making, planning, and execution to optimize weapon and weapon system effectiveness is a matter of critical concern when the IC must justify resource requirements and apportionment of those resources within the agency.

(2) Associated Generic Capabilities: Potentially all.

(3) Qualitative Attributes: Required data, coverage, scale, timeliness (including periodic or as-needed update requirements), formats, accuracy, resolution level (e.g., imagery and/or Digital Terrain Elevation Data (DTED) levels, and desired product format (electronic versus paper).

(4) Quantitative Attributes: Addresses the numeric quantity of products and the demand (level) for services.

f. Targeting Support

(1). Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities, as described in reference rrr2.

(a) The requirement for targeting support refers to a wide range of intelligence information, products, and services throughout all levels of warfare and, for the purposes of the intelligence certification, throughout all phases of the acquisition life cycle. Intelligence support to targeting may be required during munition design, development, and testing to help ensure the anticipated munition performance. Munitions effects assessment (MEA) and battle damage assessment (BDA) studies may help identify capability gaps in the force application portfolio.

(b) Sponsors with capability solutions that will employ or rely on the employment of munitions must also consider intelligence support to targeting and identify and address intelligence support requirements and shortfalls, if any, regarding not only the their capability solution but the munitions it will employ or rely upon. (i.e., intelligence support to targeting is a broad category that encompasses munitions and all associated capability solutions relying upon the munition).

(c). During the operational and sustainment phases of acquisition, targeting support refers to the intelligence information, infrastructure, or resources required:

1. To support Commanders Critical Intelligence Requirements (CCIRs), Priority Intelligence Requirements (PIRs), and development of objectives, guidance, and intent.

2. For target development (to include derivation of coordinates), validation, nomination, and prioritization.

3. To support planners at national, strategic, and tactical/operational levels.

4. To support capabilities analysis and force assignment.

5. To support mission planning and execution (e.g., mission planning support such as weaponeering, target imagery notation, collateral damage estimation, and coordinate verification at the unit levels).

6. To support operational execution (e.g., time-sensitive targeting support such as target identification, coordinate derivation, and weaponeering).

7. To support the combat assessment process (to include BDA, MEA, and supporting re-attack recommendations).

(c). Examples of targeting products include target lists, target folders, target materials, modeling and simulation products, and collection and exploitation requirements to support targeting and target briefs. Examples of targeting services include weaponeering, casualty and collateral damage estimation, point positioning/coordinate mensuration, and verification and tactical mission planning support. Note: Targeting support may overlap with the GI&S Support category because many targeting services rely upon and/or incorporate geospatial products or information.

(2) Associated Generic Capabilities: Systems that will perform or manage the application of force or conduct information operations.

(3) Qualitative Attributes: Qualitative attributes will vary greatly by specific products required, but examples could include format specifications, accuracy requirements, and timing requirements. Coordinate-seeking weapons, or weapons that can or will be able to operate in a coordinate-seeking mode, must declare required target location error -- expressed as circular and linear error in meters or feet -- with an associated confidence level.

(4) Quantitative Attributes: Quantitative attributes will also vary greatly by specific product or service required but could refer to volume of targets managed and numbers of target folders produced, numbers of missions, and associated targets or aimpoints to plan for during mission planning.

g. Combat Search and Rescue (CSAR) Intelligence Support

(1) CSAR is the specific task performed by rescue forces to recover distressed personnel during war or military operations other than war, as described in [reference rrr3](#). Intelligence plays a vital role in planning and accomplishing CSAR operations because intelligence pertaining to the adversary's threat will have the greatest influence on search criteria and the method of recovery selected. Due to the sensitivity of the information required, inherent jointness, and time-critical nature of most CSAR operations, unique CSAR intelligence support requirements may include:

(a) Understanding joint CSAR TTPs.

(b) Familiarity with selected areas for escape, evasion, contact points, and helicopter landing zones.

(c) Familiarity with national intelligence support to CSAR operations.

(d) Understanding complex communication methods and procedures throughout the tactical, operational, and strategic levels.

(e) Understanding and documenting the particular and discrete signature data associated with specific CSAR events.

(2) Associated Generic Capabilities: Capability solutions with a CSAR mission.

(3) Qualitative Attributes: Information accuracy and timeliness, training levels, the ability to reach back and timeliness of reach back, and the ability to integrate information and operations with national and/or joint intelligence assets and capability solutions.

(4) Quantitative Attributes: Will most likely be determined by intelligence manpower requirements and whether, or the degree to which, CSAR is the capability solution's primary mission.

h. Intelligence Preparation of the Operational Environment (IPOE)/Joint Intelligence Preparation of the Operational Environment (JIPOE)

(1) Reference rrr4 defines JIPOE as a continuous process that enables joint force commanders and their staffs to visualize the full spectrum of adversary capabilities and potential courses of action across all dimensions of the battlespace. IPOE, in contrast, has a narrower scope than JIPOE and consists of an analytic methodology focused on reducing uncertainties concerning the enemy, environment, and terrain for all types of operations.

(2) As with all intelligence support categories, IPOE support can apply throughout the acquisition life cycle, and the complexity associated with this type of support varies substantially based upon the scope of the battlespace involved. For example:

(a) Ensuring capability solutions are designed, delivered, and operated with the most current, continually updated, and validated threat information available -- an issue that is specifically addressed by DWO's threat validation review.

(b) Ensuring that personnel and platforms operating within the battlespace are provided with accurate and timely assessments of adversarial intentions, tactics and capabilities, and relevant threat models during both the planning and execution phases of operational missions.

(3) Associated Generic Capabilities: With regard to threat support to pre-operational phases of the acquisition life cycle, this requirement will apply to almost any proposed system (to include open-architecture information technology systems). With regard to IPOE support needs during the operational phase of the acquisition life cycle, this requirement will apply to any personnel or platform physically operating in the battlespace. In terms of IPOE support subcategories, these would apply to specialized platforms or sensors tailored for such missions.

(4) Qualitative Attributes: Accuracy, timeliness, frequency, format, latency, types of threat information required.

(5) Quantitative Attributes: Addresses the numeric quantity of products and the level of demand for intelligence support.

i. Warning Support

(1) Military intelligence has the responsibility of communicating threat information to decision makers in order to avoid surprise. Avoiding surprise requires the timely dissemination of relevant information that causes a decision-maker to act in a way that prevents, avoids, or defeats an emerging threat.

(a) Warning support (i.e., “Indications and Warning”) usually involves two steps:

- 1 Identifying and defining a potential threat.
- 2 Monitoring the threat.

(b) Warning support must be considered throughout the acquisition life cycle

(c) Warning support prior to a capability solution’s operational phase may be thought of as information that enables that capability solution to remain scientifically and technologically superior relative to developing or projected adversary capabilities. The ability to provide this support depends upon direct involvement of the sponsor or program manager in identifying critical intelligence categories (CICs). CICs refer to general or specific adversarial capabilities that, if developed, procured, or implemented, could

significantly influence the effective operation of the sponsor's program or capability. CICs therefore support the development of intelligence production requirements (and associated intelligence collection requirements) that support a sponsor's program or capability. (Note: Warning support with regard to CICs is continued throughout a capability solution's life cycle.)

(d) Warning support also includes providing programs with specific intelligence-derived products to forewarn the Sponsor of specific, imminent, and hostile adversary intent or events. For additional detail regarding this type of support, refer to the SIPRNET and Joint Worldwide Intelligence Communications System (JWICS) websites identified in [reference rrr5](#).

(2) Associated Generic Capabilities: Potentially all.

(3) Qualitative Attributes: Accuracy and timeliness of information, format of information, frequency of collection and reporting, information updates, and means of communicating information and relevance to decision making.

(4) Quantitative Attributes: This type of support is difficult to quantify, but may be addressed in terms of high, medium, or low demand levels. Depending on the technological complexity of the capability solution, the level of required warning support will vary, although the numbers of CICs developed may be an indicator of the level of support required. For operational warning support, warning support demand levels will vary by the primary mission of the capability solution.

j. Space Intelligence Support. Space intelligence support refers to intelligence information, infrastructure, or resources that provide space-specific intelligence analysis on foreign space capabilities, as described in [reference rrr6](#).

(1) Associated Generic Capabilities: Space-based capability solutions; those relying upon space-derived capabilities or requiring visibility into the foreign space picture; and those performing space control or space support, space enhancement, and space application.

(2) Qualitative Attributes: Accuracy and timeliness of information, frequency of collection and reporting information, format, information updates, and types of threat information required.

(3) Quantitative Attributes: Addresses the numeric quantity of products and the demand levels for services.

k. CI Support. CI, as outlined in [reference rrr7](#), refers to the process of gathering information on, and activities conducted to counter, adversary or other collection activities directed against U.S./allied forces, other intelligence activities, sabotage or terrorism conducted by, or on behalf of, foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist entities. CI support refers to the intelligence information, infrastructure, or resources used to educate acquisition communities on those threats. CI support also helps acquisition communities establish plans, tools, or techniques to protect designated science and technology information and critical program information from such threats in accordance with [reference rrr8](#). As with other requirements, CI support can and should be applied throughout a capability solution's life cycle. CI support may include a number of activities, from providing threat awareness education to scientists and engineers performing fundamental research to the implementation of a program protection plan.

(1) Associated Generic Capabilities: Potentially all.

(2) Qualitative Attributes: May include format of information, training level of CI personnel involved, timeliness requirements, and compliance with [reference rrr8](#).

(3) Quantitative Attributes: Entails determining the general level of effort required to plan, institute, and maintain a CI support plan or program (in terms of people, resources, etc.).

1. Intelligence Training Requirements. Some programs may require intelligence personnel to receive specialized training to support part or all phases of a given capability solution's life cycle. The training requirement may include training additional personnel in existing training programs and/or training additional personnel in a new, unique training program that will be developed to support the capability solution. In either case, the requirement for specific training to support any phase of a capability solution's life cycle must be identified, analyzed, and declared as soon as possible in the JCIDS process to permit sufficient lead time to develop personnel with the skills required to support the capability solution.

(1) Associated Generic Capabilities: Potentially all.

(2) Qualitative Attributes: Certifications required, skill specialties required (e.g., Air Force Specialty Code, Military Occupational Specialty), schools/courses required, language skills, whether there will be a requirement for a new or unique training program (and/or a need to develop new technology) to support the capability solution.

(3) Quantitative Attributes: Initial and recurring intelligence training requirements depend upon the amount of manpower required to support the capability solution and whether the capability solution requires a unique training program.

m. Dissemination Support. Although the movement toward a net-centric environment has reduced some technical challenges related to information dissemination, intelligence infrastructure (such as intelligence networks, systems, and software) and intelligence resources (such as funded programs or manpower) remain a critical means of information delivery. One way to determine a capability solution's requirement(s) for dissemination support is to examine relevant crosswalks with key intelligence ICDs. Another measure of dissemination support is compliance with IC and DOD data and metadata standards.

(1) Associated Generic Capabilities: Capability solutions that provide intelligence information; manpower, and resources to compile and deliver information; manpower, and resources to operate and maintain delivery systems and capabilities.

(2) Qualitative Attributes: Timeliness of delivery, means of delivery, interoperability of delivery/communications systems, format of information delivered, and information updates.

(3) Quantitative Attributes: Types of delivery/communications systems required, personnel needed to support a given capability solution, volume of information that will be delivered. Sponsors must consider and address the capability solution's effects on the capacity and ability of the system/capability delivering the information to continue operations and support other requirements (e.g., impact on bandwidth) and security considerations related to the information and source of information (e.g., human intelligence (HUMINT) controls), etc.

3. Requirements by Intelligence Category Descriptions. Sponsors must also address how their capability solutions comply with requirements imposed by intelligence, such as security considerations, classification levels of information and systems, procedures or authority to release or handle classified or sensitive information, and interoperability with supporting intelligence systems.

#### 4. Intelligence Supportability Content in Documents

a. This section of the guide provides guidance on drafting intelligence supportability content JCIDS documents, including paragraph-by-paragraph guidance concerning basic information and analysis that sponsors must

consider and address when appropriate. This section also serves as a reference to reviewers during the intelligence certification review process.

(1) While the threat and operational environment paragraph and the intelligence supportability paragraph of ICDs, CDDs, and CPDs are the primary intelligence-focused paragraphs in JCIDS documents, other paragraphs may need to consider intelligence support or integration concepts.

(a) Threat and Operational Environment. The intent of the threat and operational environment paragraph is to ensure capability requirements and associated capability gaps, as well as the capability solutions developed to close or mitigate the capability gaps, are based upon a consistent and up to date threat assessment, and that threat assessments are updated as needed before validation of successor documents.

(b) Intelligence Supportability. The intent of the intelligence supportability paragraph is to set forth all intelligence support requirements and anticipated shortfalls throughout the acquisition life cycle of capability solution in one, comprehensive section of the CDD or CPD.

(c) If threat or intelligence support related issues are addressed in other sections of the document, then provide a reference to the applicable paragraph in these paragraphs, and do not replicate material unnecessarily.

(2) This guidance is general in nature and must be adapted on a case-by-case basis. Each capability solution will have unique intelligence support requirements; thus, the support information section in ICDs or intelligence supportability paragraph in CDDs or CPDs should reflect a tailoring of these requirements.

(3) Understanding and specifying intelligence support requirements or shortfalls will become more refined as the program progresses through the JCIDS process, from ICDs to CDDs to CPDs.

(4) Significant changes to existing threats or the emergence of new threats associated with validated capability requirements and the development of related capability solutions may drive changes to the development of capability solutions. If updates to threat validation and other aspects of JCIDS document validation are required to react to unanticipated threat changes, see Enclosure C of this Manual for details on updates to and revalidation of JCIDS documents.

b. ICD Content

(1) ICDs address general capability requirements and associated capability gaps within an area of interest, rather than defining specific capability solutions. ICDs should therefore identify general intelligence support requirements associated with closing or mitigating the identified capability gaps. Although ICDs do not contain a paragraph dedicated to intelligence supportability, there are intelligence-related issues sponsors should consider and address, if applicable, when drafting these documents.

(2) ICD Paragraph Considerations. Consider intelligence related content in each section of the ICD as shown in Table B-I-1.

<b>Para</b>	<b>Title</b>	<b>ICD Considerations</b>
1	Operational Context	Ensure the CONOPS discussion includes intelligence-based support requirements, resources, or other programs/capabilities that are required to enable the desired outcome(s).
2	Threat Summary	No additional requirements - see the ICD format in Enclosure B of this Manual for guidance.
3	Capability Requirements and Gaps/Overlaps	Ensure that all intelligence support requirements, resources, or other programs/capabilities necessary to enable each capability are identified in terms of the broad descriptions of categories discussed in this Enclosure. Ensure that any current or projected gaps or shortfalls in intelligence support capabilities are identified.
4	Assessment of Non-Materiel Approaches	Ensure intelligence related aspects of DOTmLPF-P approaches are adequately identified and discussed in this paragraph. Ensure the documentation reflects that the IC's expertise has been adequately leveraged.
5	Final Recommendations	Ensure materiel and non-materiel recommendations reflect a thorough understanding of the threat considerations and intelligence support requirements and capabilities for the functional and operational areas.
App A	Architecture Data	Ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the OV-1, and that the illustration is consistent

		with the CONOPS described in paragraph 1 of the ICD.
App B	References	Provide citations to all applicable intelligence related references. At a minimum, cite references rrr12 and rrr13 for all JROC Interest, JCB Interest, and Joint Integration documents.
App C	Acronym List	No additional requirements - see the ICD format in Enclosure B of this Manual for guidance.
App D	Glossary	No additional requirements - see the ICD format in Enclosure B of this Manual for guidance.

Table B-I-1. ICD Intelligence Considerations

c. CDD and CPD Content

(1) The level of discussion and analysis in CDDs and CPDs is more refined than that contained in ICDs, and addresses specific support requirements for the capability solution discussed in the CDD or CPD. As a capability solution progresses from CDD to CPD, sponsors will be responsible for increasing levels of refinement and analysis relating to intelligence supportability and shortfalls.

(2) CDD and CPD Paragraph Considerations. Consider intelligence related content in each section of the CDD and CPD as shown in Table B-I-2.

<b>Para</b>	<b>Title</b>	<b>CDD and CPD Considerations</b>
1	Operational Context	Ensure any key intelligence support capabilities required to enable the capability solution's operational activities are addressed within the operational context outlined for the capability requirements.
2	Threat Summary	No additional requirements - see the CDD or CPD format in Enclosure B of this Manual for guidance.
3	Capability Discussion	Ensure the capability discussion includes interactions with intelligence capabilities where appropriate and adequately addresses detail and scope to allow sufficient supportability analysis. Ensure the summary of analysis highlights any intelligence related analyses considered.

4	Program Summary	Address whether the capability solution will be subject to, or affected by, any undeveloped (or underdeveloped) intelligence technologies, or will be affected by the deactivation of existing intelligence programs. Consider whether this will affect the effectiveness and timely delivery of the capability solution or increment. Ensure intelligence related dependencies between these capabilities are defined (e.g., information exchange) and are consistent with the related documents. Ensure all timeframes for any enabling or program-required/dependent intelligence capabilities (existing and future) are consistent with the capability solution's development schedule and planned IOC and FOC.
5	Development or Production KPPs, KSAs, and additional performance attributes	Ensure identification of KPPs, KSAs, and additional performance attributes that are dependent upon or enabled by intelligence resources or support. Ensure that objective and threshold values for intelligence related attributes are supported by adequate information and analysis, and rationale for each KPP complies with the analysis and findings of the applicable intelligence ICDs.
6	Other System Attributes	Ensure that programs or capabilities that will collect, transmit, or receive information, data, or direction from an external source requiring information flow/communications (e.g., an ISR platform), have considered appropriate information assurance measures and are in place prior to operational testing and fielding of the capability solution.
7	Spectrum requirements	If the capability will interface with, or use, JWICS or other intelligence managed dissemination systems to receive or transmit information, ensure bandwidth requirements and quality of service requirements are addressed. If there are potential issues regarding E3 interference from threat emitters, ensure these issues are identified in this section. Ensure this section is consistent with the threat

		discussion in paragraph 2 or in the related System Threat Assessment Report (STAR).
8	Intelligence Supportability	See guidance provided in the next section of this Enclosure for details of the Intelligence Supportability paragraph.
9	Weapon Safety Assurance	No additional requirements - see the CDD or CPD format in Enclosure B of this Manual for guidance.
10	Technology or Manufacturing Readiness Assessment	Ensure any critical intelligence related technologies are addressed.
11	DOTmLPF-P Considerations	Ensure any intelligence-related DOTmLPF-P considerations, identified through related ISP processes or during analysis done for paragraph 8, are addressed.
12	Program Affordability	Ensure resources required to address intelligence-related aspects of the capability solution are captured in the summary of resources required.
App A	Architecture Data	Ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the OV-1, and that the illustration is consistent with the CONOPS described in Para 1.
App B	References	Provide citations to all applicable intelligence related references. At a minimum, cite <b>references rrr12 and rrr13</b> for all JROC Interest, JCB Interest, and Joint Integration documents.
App C	Acronym List	No additional requirements - see the CDD or CPD format in Enclosure B of this Manual for guidance.
App D	Glossary	No additional requirements - see the CDD or CPD format in Enclosure B of this Manual for guidance.

Table B-I-2. CDD and CPD Intelligence Considerations

(3) Intelligence Supportability paragraph of CDDs and CPDs.

(a) Sponsors must identify, analyze, and discuss the capability solution's current and projected requirements for intelligence support (e.g., manpower, resources, and processes), and if applicable, any intelligence support shortfalls and/or impact on joint intelligence strategy, policy, and architecture planning. This paragraph must address all requirements for

intelligence support to a capability solution, regardless of whether the intelligence support required will be unique to the capability solution or common with other capability solutions.

1. Consider whether each of the intelligence support categories will be available, suitable, and sufficient throughout all phases of a given capability solution's acquisition life cycle, from the "pre-operational" phases (such as development, testing, and training) to the operational and sustainment phases of the acquisition life cycle.

2. Leverage work done for the ISP. Review the completed or ongoing analysis and architecture data from the capability solution ISP Information Needs Discovery and Analysis Process to identify intelligence supportability issues. Ensure that all intelligence requirements are captured within the architecture data in sufficient detail to assess supportability.

3. For all intelligence requirements identified, address what intelligence infrastructure (e.g., platforms, systems, software, facilities) and resources (e.g., manpower, funding) will be required to collect, compile, store, analyze, and disseminate the intelligence required. The Sponsor is not expected to "reverse analyze" the entire intelligence cycle back to the source collection; but rather use best efforts to anticipate the required support, paying particular attention to what intelligence systems, assets, and personnel may be needed to fulfill sponsor's intelligence needs.

(b) Recommended paragraph format. Introduce the paragraph with a general description of the types and level of intelligence support required to enable the capability solution. For subparagraphs below, be as specific as possible, and include all appropriate qualitative and quantitative attributes. If details regarding required qualitative or quantitative attributes are unknown, state what is not known and why.

1. Intelligence Support to Development and Testing. Address intelligence threat and threat warning support necessary for development and testing of the capability solution, and refer to Paragraph 4 of the CDD or CPD as appropriate. Sponsor must ensure that intelligence information or services required for the effective operation of the capability solution can be tested in its anticipated operational environment.

2. Intelligence Training. Address what intelligence training requirements may be required for personnel supporting the capability solution. Sponsors should address unique training requirements, if any, that the capability solution will require from its intelligence personnel (e.g., unique skills or knowledge, such as targeting or HUMINT experience) and non-intelligence personnel (e.g., security concerns, SAP requirements, etc.).

3. Intelligence Support to Training. Address whether intelligence support, systems, and/or resources are required to enable or contribute to any training programs associated with supporting the capability solution.

4. Intelligence Support to Operations. Address all requirements for intelligence support that will be necessary to ensure successful operation and sustainment of the capability solution.

5. Intelligence Security Requirements. Identify all security requirements or considerations that the capability solution will require, and address how those security considerations are satisfied (e.g., classification levels; information sharing or releasability; certifications, and facility implications for receiving, using, and storing Sensitive Compartmented Information (SCI); and all other security considerations that the capability solution will require for compliance with references rrr10 and rrr11.

6. Potential Intelligence Support Shortfalls. Consider and address known, projected, or potential intelligence support shortfalls, including shortfalls related to the capability solution itself, those caused by the capability solution that affect other existing or planned capability solutions, or which may exacerbate currently known intelligence support shortfalls.

a. Particular focus should be placed on shortfalls that could affect or delay development, testing, or fielding the capability solution, or those shortfalls that may degrade operational effectiveness or sustainment.

b. Identify the nature of these shortfalls, such as technological capability shortfalls, undefined common intelligence data/metadata standards, scheduling problems, or funding issues, and if possible, estimate the magnitude of the shortfall in terms of scheduling delays, vulnerability, materiel, resources, training, manpower, and any other relevant criteria. Note that information related to intelligence shortfalls may be, or may become, classified information when associated with a shortfall; therefore, sponsors must ensure compliance with all necessary security procedures.

c. Proposed Solutions. Provide a plan and schedule to address each identified shortfall, including key issues that must be resolved. If the solution lies outside the control of the Sponsor, or is deemed to be unobtainable under the existing intelligence infrastructure, manpower, etc., provide a recommendation on how to work around the shortfall, and identify the organization with the authority and responsibility to address the shortfall.

d. Joint DCR Document Content

(1) While many Joint DCRs do not require threat validation or intelligence certification, some may be driven by changes to threat environment, or propose DOTmLPF-P changes which affect intelligence supportability of existing capability solutions. In addition, some Joint DCRs may be specifically focused on intelligence activities or existing capability solutions. In these cases, an intelligence certification will generally be required.

(2) Joint DCR Paragraph Considerations. Consider intelligence related content in each section of the Joint DCR as shown in Table B-I-3.

<b>Para</b>	<b>Title</b>	<b>Joint DCR Considerations</b>
1	Operational Context	Ensure any key intelligence support capabilities affected by the changes to DOTmLPF-P are addressed within the context of the CONOPS.
2	Threat Summary	No additional requirements - see the Joint DCR format in Enclosure B of this Manual for guidance.
3	Capability Discussion	Ensure any key intelligence support capabilities affected by the changes to DOTmLPF-P are addressed. Ensure the summary of analysis highlights any intelligence related analyses considered.
4	Change Recommendations and Implementation Plans	Ensure that existing or newly introduced key intelligence support capabilities affected by the changes to DOTmLPF-P are identified and adequately addressed in the implementation plan
5	Constraints	Ensure that new intelligence shortfalls driven by resource constraints, or existing shortfalls aggravated by the changes to DOTmLPF-P, are addressed. Ensure intelligence related policies affecting, or affected by, the DOTmLPF-P changes are addressed. Ensure that new intelligence shortfalls driven by reasons other than resource constraints or policy, or existing shortfalls aggravated by the changes to DOTmLPF-P, are addressed.
App A	Architecture Data	Ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated in the

		OV-1, and that the illustration is consistent with the CONOPS described in Para 1.
App B	References	Provide citations to all applicable intelligence related references. At a minimum, cite references rrr12 and rrr13.
App C	Acronym List	No additional requirements - see the Joint DCR format in Enclosure B of this Manual for guidance.
App D	Glossary	No additional requirements - see the Joint DCR format in Enclosure B of this Manual for guidance.

Table B-I-3. Joint DCR Intelligence Considerations

DRAFT

- rrr2. JP 3-60, 13 April 2007, "Joint Targeting"
- rrr3. JP 3-50, 20 December 2011, "Personnel Recovery"
- rrr4. JP 2-01.3, 16 June 2009, "Joint Intelligence Preparation of the Operational Environment"
- rrr5. DOD Indications and Warning System Operations Manual website. On SIPRNET – [http://www.dia.smil.mil/intel/j2/j2m/pubs/j2m-0177-01-96/j2m-0177-01\\_cov.html](http://www.dia.smil.mil/intel/j2/j2m/pubs/j2m-0177-01-96/j2m-0177-01_cov.html). On JWICS – [http://www.dia.ic.gov/intel/j2/j2m/pubs/J2M-0177-01-96/J2M-0177-01\\_cov.html](http://www.dia.ic.gov/intel/j2/j2m/pubs/J2M-0177-01-96/J2M-0177-01_cov.html).
- rrr6. JP 3-14, 6 January 2009, "Space Operations"
- rrr7. JP 2-01.2, 16 March 2011 incorporating Change 1 of 26 August 2011, "Counterintelligence and Human Intelligence in Joint Operations (U)"
- rrr8. DODI 5200.39, 16 July 2008 incorporating Change 1 of 28 December 2010, "Critical Program Information (CPI) Protection Within the Department of Defense"
- rrr9. DTM 09-013, 18 December 2009 incorporating Change 3 of 9 January 2012, "Registration of Architecture Descriptions in the DoD Architecture Registry System (DARS)"
- rrr10. DCID 6/3, 5 June 1999 **(still valid version??)**, "Protecting Sensitive Compartmented Information within Information Systems"
- rrr11. DCID 6/9, 18 November 2002 **(still valid version??)**, "Physical Security Standards for Sensitive Compartmented Information Facilities"
- rrr12. DIAD 5000.200, 19 January 2005, "Intelligence Threat Support for Major Defense Acquisition Programs"
- rrr13. DIAI 5000.002, 30 March 2005, "Intelligence Threat Support for Major Defense Acquisition Programs"
- rrr14. J282/IRCO Intelligence Certification Tool. On SIPRNET - <http://j2sid.js.smil.mil/IntelCertification/j2sid.html>. On JWICS - <http://164.185.180.14:8001/IntelCertification/j2sid.html>

(INTENTIONALLY BLANK)