

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-2

DISTRIBUTION: A, B, C, JS-LAN, S

CJCSI 3312.01B

10 June 2010

JOINT MILITARY INTELLIGENCE REQUIREMENTS CERTIFICATION

References: See Enclosure F.

1. Purpose. The purpose of this instruction is to establish the policies and procedures for Joint Military Intelligence Requirements Certification of capabilities being reviewed under the Joint Capabilities Integration and Development System (JCIDS), as specified by the CJCS 3170.01 series directives (references a and b). The procedures established by this instruction support the Joint Staff Director for Intelligence (J-2) and the Intelligence Review and Certification Office (J282/IRCO or IRCO) in identifying, assessing, and certifying capabilities reviewed pursuant to the JCIDS process. The intelligence review process supports programs in the JCIDS acquisition process and is based on a collaborative, analytical process that evaluates what proposed capabilities will require from, or contribute to, the intelligence enterprise throughout their acquisition life cycle. The intelligence certification is a statement of adequacy based on previously completed reviews and assesses whether the projected intelligence architecture will be available, suitable, and sufficient to support those needs. This instruction establishes:

a. Policies, procedures, and criteria for intelligence review and certification of all JCIDS documents, and of information support plans (ISPs) in accordance with the CJCS 3170.01 series, the current version of the CJCSI 6212.01 series, DODI 4630.8, and the Acquisition Knowledge Sharing System Deskbook (references a, b, d, h, and l).

b. Policies and procedures for Defense Intelligence Agency (DIA) validation of threat intelligence support to the JCIDS analysis and document development process, as required by the CJCS 3170.01 series (references a and b).

2. Cancellation. CJCSI 3312.01A, 23 February 2007, "Joint Military Intelligence Requirements Certification," is hereby canceled.

3. Applicability

a. This instruction:

(1) Applies to initial capabilities documents (ICDs), capability development documents (CDDs), and capability production documents (CPDs), and updates or annexes (hereafter collectively referred to as “JCIDS documents”). All programs designated as Joint Requirements Oversight Council (JROC) interest (“JROC interest”) and “Joint Integration” joint potential designators (JPDs) by J-8 shall undergo intelligence certification according to this instruction, unless a written waiver has been granted by J282/IRCO (see the definition of “JPD” in the Glossary for an explanation of JROC interest and Joint Integration designations). Waiver requests will be considered on a case-by-case basis, and such requests shall be evaluated on the degree to which a program or capability is determined to consume, produce, process, or handle intelligence (throughout any and all stages of the acquisition life cycle). Document sponsors should use enclosures C and E as primary guides to assess whether, or to what extent, programs and capabilities produce, consume, process, or handle intelligence. Sponsors must coordinate waiver requests directly with the responsible J282/IRCO staff member prior to submission of a sponsor’s program document into the JCIDS process or, if the waiver is sought for a particular phase or milestone, prior to that given phase or milestone (see Enclosure B for an explanation of the review process, including milestones and phases).

(2) Applies to all entities subject to the JCIDS review process, in accordance with the CJCS 3170.01 series, which includes the Services, combatant commands, Joint Staff, Defense and national intelligence agencies, and joint and combined activities.

(3) Applies to agencies and organizations preparing and submitting Information Support Plans (ISPs) in accordance with DODI 5000.2, DODI 4630.8, and the Acquisition Knowledge Sharing System Deskbook (references f, h, and l). For simplicity and ease of reference, JCIDS documents and ISP documents shall be referred to collectively as “program documents” when appropriate.

b. Documents classified above Secret Collateral will also comply with this instruction but may be tailored as necessary to account for special security handling considerations (see the CJCSM 3170.01 series, reference b, for additional guidance).

c. This instruction complements and does not preclude the need to conform to the guidance and direction on defense acquisition, the JCIDS process, or other directions concerning intelligence support to acquisition (see

the CJCS 3170.01 series, the current version of the CJCSI 6212.01 series, DODD 5000.1, DODD 5000.2, and the Acquisition Knowledge Sharing System Deskbook -- references a, b, d, e, f, and l, respectively).

4. Policy

a. Objectives. The objective of Joint Military Intelligence Requirements Certification is to identify, at the earliest possible point, any and all likely intelligence support requirements and shortfalls (if applicable), and to ensure that continuous threat analysis of applicable adversary threat capabilities is completed and such threat information is incorporated into program documents throughout the JCIDS process to ensure the operational needs of U.S. military forces are satisfied. Intelligence certification shall seek to:

(1) Preclude fielding capabilities, systems, or programs that are unsupportable by the national and defense intelligence communities.

(2) Prevent scientific and technological surprise on the battlefield of the future by ensuring sponsors consider and incorporate the most current, applicable intelligence information, analysis, and findings into their programs and capabilities.

(3) Ensure that national and defense intelligence architectures remain capable of, and agile enough, to support future warfighting requirements by identifying and assessing possible intelligence support requirement shortfalls created by, or existing shortfalls aggravated by, programs and capabilities being reviewed in the JCIDS process.

b. Collaboration. Intelligence certification must be the result of a collaborative process that leverages the expertise and unique perspectives of all applicable DIA offices (in particular, the Directorate of Analysis, Defense Warning Office (DWO); the Directorate for Information Management and Chief Information Officer (DS); and the Directorate for Measurement and Signatures Intelligence and Technical Collection (DT)), and other applicable Joint Staff intelligence entities. On behalf of the J-2 directorate, J282/IRCO shall lead this collaborative intelligence certification process for the Joint Staff; consolidate and analyze comments from applicable DIA and Joint Staff entities; and make a final recommendation to the J28 concerning all intelligence certifications. Extensive cooperation, coordination, and collaboration are critical to ensure the full range of potential intelligence supportability issues is addressed.

c. Intelligence Certification

(1) The general path that a program or capability will follow through the JCIDS and intelligence certification process is set forth in the CJCS 3170.01

series (references a and b). This instruction complements the CJCS 3170.01 series and sets forth specific processes, procedures, and requirements that all sponsors must fulfill before intelligence certification will be considered for a given program or capability.

(2) The intelligence certification process will evaluate and analyze a program's intelligence support requirements for completeness, supportability, and impact on joint intelligence strategy, policy, and architectural planning. Sponsors shall be responsible for identifying and explaining each proposed or affected capability, and any and all associated intelligence support requirements and shortfalls related to such capabilities, to enable a complete analysis of the program in anticipation of intelligence certification. The intelligence certification will analyze programs for applicable threats and validate a program document's threat information. It will also evaluate intelligence-related systems with respect to security and intelligence interoperability standards. (Note: The J-6 directorate will perform a separate but related interoperability certification, which is explained in the current version of the CJCSI 6212.01 series (reference d).) Intelligence certification shall be completed at each milestone and in each phase of the JCIDS document drafting and review process, in accordance with the CJCS 3170.01 series and with this instruction. Descriptions of completeness, supportability, and impact on intelligence architecture, strategy, and policy are explained below.

(a) Completeness. Completeness refers to whether a sponsor's document adequately addresses requirements for intelligence support, and whether the capability or program complies with requirements by intelligence (as more fully explained below).

1. Requirements for Intelligence Support. It is understood that intelligence support requirements will become more readily identifiable and refined as a program or capability proceeds through the JCIDS process. Nevertheless, program documents must, as specifically as possible and at the earliest possible phase of review, identify and explain known or anticipated intelligence support requirements and shortfalls that sponsors expect will be necessary/result from the program -- the scope of this analysis includes the program's entire expected acquisition 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.). Sponsors must include qualitative and quantitative attributes (see the CJCSM 3170.01 series, Enclosure B) for each intelligence support requirement, if available. Enclosure C provides general descriptions of intelligence support categories, associated qualitative and quantitative attributes, and associated capabilities. Enclosure E provides a general format and guidance to

incorporate intelligence support information in specific paragraphs of JCIDS and ISP documents.

2. Requirements by Intelligence. Sponsors must also address how their capabilities or programs 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. Enclosure C provides additional guidance on these intelligence certification criteria.

(b) Supportability. Supportability refers to the availability, suitability, and sufficiency of intelligence support required by a program or capability. Assessing supportability requires a comparison of the sponsor's stated or derived intelligence support requirements with the expected intelligence support capabilities, as expected throughout a program or capability's life cycle. The ability to adequately assess supportability depends upon the completeness of the sponsor's declaration of support required by its program or capability, and must also be evaluated within the context of any shortfall mitigation strategies identified. Although availability, suitability, and sufficiency are discussed separately below, these criteria often overlap and do not necessarily represent discrete assessments (these assessments, therefore, may be combined when appropriate).

1. Availability: whether the intelligence information, infrastructure, or resources are, or are expected to be, available (i.e., the required intelligence support exists) to support the program or capability throughout all phases of its acquisition life cycle.

2. Suitability: whether the required intelligence information, infrastructure, or resources are, or are expected to be, appropriate to support the program or capability.

3. Sufficiency: whether the intelligence information, infrastructure, or resources are, or are expected to be, adequate to support sponsor's program or capability. Sufficiency may apply to quantitative as well as qualitative (i.e., specificity of information, types or forms of information, amount of analytical refinement, etc.) aspects of intelligence support.

(c) Impact on Intelligence Strategy, Policy, and Architecture Planning. Impact refers to the identification and analysis of additional inputs to, or outputs from, the intelligence community/infrastructure as a result of the sponsor's program or capability. Requirements for intelligence support may not be a concern with regard to the intelligence support infrastructure if planned products, information, or services are, or are already projected to be available, suitable, and sufficient throughout a program or capability's

acquisition life cycle. In other cases, programs or capabilities may require new types of support or a greater degree of/more demanding standard of support that differs from existing intelligence support. These additional inputs or outputs may also require changes across the doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) spectrum. In sum, these potential changes may have an impact on intelligence strategy, policy, and architecture that may require planning to support. This impact assessment provides a mechanism to provide critical feedback to the defense and national intelligence communities to identify actual or potential shortfalls in current and/or planned intelligence support, and provides a means to address these shortfalls at the earliest possible phase of development of a program or capability.

d. Threat Validation. All acquisition programs or capabilities that are expected to operate in a threat environment (lethal or non-lethal) must be developed in accordance with the most current threat information. The applicable threat information must, moreover, be continually updated to account for threats throughout the program or capability's projected acquisition life cycle, in accordance with the DWO threat analysis and findings. Sponsors shall also account for threats to research, development, testing and evaluation, production, and operation and maintenance resulting from technology transfer, espionage, and other adversarial collection efforts.

(1) Collaboration among the intelligence, counter intelligence, capability development, and capability acquisition communities shall be maintained throughout the JCIDS process to ensure technological superiority over adversarial capabilities is maintained. This collaborative effort shall begin with identifying all anticipated capabilities that adversaries might employ against the program or capability being reviewed, and including these threats as inputs to the sponsor's functional area analysis (FAA) (as discussed in the CJCSM 3170.01 series, reference b). Operational tasks, conditions, and standards identified in the FAA should then be submitted to DIA to enable production of an initial threat warning assessment (ITWA). The ITWA will identify projected adversarial threat capabilities, to include scientific and technological developments, which may affect a program or capability's design or implementation. DWO will assist sponsors with incorporating adversarial capabilities throughout the remainder of the program's JCIDS review process.

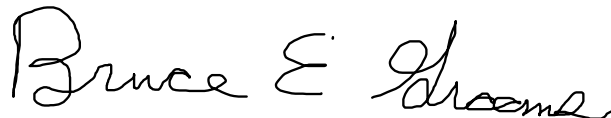
(2) All JCIDS program documents that are designated "JROC interest" or "Joint Integration" by J-8 must receive DWO threat validation for each phase of document review in the JCIDS process. DWO will validate sponsor's threat information and threat analysis by evaluating sponsor's JCIDS documents for appropriateness of judgments concerning the extent and scope of threats, ensuring consistency with DIA- or Service-validated threat assessments, and by ensuring that sponsor has included current threat references, information, and findings. See enclosures C and E for general intelligence areas of concern

10 June 2010

that sponsors must address before they receive DWO's threat validation and associated intelligence certification.

5. Definitions. Definitions are provided in the Glossary.
6. Responsibilities. Responsibilities are provided in Enclosure A.
7. Summary of Changes. This instruction has been extensively revised to reflect the current intelligence certification process that has evolved since the initial publication. For this reason, there is no summary of changes provided.
8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--
http://www.dtic.mil/cjcs_directives.
9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:



B. E. GROOMS
RADM, USN
Vice Director, Joint Staff

Enclosures:

- A -- Responsibilities
- B -- Intelligence Certification Procedures
- C -- Intelligence Support Requirement Category Descriptions
- D -- Intelligence Certification Summary and Letter
- E -- Program Document Guidance
- F -- References
- GL -- Glossary of Acronyms and Definitions

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C, and JS-LAN plus the following:

	<u>Copies</u>
Secretary of State.....	2
Secretary of Defense.....	2
Director of the Central Intelligence Agency	2
USD(AT&L)	2
USD(I).....	2
USD(P).....	2
ASD(NII)/DOD CIO.....	2
Director, National Geospatial-Intelligence Agency	2
Director, Defense Intelligence Agency	2

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of the document. An “O” indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 8	O	D-1 thru D-2	O
I thru viii	O	E-1 thru E-22	O
A-1 thru A-6	O	F-1 thru F-4	O
B-1 thru B-14	O	GL-1 thru GL-18	O
C-1 thru C-12	O		

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	<u>Page</u>
ENCLOSURE A -- RESPONSIBILITIES	
Joint Staff, J-2	A-1
Joint Staff, J-6	A-2
Joint Staff, J-8	A-2
Director, Defense Intelligence Agency (DIA)	A-3
Director, National Geospatial-Intelligence Agency (NGA).....	A-3
Director, National Security Agency/Central Security Service (NSA/CSS) .	A-4
Director, National Reconnaissance Office	A-5
Military Services	A-5
Combatant Commanders	A-5
Defense Information Systems Agency/Joint Interoperability Test Command (DISA/JITC).....	A-6
ENCLOSURE B -- INTELLIGENCE CERTIFICATION PROCEDURES	
Purpose	B-1
General	B-1
Certification Process	B-2
Intelligence Certification	B-10
Certification Failure.....	B-13
ENCLOSURE C -- INTELLIGENCE SUPPORT REQUIREMENT CATEGORY DESCRIPTIONS	
Intelligence Manpower	C-1
Intelligence Resource Support	C-2
Collection Management Support	C-2
Signature Support	C-3
Geospatial Intelligence Support (GEOINT)	C-3
Targeting Support	C-5
Combat Search and Rescue Intelligence Support	C-6
Intelligence Preparation of the Operational Environment (IPOE)/Joint ...	C-7
Intelligence Preparation of the Operational Environment (JIPOE)	
Warning Support	C-8
Space Intelligence Support	C-9
Counter Intelligence Support	C-10
Intelligence Training Requirements	C-10
Dissemination Support.....	C-11

ENCLOSURE D -- INTELLIGENCE CERTIFICATION SUMMARY AND LETTER

Intelligence Certification Summary D-1
Example JCIDS Intelligence Certification Letter D-2

ENCLOSURE E -- PROGRAM DOCUMENT GUIDANCE

Purpose E-1
General E-1
The Information Support Plan (ISP) Development Process and its
Connection to the JCIDS Process E-1
Joint Capabilities Integration and Development System Document
Development E-2
Guidance on Developing CDD and CPD Paragraph 9, “Intelligence
Supportability” E-9
Intelligence Supportability E-14
Information Support Plan Document Development E-16

ENCLOSURE F -- REFERENCES F-1

GLOSSARY OF ACRONYMS AND DEFINITIONS

Abbreviations and Acronyms G-1
Definitions G-4

FIGURES

Figure B-1. Association Between JCIDS and ISP Processes B-3
Figure B-2. JROC Interest Intelligence Certification Process B-7
Figure B-3. Joint Information and Independent Staffing Processes B-8
Figure B-4. Joint Integration Staffing Process B-9
Figure B-5. Intelligence Review and Certification Approval Authorities .B-11

TABLES

Table D-1. Intelligence Review and Certification Approval Authorities ... D-1
Table E-1. Initial Capabilities Document Intelligence Considerations E-4
Table E-2. CDD and CPD Intelligence Considerations E-9
Table E-3. ISP Intelligence Considerations E-17

ENCLOSURE A
RESPONSIBILITIES

1. Joint Staff, J-2

a. Provides intelligence support and advises the Joint Requirements Oversight Council (JROC) and supporting organizations on intelligence supportability and intelligence interoperability issues in support of the Joint Capabilities Integration and Development System (JCIDS) process, as required by the CJCS 3170.01 series and JSM 5100.01 series (references a, b, and bb).

b. As the certifying official on behalf of the JROC, the Director for Intelligence (DJ-2), shall implement the procedures of this CJCSI.

c. The Deputy Directorate for Battlespace Awareness (J28), Intelligence Requirements Certification Office (IRCO) (J282/IRCO), will act on behalf of the J-2 and the Deputy Director for Battlespace Awareness (J28), and shall be the lead intelligence entity within the Joint Staff concerning intelligence certification of JCIDS documents designated JROC Interest and Joint Integration. J282/IRCO shall also serve as the lead office within the Joint Staff for intelligence reviews of ISPs. Such reviews shall be completed in accordance with this instruction and in accordance with the CJCS 3170.01 series and DODI 4630.8 (references a, b, and h, respectively), regardless of acquisition category (ACAT) level (see the Glossary for an explanation of ACAT levels). J282/IRCO shall facilitate the intelligence certification process outlined in Enclosure B and shall receive, review, and consolidate comments from DWO, DS, DT, and all other appropriate Joint Staff and DOD intelligence entities concerning JCIDS and ISP document reviews.

d. The DJ-2, or his/her authorized designate, shall have final approval authority within the Joint Staff concerning all intelligence certification matters as they relate to this instruction, and shall provide intelligence certifications to the lead Functional Capability Board (FCB) for JROC interest designated programs. The J28, or his/her authorized designate, shall provide intelligence certifications to the sponsoring DOD component or agency for Joint Integration designated programs. (Note: The JROC, as the lead DOD entity in the JCIDS process, may review all intelligence certification actions completed by J-2 and has final approval authority over such intelligence certification matters. For the purposes of this instruction, the JROC's final approval authority will be assumed and, in any section stating final approval of intelligence certification, it will be assumed that the JROC has such authority.)

10 June 2010

e. J282/IRCO may, when appropriate, coordinate and compile comments from other Joint Staff intelligence entities (e.g., J26), Defense Information Systems Agency (DISA), the Office of the Under Secretary of Defense for Intelligence (OUSDI), the Office of the Assistant Secretary of Defense (Networks and Information Integration/DOD Chief Integration Officer) (OASD[NII]/DOD CIO), and other members of the Intelligence Community (IC), when appropriate, regarding intelligence-related supportability and interoperability concerns and issues.

f. J282/IRCO shall collaborate with the Battlespace Awareness Functional Capability Board (BA FCB) and its associated working group (BAWG) on program intelligence issues identified during the intelligence certification process that affect the BA FCB, and shall brief the BAWG and BA FCB as required on any intelligence issues that remain unresolved following document reviews.

g. Recommends policy and guidance to the JROC concerning the intelligence certification process and on the intelligence supportability issues, as appropriate.

2 Joint Staff, J-6

In addition to its duties set forth in the CJCS 3170.01 series (references a and b), J-6 shall provide command, control, communications, and computers (C4) expertise to the J-2 and J282/IRCO, when requested, during program or capability JCIDS and ISP review processes, and shall further provide certification of intelligence-related information system interoperability requirements.

3. Joint Staff, J-8

Shall, generally, serve as the “gatekeeper” of the JCIDS process in accordance with the CJCS 3170.01 series (enclosures A and B). Without intending to limit the duties set forth in the CJCS 3170.01 series, it is understood that J-8 shall serve as the primary contact for receiving and issuing program and capability review tasking, scheduling and coordinating JCIDS reviews, and coordinating the posting sponsor’s final FCB draft (and the associated final comment resolution matrix [CRM]) to the knowledge management/decision support tool (KM/DS) for review. After these documents have been posted to KM/DS, J-8 shall coordinate with J-2 to begin J-2’s intelligence certification letter review and approval process (as directed by the CJCS 3170.01 series and in accordance with this instruction). Note: KM/DS is a J-8 program that is resident on JSIN-S/SIPRNET.

4. Director, Defense Intelligence Agency (DIA)

a. Provides intelligence support and advises the JROC (and supporting organizations) on adversarial capabilities in support of the JCIDS process, as required by DODD 5105.21 (reference i).

b. DIA/DI/Defense Warning Office (DWO) shall review and validate JCIDS and ISP program documents to ensure relevant threat information and analysis is included in each document as a sponsor's program or capability progresses through the JCIDS and ISP review process. DWO shall also ensure that sponsors identify and analyze their programs and capabilities for projected threat information concerning future development and/or testing of their programs or capabilities, in accordance with the CJCS 3170.01 series (references a and b).

c. DIA/Directorate for Information Management and Chief Information Officer (DS) shall review programs and capabilities for information assurance and information security protocols stated in applicable Director of Central Intelligence directives, and in all other applicable security and information assurance directives related to accessing and using the JWICS system. Programs and capabilities to be funded by General Defense Intelligence Program (GDIP) IT shall submit a business case for approval in accordance with the GDIP IT Capital Planning and Investment Control Process.

d. DIA/Directorate for MASINT and Technical Collection (DT) shall review and analyze all programs and capabilities for Measurement and Signatures Intelligence (MASINT), Human Intelligence (HUMINT), counter intelligence, all-source intelligence, and technical collection and support for completeness, supportability, and impact on strategy, policy, and architecture planning. DT's reviews shall be in accordance with DODD 5102.21 and DODD 5200.37 (references i and mm). The Signatures Support Program (SSP), a resident entity within DT, shall assess and evaluate the ability or capacity of the National Signatures Community to support signature requirements of, or for, sensing programs or capabilities that are proposed in a sponsor's JCIDS document.

e. Unless otherwise requested, DIA and Joint Staff reviewers shall provide their comments and suggestions directly to J282/IRCO prior to the collaborative review suspense established by J282/IRCO and J-8. J282/IRCO shall be responsible for incorporating all intelligence-related comments into a single, consolidated DIA/Joint Staff comment matrix, and shall deliver/post the matrix to the J-8 KM/DS.

5. Director, National Geospatial-Intelligence Agency (NGA), as the DOD functional manager geospatial intelligence (GEOINT) (GEOINT – the exploitation

and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth x and y), will:

a. Designate a point of contact (POC) to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

b. Assess intelligence support requirements for completeness, supportability, and impact on GEOINT strategy, policy, and architecture planning. NGA will also evaluate open systems architectures, interoperability, and compatibility standards for GEOINT-related information systems. NGA will provide J282/IRCO with comments and recommendations for DOD-wide collaboration in accordance with enclosures B and G, with specific regard to NGA-unique contributions as identified in Enclosure C.

c. Participate in intelligence certification working groups (ICWGs), as requested, to provide advice and expertise on GEOINT support to the operational requirements in program documents.

6. Director, National Security Agency/Central Security Service (NSA/CSS), as the DOD Functional Manager for Cryptology in accordance with reference aa, will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by intelligence certification of program documents.

b. Review the intelligence support and intelligence-related operational requirements specified in or derived from program documents. Provide J282/IRCO with comments and recommendations (in accordance with enclosures B and G) with specific regard to the NSA/CSS-unique concerns as identified in Enclosure C. When applicable, provide feedback on projected impact to cryptologic (signals intelligence [SIGINT] and information assurance [IA]) strategy, policy, and architecture planning. Evaluate open systems architectures, interoperability, and compatibility standards for cryptologic and cryptologic support systems to include multi-INT cross-cueing capabilities.

c. In conjunction with similar responsibilities defined in reference d, provide expertise and assistance in assessing that there will be an adequate level of IA to meet the information threat identified.

d. Participate in ICWGs, as requested, to provide advice and expertise on cryptologic support (which includes SIGINT) to the operational requirements in program documents.

7. Director, National Reconnaissance Office

a. Designates a POC to serve as a focal point for the coordination and collaboration required by intelligence certification of program documents.

b. Reviews the intelligence support and intelligence-related operational requirements specified in or derived from program documents and provide J282/IRCO with comments and recommendations (in accordance with enclosures B, D, and G). If applicable, provides feedback on projected impact to space intelligence, space control, access, space support, space enhancement, space application, SIGINT, IMINT, MASINT, combat search and rescue (CSAR) or personnel recovery, indications, and warning and satellite communications support strategy, policy, and architecture planning.

c. Participates in ICWGs, as requested, to provide advice and expertise on operational requirements in program documents.

8. Military Services. Each Service will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

b. Review the intelligence support and intelligence-related operational requirements specified in (or derived from) program documents. Provide J282/IRCO with comments and recommendations (in accordance with enclosures B and G) related to the completeness, supportability, and impact of intelligence support requirements, with specific regard to Service-unique contributions as identified in Enclosure C.

c. Participate in ICWGs, as requested, to provide advice and expertise on the intelligence-related operational requirements of concern to the Service.

9. Combatant Commanders. The combatant commanders will review and comment on all JROC interest documents as part of the routine JCIDS staffing process (reference a). Combatant commanders also are provided the opportunity to review and comment on Joint Integration documents during the J-2 and J-6 certification processes. Combatant commanders are invited to review ISPs for acquisition programs at all ACAT levels. In conjunction with these procedures and to help facilitate the DOD-wide collaboration required by intelligence certification of JCIDS documents, combatant commanders will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

10 June 2010

b. Review the intelligence support and intelligence-related operational requirements specified in or derived from program documents. Provide J282/IRCO with comments and recommendations (in accordance with enclosures) with regard to the unique perspective of the respective command.

c. Participate in ICWGs, as requested, to provide advice and expertise on the intelligence-related operational requirements of concern to the command.

10. Defense Information Systems Agency/Joint Interoperability Test Command (DISA/JITC). JITC conducts interoperability certification testing and assessments of all information technology (IT) and National Security Systems (NSSs), including intelligence information systems (see references d and h for more information). In this capacity, JITC will:

a. Designate a POC to serve as a focal point for the coordination and collaboration required by the intelligence certification of program documents.

b. As appropriate, provide interoperability expertise to J282/IRCO during certification of intelligence-related information systems or certification of other capabilities supported by intelligence information systems.

c. Participate in ICWGs, as requested, to provide advice on interoperability considerations related to intelligence information systems or other capabilities supported by intelligence information systems.

ENCLOSURE B

INTELLIGENCE CERTIFICATION PROCEDURES

1. Purpose. This enclosure sets forth the requirements and procedures of the intelligence certification process. The underlying purpose of intelligence certification, and the mission of IRCO in leading this effort, is to: 1) prevent fielding programs and capabilities that are unsupportable by intelligence architecture (combatant command, Service, and/or national); 2) prevent technological or scientific surprise from adversarial capabilities; and 3) support intelligence architecture development through the earliest possible identification of likely or possible shortfalls in intelligence support availability, suitability, and sufficiency. The scope of review for intelligence certification (including threat validation) shall include the entire acquisition life cycle of the program or capability being reviewed (i.e., the review will include the concept, development, and fielding phases of the program or capability; and reviewers will use best efforts to estimate the intelligence support requirements and applicable threats during the entire operation and sustainment period of a program or capability).

2. General

a. JCIDS Reviews. The intelligence certification process for JCIDS documents begins when a DOD component submits a draft document to the KM/DS tool for JPD assignment (see the Glossary for a definition of JPD) through J-8's gatekeeper process, as outlined in the CJCS 3170.01 series (references a and b). Following JPD assignment, the document will enter the JCIDS staffing process as outlined in the CJCSM 3170.01 ("Operation of the Joint Capabilities Integration and Development System"). Sponsor shall seek intelligence certification for its program from IRCO for all JROC interest or Joint Integration programs or capabilities (this certification shall include DWO's threat certification), unless a waiver is requested and provided by IRCO.

b. ISP Reviews. OASD(NII)/DOD CIO will initiate the staffing of all ACAT I and Office of the Secretary of Defense (OSD)-designated special interest ISPs through the Joint C4I Program Assessment Tool-Empowered (JCPAT-E), in accordance with DODI 4630.8 (reference h). This tasking will include a requirement for J-2 and DIA review.

c. The J282/IRCO is tasked with providing intelligence certification for all DOD acquisitions with a JPD of JROC Interest or Joint Integration. The IRCO office will use the Intelligence Certification Tool located in the J28 Integrated Database to accomplish this task. IRCO and collaborators will post comments to the Intelligence Certification Tool prior to J282 rolling the comments up and

10 June 2010

submitting to KM/DS during the review stages of the certification process. The certification tool will generate certification letters and comment resolution matrices (CRMs) for posting to KM/DS during the certification letter portion of the certification process. The link to the J28 Integrated Database is: <http://164.185.180.14:8001/IntelCertification/j2sid.html> on JWICS and <http://j2sid.js.smil.mil/IntelCertification/j2sid.html> (<http://j2sid.js.smil.mil/IntelCertification/logout.jsp>) on JSIN-S/SIPRNET. To obtain a password, go to the Contact Us link at the above URLs and contact a J282/IRCO representative.

3. Certification Process

a. General Staffing and Coordination. Intelligence certification is a process consisting of a concept stage (a concept is introduced to the defense community that states an overarching area of interest that will serve as a starting point for future development), followed by three stages of program development and document production that range from initial, development, and production stages of a given program (the three stages are termed milestones A, B, and C of the review process). For a detailed discussion of the JCIDS process, along with a discussion of the associated tasks associated with each stage of the JCIDS process, refer to reference b, CJCSM 3170.01 series, enclosures A, B, and C. For a detailed discussion of the JCIDS document staffing process, refer to the CJCSM 3170.01 series, Enclosure D. For the purposes of this instruction, each stage of the intelligence certification begins with the submission of a JCIDS document to J-8. J-8 will act as the gatekeeper and will task J-2 to complete reviews and to perform intelligence certifications.

(1) The first document in the JCIDS process is the ICD. The ICD may generate or influence the development of one or more CDDs and CPDs. The milestones consist of Milestone A, where an ICD is submitted and reviewed; Milestone B, in which a CDD is submitted and reviewed; and Milestone C, where a CPD is submitted and reviewed. As programs proceed through milestones, program documents will be expected to increase in refinement and specificity (corresponding with the stage and document type). Each milestone culminates with a final intelligence certification that includes a threat validation.

(2) Each review stage may include up to two phases of review. In each phase, a program document is distributed for review and comment (see paragraph b, below, for an explanation of when two phases of review are necessary). Sponsors are responsible for adjudicating each comment and indicating whether the comment is accepted, partially accepted, or rejected in their final CRM. When a sponsor partially accepts or rejects comments, a brief explanation should be included within the CRM. Sponsors must adjudicate all comments prior to submitting their final CRM and FCB draft to J-8 to begin

intelligence certification for a particular milestone. After the final CRM and sponsor's final FCB draft (as further explained below) have been submitted to J-8 and posted on KM/DS, sponsors shall seek intelligence certification in accordance with this instruction.

(3) As documents proceed through the staffing and intelligence certification process, IRCO will lead and conduct a coordinated, collaborative review of the sponsor's document for completeness, intelligence supportability, and impact on strategy, policy, and architecture planning, as defined by this instruction. DIA will provide threat validation at each phase of review and must be accomplished at each milestone decision point for intelligence certification. At each milestone decision, IRCO will perform an intelligence certification review after being tasked by J-8, and shall provide an intelligence certification letter for a program or capability only if the sponsor has satisfactorily adjudicated each critical intelligence-related comment. IRCO's intelligence certification letter shall be associated with the specific document and shall be effective only as to its associated acquisition document milestone (e.g., an intelligence certification letter issued for a CDD will be effective only for Milestone B). ISPs shall follow the same general procedure of review as JCIDS documents (i.e., two phases of review for each document milestone, if necessary), and shall be subject to the review standards and criteria set forth in Enclosure E (however, ISP reviews are governed by DODI 4630.8 as opposed to the CJCS 3170.01 series). See the overview below for a general roadmap of the intelligence certification process and its association with the overall JCIDS and ISP processes.

Overview of the JCIDS Staffing Process with ISP Staffing Process Overlay

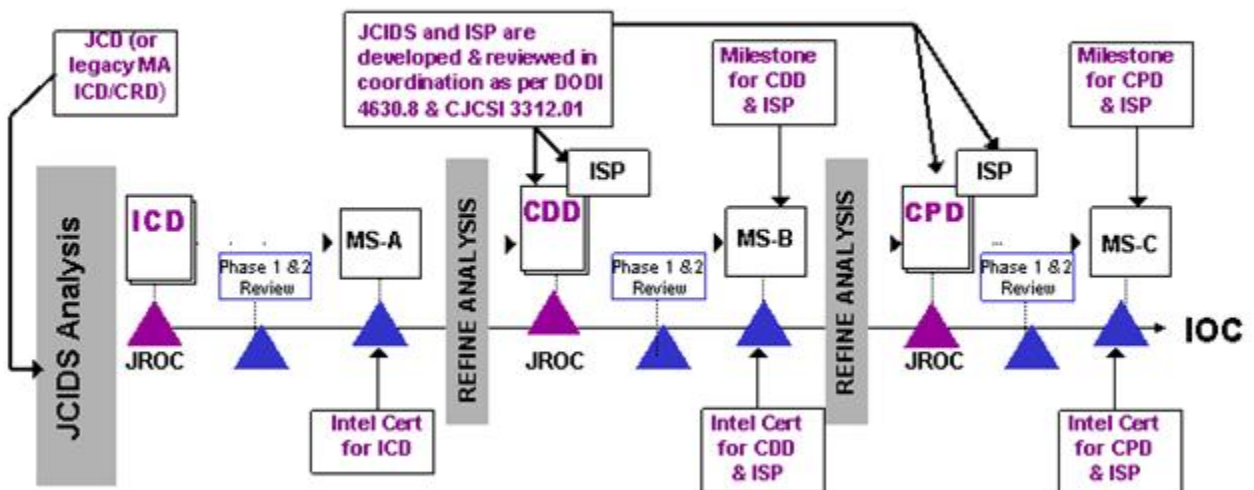


Figure B-1. Association Between JCIDS and ISP Processes

10 June 2010

(4) Concerning the connection between ISPs and JCIDS reviews: In accordance with DODI 4630.8, Enclosure 4, and the OASD(NII)/DOD CIO memorandum for the Secretaries of the Military Departments (setting forth interim changes to DODI 4630.8), sponsors are required to prepare and update ISPs in conjunction and/or concurrent with the JCIDS documents and within the JCIDS milestone decision framework. The above instruction and memorandum also state ISP development must permit sufficient time for DOD-level ISP reviews prior to each milestone or decision review and are to be used in the production of CDDs and CPDs. Therefore, to ensure that DOD-level reviews can be accomplished prior to document phase or milestone decision reviews, sponsors must coordinate ISP production with CDD and CPD document production. A failure to complete the ISP document and review process in a timely manner may, moreover, result in a nonconcur to proceed from the OOASD(NII)/DOD CIO at milestone B, C, or any future incremental decision. Therefore, it is recommended that ISPs and CDDs/CPDs be developed and submitted simultaneously to allow coordinated review and commenting.

b. Intelligence Certification Phases and Intelligence Certification. Following the development and certification of a JCD -- an overarching concept document stating a general area of military interest -- sponsors will develop documents related to specific gaps within that area of interest expressed in the JCD. The intelligence certification process for these capabilities-based documents (ICDs, CDDs, and CPDs) includes the three stages, or "milestones," of review (milestones A, B, and C). Each milestone is separated into two possible phases of review. (All JCIDS documents are subject to a Phase 1 review within each milestone; Phase 2 reviews are completed when sponsors receive critical comments at Phase 1 and do not satisfactorily adjudicate such comments before the final CRM and Phase 1 comments are finalized -- satisfaction being at the discretion of the entity submitting the comment.) After one or both phases of review are completed for a given milestone, sponsors must receive an intelligence certification letter before their programs or capabilities may progress to the next milestone or, if at Milestone C, exit the JCIDS process. This process is more specifically explained below. (As a reminder, this instruction applies only to documents with a Joint Potential Designation of "JROC interest" and "Joint Integration," and to ISPs through DODI 4630.8. Documents designated "Joint Information" are not reviewed according to this instruction.)

(1) Phase 1 Reviews. The first iteration of inputs to the intelligence certification process corresponds with the O-6/planner-level review. Intelligence certification will be informal at this stage, as no certification letter will be issued. Sponsor shall be responsible for adjudicating each comment submitted by each reviewer prior to progressing to certification of its program or capability. If any critical intelligence-related comments remain after Phase 1

review and comment resolution, sponsor's program or capability will proceed to Phase 2 review.

(2) Phase 2 Reviews. The second iteration of inputs to the intelligence certification process, if required, corresponds with general/flag officer-level review. Again, intelligence certification will be informal at this stage, as no certification letter will be issued. Sponsors are nevertheless responsible for adjudicating each comment submitted by reviewers prior to progressing to finalizing its CRM.

(3) Final Intelligence Certification. Final comment resolution and FCB draft. Upon completion of the necessary phases of review for a given JCD or milestone, sponsor shall provide J-8 with a final CRM (i.e., all comments have been adjudicated) and a final FCB document to post on KM/DS (JCIDS documents) or JCPAT-E (ISPs). The final CRM will contain all comments to date and indicate the status of adjudication (sponsors will note that a comment is "accepted," "partially accepted," or "rejected" and provide rationales for comments it partially accepts and rejects). J-8 shall notify J-2 that the final CRM and FCB draft have been posted and are ready for review. IRCO shall thereafter complete an intelligence certification review of the final CRM and FCB draft. IRCO shall review and analyze all intelligence-related comments; regardless of the source of the comment (i.e., IRCO will review comments from entities outside of DIA and the Joint Staff). IRCO will identify critical intelligence-related comments during its final CRM review and coordinate with the applicable reviewer and sponsor to determine the status of the comment (i.e., either the comment remains a critical comment or the comment has been adjudicated to the reviewer's satisfaction and is no longer critical). Note: Sponsors are required to adjudicate all comments with the DIA and Joint Staff reviewers, regardless of the comment type (administrative, substantive, or critical). IRCO will also ensure all comments have been appropriately incorporated in the FCB draft. Intelligence certification is explained in detail in paragraph 4, "Intelligence Certification," below. Intelligence certification failure is addressed in paragraph 5 below.

c. Collaborative Inputs. IRCO shall receive inputs from subject matter experts within DIA and J-2, which shall include DWO, DS, DT, J25, J26, and all other applicable DOD and Joint Staff entities, when appropriate. As noted earlier, IRCO may consider all intelligence-related comments and collaborate with other reviewers throughout the Intelligence Community (IC) regarding the program's intelligence support requirements and supportability.

d. Criteria. Intelligence reviewers will assess both requirements for intelligence (such as requirements for intelligence information or services) and compliance with standards required by intelligence (such as interoperability and security), in accordance with the main text of the instruction and, more specifically, in accordance with enclosures C and E. Enclosure C provides

10 June 2010

general descriptions of the intelligence support categories, to include general qualitative and quantitative attributes that are expected. Enclosure E provides reviewers with additional guidance for ICDs, CDDs, CPDs, ORD updates/annexes, and ISPs to ensure completeness and standardization. DIA and Joint Staff reviewers will forward comments directly to IRCO in the format prescribed by the KM/DS staffing tool (JCIDS documents) or JCPAT-E (ISPs), as described in detail in the CJCS 3170.01 series and DODI 4630.8 (references a, b, and h).

e. Resolving Intelligence-Related Issues

(1) Sponsors shall coordinate with IRCO and with reviewers concerning any intelligence-related comments. Sponsors shall attempt to resolve issues at the lowest level possible (e.g., discuss incomplete declaration of intelligence support requirements with the commenter) before the program's CRM is submitted to J-8 for posting on KM/DS following a given phase or at a milestone decision. Informal resolution efforts should be used when appropriate and will be considered by IRCO when possible; note, however, that these informal efforts will not preclude submission of a nonconcur or preclude the need for formal comment resolution by sponsors. Critical comments that cannot be resolved as mentioned above will be documented and brought to the attention of the appropriate FCB(s).

(2) IRCO will coordinate intelligence certification issues continuously with respective FCBs. Intelligence support issues, especially those related to potential shortcomings in intelligence support, provide a critical input into the development of joint intelligence architecture planning and policy, and support FCB's responsibility to identify, analyze, prioritize, and validate capability needs in the area of intelligence. IRCO will coordinate with the assigned FCB when intelligence-related comments arise during the review and adjudication process, or when a program or capability is facing a recommendation of non-certification, to ensure the FCB is made aware of potential intelligence-related issues that must be addressed and resolved prior to approval of an intelligence certification letter.

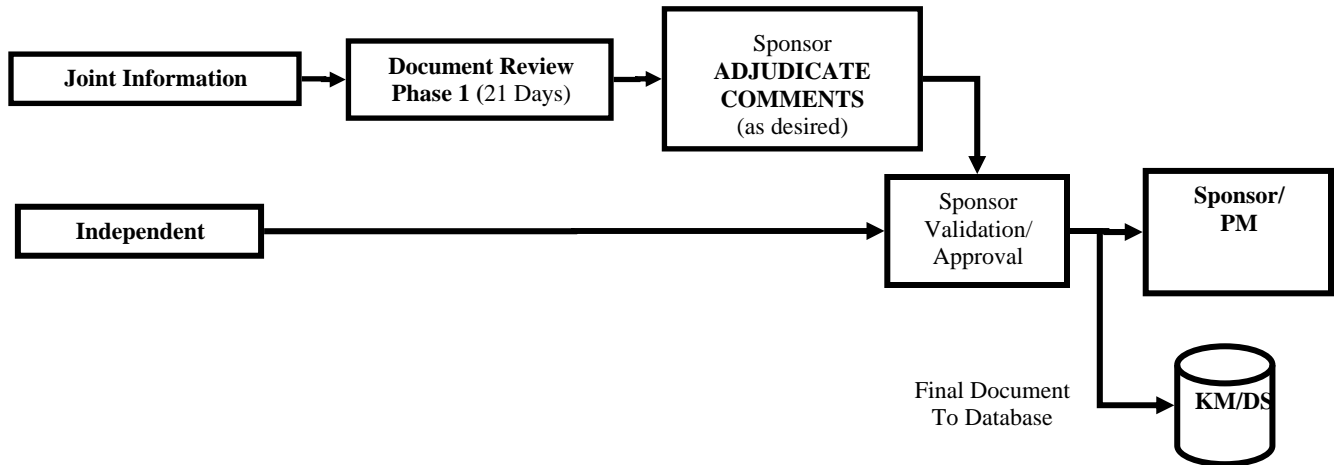


Figure B-3. Joint Information and Independent Staffing Processes

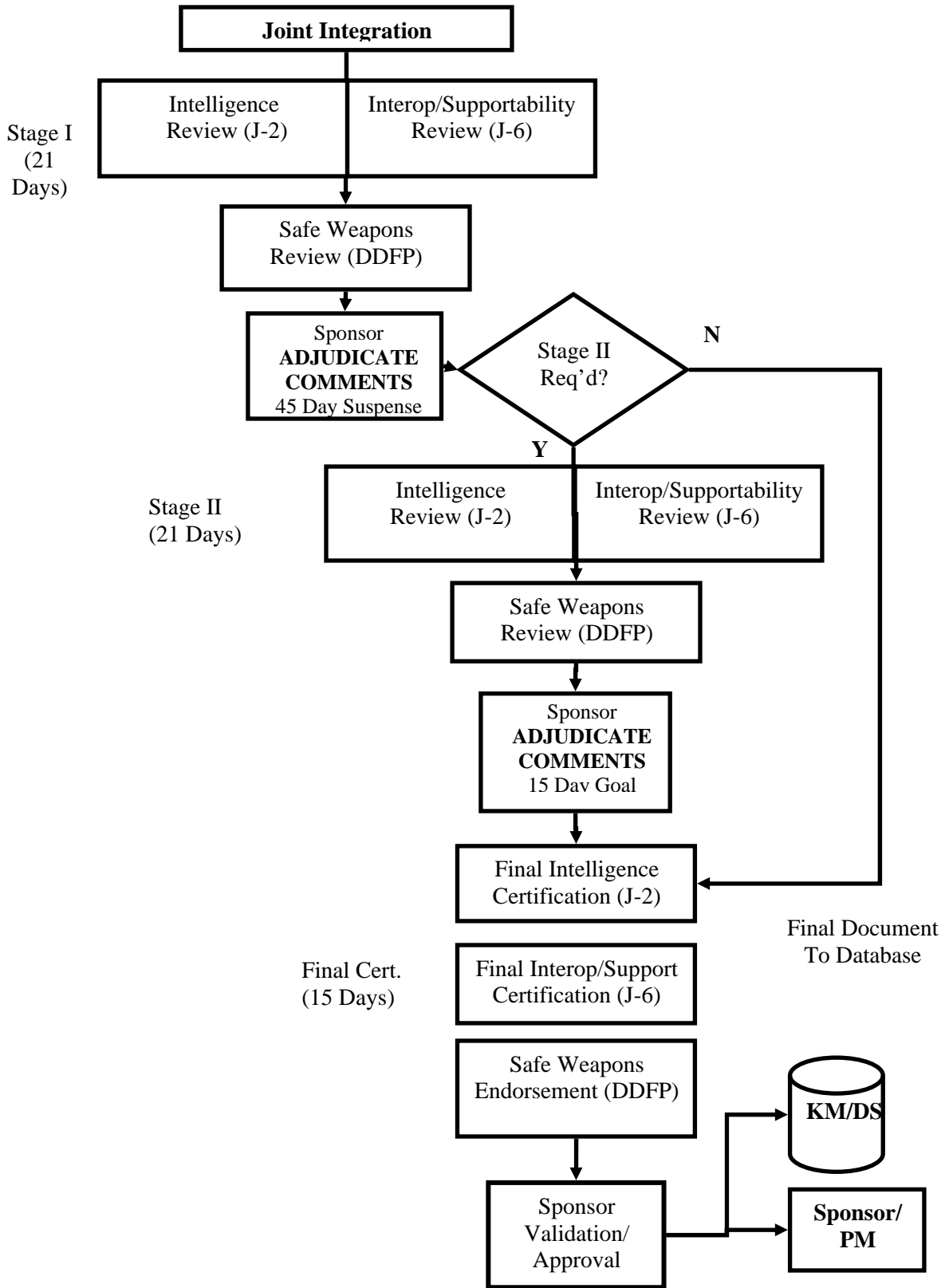


Figure B-4. Joint Integration Staffing Process

4. Intelligence Certification

a. Intelligence certification shall be completed at each phase of document review. A final intelligence review (leading to an intelligence certification letter, if appropriate) will be completed at the final JCD review stage and at each milestone (milestones A-C) decision point. At the final JCD review and at the milestone decision reviews, sponsor shall post its final CRM and FCB draft to KM/DS. If sponsor's program has no critical intelligence-related comments, or if the critical intelligence-related comments have been adjudicated (i.e., all critical comments are addressed by sponsor to the satisfaction of the commenter), and the appropriate edits have been satisfactorily incorporated in the FCB draft, IRCO will recommend that the program or capability receive intelligence certification. The above certification will be effective for only that specific document and its associated acquisition milestone. IRCO will post intelligence certification letters (as illustrated in Enclosure D) to KM/DS. Authority to approve or deny intelligence certification shall rest with the J-2 (or his/her designated representative) for JROC interest programs; the J28 (or his/her designated representative) shall have authority to grant intelligence certifications for Joint Integration programs. When appropriate according to this instruction, the J28 (for JROC interest and Joint Integration programs) shall publish an intelligence certification letter, and IRCO shall post the letter to KM/DS. (Programs designated Joint Information shall not be reviewed or certified.) The following table summarizes approval authorities by review disposition and document type.

Joint Point Designator	Phase 1	Phase 2	Intelligence Certification or Reviews
JROC Interest	J282 ¹	J28	J28
Joint Integration	J282 ¹	J28	J28
JCB Interest	J282	J282	J28
Joint Information ²	N/A	N/A	N/A
ISPs	IRCO Chief	IRCO Chief	IRCO Chief

¹ J282 is the O-6/planner-level approval authority for JROC Interest and Joint Integration programs.

² Joint Information programs are not reviewed by IRCO.

Figure B-5. Intelligence Review and Certification Approval Authorities

b. Intelligence certification shall affirm that:

(1) The program or capability meets minimal requirements for intelligence support needs related to completeness and supportability, and that an assessment concerning the program's impact on intelligence strategy, policy, and architecture has identified no significant shortfalls in current or planned intelligence support.

(2) Any critical intelligence-related comments or critical threat-related comments relating to the program or capability have been appropriately adjudicated to the satisfaction of the entity submitting the comment, or otherwise resolved by the appropriate FCB WG, FCB, or the JROC.

(3) DIA/DI/DWO (DWO) has reviewed this document and concurs with the threat section pursuant to DIAI 5000.002 and DIAD 5000.200, "Intelligence Threat Support for MDA Programs" (references j and k). (Note: As with intelligence certifications, DWO's threat validations are associated with the

10 June 2010

specific document phase or milestone reviewed.) Note: Program sponsors are required to ensure that the most current and relevant threat information is considered and included prior to, and during, all phases and milestones of JCIDS and ISP review and document drafting process.

(4) Any projected shortcomings in joint intelligence support will be included in the annual BAWG analysis to identify and prioritize capability gaps within the battlespace awareness functional area in accordance with the CJCS 3170.01 series and 3137.01C (references a, b, and gg).

c. General Interpretation of Intelligence Certification. As stated earlier, the intent of the intelligence certification process is to avoid intelligence shortfalls by:

(1) Avoiding fielding programs and capabilities that are not supportable by the Intelligence Community.

(2) Preventing scientific and technological surprise.

(3) Ensuring that the Intelligence Community is able to support warfighters (now and in the future).

Each program represents a possibility -- or likelihood -- that the Intelligence Community cannot support that program's intelligence support requirements (i.e., a shortfall may result from developing a program). The likelihood that a program may create an intelligence shortfall equates to a risk; it is this risk of an intelligence shortfall that is of central concern in the intelligence certification process. It is acknowledged that each program or capability has unique attributes that require differing levels and forms of intelligence support. Assessing a program or capability's risk of creating an intelligence shortfall is, therefore, many times imprecise due to the wide range of variables that affect a program's intelligence support determination (e.g., types of collection assets required, allocation and prioritization of funds or collection time to fulfill intelligence support requirements, complexity of the support necessary, quantity of support necessary, expectation of support, level of intelligence dependence, etc.). Variables involved with assessing shortfall risks are often difficult to define and measure, and therefore cannot be easily classified to permit a definite forecast of support requirements. As a result, a program or capability's likely effect on the Intelligence Community and its risk (or likelihood) of creating an intelligence shortfall will need to be determined on a case-by-case basis using available information related to intelligence support. Sponsors are required to provide sufficient information, and to perform adequate analysis, to enable reviewers to assess and identify intelligence support requirements and shortfalls, if any.

5. Certification Failure. If IRCO determines that there are critical intelligence-related comments (or other comments that are otherwise subject to this instruction) that remain unsatisfactorily adjudicated upon its review of the final CRM and FCB draft, then it shall use best efforts within J-8's stated review certification review period to contact the commenter and sponsor to determine if the critical comments have been resolved. If a critical comment has not been resolved, or has not been appropriately incorporated into the FCB draft, then IRCO will recommend withholding intelligence certification for the sponsor's program. (See subparagraph 4(a), above, for a table summarizing certification approval authorities.) If there is concurrence in IRCO's assessment by the certifying authority, then an intelligence certification failure will result and sponsor's intelligence certification letter shall be withheld. Intelligence certification shall be withheld until all critical intelligence-related comments have been satisfactorily adjudicated (satisfaction being at the discretion of the commenter). (Note: As discussed in paragraph 3e, comment resolution should be handled progressively, beginning with direct sponsor/commenter discussion and followed by referring the matter to the appropriate FCB, if necessary. Should issues remain unresolved by the FCB, the program will proceed through the JCIDS process in accordance with the CJCSI 3137.01 series.

(INTENTIONALLY BLANK)

ENCLOSURE C

INTELLIGENCE SUPPORT REQUIREMENT CATEGORY DESCRIPTIONS

This enclosure provides document drafters with general descriptions of intelligence support requirement categories. The intent of this enclosure is to assist sponsors and assessors/commenters with the identification of intelligence support requirements. The following descriptions are not all-inclusive; rather, the descriptions serve as a reference tool and should be tailored to satisfy each program or capability's unique intelligence support requirements. In addition, generic operational capabilities that these support requirements are usually associated with, along with general quantitative and qualitative attributes, are discussed. With regard to quantitative attributes, not all types of intelligence support can be easily measured. The purpose of requiring sponsors to measure and articulate intelligence support requirements is simply to provide a means to identify and evaluate each program or capability's specific intelligence support requirements and likely shortfalls (or risk of shortfalls).

1. Intelligence Manpower. This category should be addressed if the operational or support aspects of a program will require intelligence personnel for any and all phases (to include development, testing, training, and operation) of the program's acquisition life cycle. Depending on the maturity of the program, a Manpower Estimation Report (MER) may have been completed and included in the applicable CDD or CPD; if an MER has not yet been completed, intelligence implications from that report should be included in the applicable CDD or CPD.

Associated Generic Capabilities: Potentially all.

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

Quantitative Attributes: Address how existing intelligence (or other support) manpower resources will meet the program or capability's intelligence support requirements (i.e., existing organizations and billets will provide sufficient support) or whether the program will require additional, dedicated intelligence personnel (i.e., 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).

2. Intelligence Resource Support. This requirement category should be addressed if either the operational capabilities of the program or support capabilities will require, or depend upon, intelligence funding. In particular, if the program or capability will rely upon intelligence capabilities or systems that have not yet been provided dedicated funding, have not received necessary approvals to begin operations, or have not received approvals to remain operational, then these dependencies should be identified.

Associated Generic Capabilities: Potentially all.

Qualitative Attributes: Not applicable.

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

3. Collection Management Support. The requirement for collection management support refers to both management of collection assets and identification and management of intelligence information requirements. Generally speaking, 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 validated information requirements. At the strategic and operational level, collection management support refers to the personnel, expertise, training, and systems required to ensure intelligence collection assets (e.g., national, joint, Coalition, 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 the information, once collected, is disseminated to the entity that made the original request and to all other end users requiring such information.

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).

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(s) or collection asset capabilities that will be needed to collect the requested information.

Quantitative Attributes: Address what intelligence information needs the program or capability will require during its entire acquisition life cycle (from development to program/system retirement). Identify, if possible, what entity(ies) will provide the required collection management support and whether the entity(ies) will have the capacity to provide such support (i.e., will the entity be available to support the sponsor's program or capability).

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

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

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

Quantitative Attributes: Volume of data required.

5. Geospatial Intelligence Support (GEOINT). GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. The DOD functional manager for GEOINT is the National Geospatial-Intelligence Agency (NGA).

a. GEOINT provides two irreplaceable components that contribute to the effectiveness of weapons and weapon systems: a framework that renders other intelligence actionable by virtue of referencing it to a four-dimensional space-time context; and, critical qualitative and quantitative information to describe the physical and functional characteristics of the political, economic, military, social, informational, and infrastructure components of an enemy's capabilities. The fusion of imagery-based intelligence (to include imagery-based MASINT) with geospatial information to create GEOINT conveys understandings of enemy assets and actions that play a dominant role in

determining weapon and weapon system effectiveness. The critical contribution of GEOINT to force effectiveness spans all categories of capabilities, kinetic/non-kinetic and lethal/non-lethal. Furthermore, the critical contributions of GEOINT to effectiveness span 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. 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 NGA must justify requirements for resources and apportionment of those resources within the agency. An example of such GEOINT shortfalls would be the identification of routine data exploitation and production requirements for specific construction details of buildings that affect the performance of a miniaturized munition. Another example would be concise description of man-made features and demographic distributions in urban areas where planned operations must consider high-fidelity estimation of collateral damage risks.”

b. With respect to the geospatial component of GEOINT, this category refers to a program or capability’s requirement for geospatial information, services, or products traditionally associated with the mapping, charting, and geodesy disciplines. To fulfill geospatial requirements for their programs or capabilities, sponsors must factor in significant lead times needed to accommodate the planning, allocation, and deconfliction of geospatial information and services (GI&S)-related collection, analytic, and dissemination resources that are consistently in high demand.

c. Different missions require different types of GEOINT support and create different effects upon NGA and the other Intelligence Community members providing geospatial intelligence (these effects impact collection assets, intelligence systems, and manpower [e.g., collection managers, analysts, etc.]). For example, GEOINT support during system development may include prototyping products and services unique to the system, possibly impacting NGA capabilities by virtue of the time and resources required to develop new methods, technologies, architectures, and/or tradecraft. On the other hand, GEOINT support to operations and sustainment is based on deployment footprints and primarily affects the capacity of NGA and its mission partners to collect, analyze, and disseminate such intelligence. Because of the potential resource demands of these support requirements and the resulting effect on the GEOINT community; they must be qualitatively and quantitatively identified at the earliest possible point in the JCIDS review process.

Associated Generic Capabilities: Potentially all.

Qualitative Attributes: Required data, coverage, scale, timeliness, formats, accuracy, resolution level (e.g., imagery and/or Digital Terrain Elevation Data

[DTED] levels). Sponsors should consider and ensure that the necessary or desired product format (electronic versus paper) and necessary update requirements (periodic versus. as-needed) will be available and have been requested to support their programs and capabilities. Note: Compliance with NGA standards and dissemination policies is a mandatory requirement.

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

6. Targeting Support. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (See Joint Publication 2-01.1, “Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting.”) With regard to this instruction, 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. Note: Sponsors must consider intelligence support to targeting if their program or capability will employ, or will rely upon the employment of, munitions (both kinetic and non-kinetic) because intelligence targeting support shortfalls may detrimentally affect the program or capability’s successful development, on-time delivery schedule, and ultimately its operational status (i.e., intelligence support to targeting is a broad category that encompasses munitions and all associated programs or capabilities relying upon the munition).

a. 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 gaps in force application capabilities.) Sponsors with programs and capabilities 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 program but the munitions it will employ or rely upon.

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

(1) To support commanders’ 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 Geospatial Information and Services Support category because many targeting services rely upon and/or incorporate geospatial products or information.

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

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.

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.

7. Combat Search and Rescue Intelligence Support. CSAR is the specific task performed by rescue forces to recover distressed personnel during war or military operations other than war (see Joint Publication (JP) 3-50.2, "Doctrine for Joint Combat Search and Rescue"). 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, there are usually unique CSAR intelligence support requirements, which 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.

Associated Generic Capabilities: Platforms or capabilities with a CSAR mission.

Qualitative Attributes: Information accuracy and timeliness, training levels, the capability to reach back and timeliness of reachback, and the capability to integrate information and operations with national and/or joint intelligence assets and capabilities.

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

8. Intelligence Preparation of the Operational Environment (IPOE)/Joint Intelligence Preparation of the Operational Environment (JIPOE). In the most basic and general sense, IPOE refers to intelligence analysis that compiles orders of battle information, converts this information into a visual depiction of the battlespace, and enables the depiction of possible enemy courses of action. Naturally, the complexity associated with this type of support varies substantially based upon the scope of the battlespace involved. JP 2-01.3, "Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Operational Environment," 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.

As with all intelligence support categories, IPOE support can apply throughout all phases of the acquisition life cycle. (An example is the requirement that sponsors ensure their programs and capabilities 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.) Likewise, IPOE ensures 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.

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.

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

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

9. Warning Support. 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.

For the purposes of this instruction, warning support must be thought of as being necessary throughout all phases of acquisition life cycle -- from development to employment and sustainment

b. Warning support prior to a program's operational phase of acquisition may be thought of as information that enables that program or capability to remain scientifically and technologically superior relative to developing or

projected adversary capabilities. The capability to provide this support; however, 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 program or capability's acquisition life cycle.)

c. 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 current DOD Indications and Warning System Operations Manual, which may be found on the DIA JSIN-S/SIPRNET Web site at http://www.dia.smil.mil/intel/j2/j2m/pubs/j2m-0177-01-96/j2m-0177-01_cov.html or on the Joint Worldwide Intelligence Communications System (JWICS) at http://www.dia.ic.gov/intel/j2/j2m/pubs/J2M-0177-01-96/J2M-0177-01_cov.html.

Associated Generic Capabilities: Potentially all.

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.

Quantitative Attributes: This type of support is impossible to accurately quantify, but may be addressed in terms of high, medium, or low demand levels. Depending on the technological complexity of the program or capability, the level of warning support that may be required could vary (although the numbers of CICs developed may be a good indicator of the quantitative levels of support required). For operational warning support, warning support demand levels will vary by the primary mission of the program.

10. Space Intelligence Support. Space intelligence support refers to intelligence information, infrastructure, or resources that provide space-specific intelligence analysis on foreign space capabilities. (See JP 3-14, "Joint Doctrine for Space Operations.")

Associated Generic Capabilities: Space-based programs; programs relying upon space-derived capabilities, platforms that require visibility into the foreign space picture; and platforms that perform space control or space support, space support, space enhancement, and space application.

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

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

11. Counter Intelligence Support. Counter intelligence 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 (see JP 2-01.2, "Joint Tactics, Techniques, and Procedures for CI Support to Joint Operations"). In the context of this instruction, counter intelligence support (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 DODD 5200.39, "Security, Intelligence, and Counter Intelligence Support to Acquisition Program Protection" (reference ii).

As with other requirements, counter intelligence support can and should be applied throughout a program's entire acquisition 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.

Associated Generic Capabilities: Potentially all.

Qualitative Attributes: May include format of information, training level of CI personnel involved, timeliness requirements, and compliance with reference ii.

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.).

12. Intelligence Training Requirements. Some programs may require intelligence personnel supporting a program or capability to receive specialized training to support part or all phases of a given program or capability's acquisition 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 program or capability. In either case, the requirement for specific training to support any phase of a program or capability's acquisition life cycle must be identified, analyzed, and declared as soon as possible in the JCIDS process to permit

sufficient lead time to develop personnel with the skills required to support sponsor's program or capability.

Associated Generic Capabilities: Potentially all.

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) for sponsor's program or capability.

Quantitative Attributes: Intelligence training requirements will be dependant upon the amount of manpower required to support the program or capability (and subsequent training requirements) and whether the program or capability will require a new or unique training program to support it.

13. Dissemination Support. Although the movement toward a net-centric environment has, to some extent, reduced the technical challenges related to information dissemination, intelligence infrastructure (such as intelligence networks, systems, and software) and intelligence resources (such as funded programs or manpower) nevertheless remain a critical (and necessary) means of information delivery. One way to determine a program or capability'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.

Associated Generic Capabilities: Systems/capabilities that provide intelligence information, manpower, and resources to compile and deliver information, manpower, and resources to operate and maintain delivery systems and capabilities.

Qualitative Attributes: Dependant upon the specific requirements of sponsor's program or capability being supported, which may include: timeliness of delivery, means of delivery, interoperability of delivery/communications systems, format of information delivered, and information updates.

Quantitative Attributes: Dependant upon the specific requirements of sponsor's program or capability being supported, which may include types of delivery/communications systems required, personnel needed to support a given program or capability, volume of information that will be delivered.

Note: Sponsors must consider and address their program or capability's effects on the capacity and ability of the system/capability delivering the information to continue operations and support other, non-program related requirements (e.g., impact on bandwidth) and security considerations related to the information and source of information (e.g., HUMINT controls), etc.

(INTENTIONALLY BLANK)

ENCLOSURE D

INTELLIGENCE CERTIFICATION SUMMARY AND LETTER

After a sponsor has posted the final CRM and FCB Draft to KM/DS, J-8 will notify J-2 (via e-mail) and J-8 will post the FCB Draft and final CRM to the J-8 KM/DS and provide notice to all IRCO AOs via their KM/DS inbox. This will initiate final intelligence certification of the program or capability. IRCO (acting on behalf of the J-2 and J28), shall perform a review of the final CRM and FCB draft to determine whether the program or capability should receive certification. If the FCB draft and final CRM satisfies all requirements set forth in this instruction, IRCO shall recommend to the J28 (for JROC Interest programs and Joint Integration programs), or the IRCO Chief (for ISPs) that intelligence certification or review be granted. Authority to approve or deny intelligence certification is summarized in the table below:

Joint Point Designator	Phase 1	Phase 2	Intelligence Certification or Reviews
JROC Interest	J282 ¹	J28	J28
Joint Integration	J282 ¹	J28	J28
Joint Information	N/A	N/A	N/A
ISPs	IRCO Chief	IRCO Chief	IRCO Chief

¹ J282 is the O-6/planner-level approval authority for JROC Interest and Joint Integration programs.

² Joint information programs are not reviewed by IRCO.

(Note: Programs designated joint information are not reviewed under this instruction.)

Table D-1. Intelligence Review and Certification Approval Authorities

THE JOINTSTAFF
WASHINGTON,DC



Reply ZIP Code:
20318-2000

U-12345/J2S
(DATE)

MEMORANDUM FOR J28, BATTLESPACE AWARENESS FCB, AND U.S. ARMY

Subject: Intelligence Certification of the [Name of program and type of document]
(KM/DS Control Number: XX-XXXXXXXX-XX)

1. Intelligence certification is granted for [Name of program and type of document with acronym] and is written in preparation for a Milestone [] decision, as required by CJCSI 3170.01E, *Joint Capabilities Integration and Development System*, and by CJCSI 3312.01, *Joint Military Intelligence Requirements Certification*. Any shortfalls captured from this capability assessment will be included in the annual Functional Capabilities Board (FCB) analysis of capabilities and gaps in accordance with CJCSI3170.01E.
2. This certification states that as of the date of this letter: [program acronym] meets minimal requirements for intelligence completeness and supportability according to CJCSI 3312.01, and that an assessment concerning [program acronym]'s impact on intelligence strategy, policy, and architecture has identified no significant shortfalls in current or planned intelligence support. It is affirmed that all critical intelligence-related comments submitted during the intelligence certification process have been satisfactorily adjudicated.
3. DIA/DI (DWO) has reviewed this document and concurs with the threat section for [program acronym] pursuant to DIAI 5000.002 and DIAD 5000.200, *Intelligence Threat Support for MDA Programs*. Programs should refer to the latest applicable DIA validated threat documentation or System Threat Assessment Report (STAR), if available, for threat information specific to [program acronym]. Programs should endeavor to ensure the most current and relevant threat information is considered prior to and during production.
4. The Joint Staff/J-2 point of contact is [IRCO POC Info].

R. E. L. ALLEN
Deputy Director for Battlespace
Awareness(J28)

Example JCIDS Intelligence Certification Letter

ENCLOSURE E

PROGRAM DOCUMENT GUIDANCE

1. Purpose. This enclosure provides guidance on drafting intelligence supportability sections, and expands upon the guidance set forth earlier in this instruction and in the CJCS 3170.01 series (for JCIDS documents). This enclosure is meant to be read and used in conjunction with the main section of this instruction and the other enclosures -- particularly Enclosure C. This enclosure provides paragraph-by-paragraph guidance concerning basic information and analysis that sponsors must consider and address and, secondarily, is meant to serve as a guide to assessors/commenters to assess programs during the intelligence supportability review process.

2. General. The guidance that follows is general in nature and must be adapted to fit program requirements. Each program or capability will have unique intelligence support requirements; thus, the support information section (in ICDs) or intelligence supportability paragraph (in CDDs or CPDs) should reflect and address such unique requirements. In addition, understanding and specifying intelligence support requirements or shortfalls will become more refined -- or change -- as the program progresses through the JCIDS process (i.e., a program matures). The level of refinement and analysis concerning intelligence supportability will generally increase over time, from ICDs (in which capability gaps are identified within a concept) to CDDs and CPDs (where specific programs and capabilities are developed and produced, respectively, to meet identified gaps).

3. The Information Support Plan (ISP) Development Process and its Connection to the JCIDS Process

a. In accordance with DODI 4630.8, Enclosure 4, and the OASD(NII)/DOD CIO memorandum for Secretaries of the Military Departments (setting forth interim changes to DODI 4630.8), sponsors are required to prepare and update ISPs in conjunction with the JCIDS documents and within the JCIDS milestone decision framework. The above instruction and memorandum also state ISP development must permit sufficient time for DOD-level ISP reviews prior to each milestone or decision review and that ISPs are to be used in the production of CDDs and CPDs. Therefore, to ensure that DOD-level reviews can be accomplished prior to the milestone or decision reviews, sponsors must coordinate ISP production with CDD and CPD document production. A failure to complete the ISP process in a timely manner may result in issuance of a

10 June 2010

nonconcur to proceed by the OASD(NII)/DOD CIO at milestone B or C. Likewise, failing to coordinate ISP production with the CDD/CPD document production process may result in intelligence certification delays or possibly intelligence certification failure -- this is of particular concern when the sponsor's program relies upon certain technological or interoperability capabilities and the sponsor has not conveyed such data/information in its JCIDS documents, which may result in the inability of an assessor/commenter to determine whether the program is technologically supportable or interoperable with existing or planned intelligence systems, and a determination that the program is not supportable. It is, therefore, recommended that ISPs and CDDs/CPDs be developed and submitted simultaneously to allow simultaneous review and commenting.

b Although ISPs are not considered a JCIDS document (it is required by OOASD(NII)/DOD CIO, not the JROC), the outputs from the Information Needs Discovery and Analysis Process detailed in DODI 4630.8 (reference h, Enclosure 4) may assist sponsors in addressing intelligence support requirements in CDDs and CPDs. In accordance with the CJCS 3170.01 series and DODI 4630.8 (references a, b, and h), intelligence information needs (and the associated architecture and exchange requirements) must be clearly illustrated in architecture graphics within JCIDS documents and more specifically identified and analyzed in ISPs. (Note: JCIDS documents do not require the level of technical detail ISPs will contain.) This shared interest in certain aspects of technical intelligence-related supportability provides sponsors drafting CDDs/CPDs and ISPs the opportunity to leverage the analysis performed in each process, which will assist sponsors in meeting the requirements of this instruction and DODI 4630.8 concerning the identification and assessment of a program's technical intelligence support requirements (IT architecture, interoperability, etc.). Please note, however, that this leveraging process does not negate the requirement to address intelligence support requirements as completely as possible in the JCIDS process -- the sponsor may not defer intelligence requirements for a JCIDS document to the ISP.

5. Joint Capabilities Integration and Development System Document Development. While the fifth paragraph of ICDs (Threat and Operational Environment) and the fourth and ninth paragraphs of CDDs and CPDs (Threat Summary and Intelligence Supportability, respectively) are the primary intelligence-focused paragraphs in JCIDS documents, there are several other paragraphs in JCIDS documents that may need to refer to intelligence support or integration concepts. The tables on the following pages will identify specific intelligence support issues, by document type and paragraph, that sponsors should consider. To begin, ICDs require a different level of detail in identifying and discussing intelligence support. ICDs are somewhat focused and address specific capability gaps within the area of interest. ICDs should therefore provide sufficient information and analysis to allow identification of intelligence support needs, generally, for the applicable capability gaps.

Note: 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. The following list of general intelligence support considerations is provided to help sponsors and reviewers identify and assess intelligence supportability:

a. DOTMLPF considerations -- is the program expected to require new, unique, and unplanned support, or will it require additional existing support (as projected by the intelligence architecture)? If yes, then consider and address whether the current intelligence community architecture can support the new or additional support requirements identified and, if necessary, what DOTMLPF changes are required.

b. Dissemination of intelligence -- have dissemination support requirements (interoperability, connectivity, networks, systems, software, manpower, security) been addressed? Note: If the program will require or transmit TS/SCI information, then appropriate physical security concerns (accreditation and use of a SCIF) will need to be considered and addressed. Note: This may require addressing resource allocation (particularly with respect to finite resources, e.g., certain collection platforms).

c. If the program will require the use TS/SCI traffic systems, then: 1) will the end-to-end capability be compliant with all applicable security directives; and, 2) will the communication interface be technically compatible and compliant with DOD Intelligence Information System (DODIIS) and all other applicable standards?

d. Does the program expect to use or will it require systems that interface with foreign or Coalition information systems? If yes, has management and control of sensitive or classified information been addressed?

e. For programs using systems that have intelligence authorities as designated accrediting authorities, have security testing considerations been addressed in interoperability testing plans?

f. If the program will provide or enable intelligence collection, tasking, processing, exploitation, dissemination or production, consider whether required attributes of each capability are defined using appropriate measures of effectiveness (e.g., time, distance, effect [including scale]) and obstacles to overcome.

General Considerations: Consider whether each of the anticipated intelligence support categories will be available, suitable, and sufficient throughout all phases of the acquisition life cycle of the program or capability, not just any particular stage of the acquisition life cycle.

Para	Title	Initial Capabilities Document Considerations
1	Joint Functional Area	Ensure all appropriate functional areas are included as either a lead or supporting FCB (i.e., falls within the scope of a particular functional area or will require significant support from a functional area).
2	Required Capability	Address whether the desired capabilities described in the document relate to any of the key intelligence previous ICDs.
3	Concept of Operations	Identify and discuss any and all intelligence-based support requirements, resources, or other programs/capabilities that are required to enable the development and/or operational phase of the capability(ies) to achieve the desired outcome(s) throughout the acquisition life cycle.
4	Capability Gap	Ensure all required missions, tasks, and functions to enable operation of each capability are identified and discussed, and (following the analysis in paragraph 1) ensure that all intelligence support requirements, resources, or other programs/capabilities that will be necessary to achieving each capability are identified (in terms of the broad descriptions of categories discussed in Enclosure C).
5	Threat/Operational Environment	Provide a general description of the expected operational environment that the capabilities will be expected to operate in -- include specific threat capabilities, the nature of the threat, and threat tactics (both existing and anticipated, if available, and both lethal and non-lethal threats). For all ACAT ID programs, ensure the most current versions of DIA-validated threat documents are used to support JCIDS analysis and documentation. For all other programs, ensure the most current DIA- or Service-validated threat documents have been used to support threat analysis. Ensure judgments or extrapolations regarding adversarial capabilities are appropriate, logical, and consistent with existing DIA- and Service-validated assessments. Provide references to all applicable threat documents, and ensure current DIA-validated threat documents are provided (contact DIA/DWO as needed for specific guidance). Note: Threats are factors that an adversary can control and direct, or will be able to direct; threats are not environmental or natural factors such as weather or terrain.

6	Functional Solution Analysis	Ensure all materiel and non-materiel solutions considered during the functional solutions analysis (FSA) are adequately identified and discussed in this paragraph. Ensure the FSA efforts and documentation reflects that the intelligence community's expertise has been adequately leveraged. Discuss and analyze the intelligence-based DOTMLPF issues or items identified in the FSA.
7	Final Materiel Recommendation	Ensure the key boundary conditions, including DOTMLPF and policy considerations, for the performance of the AoA reflect a thorough understanding of the functional and operational areas, to include applicable threat considerations and intelligence support requirements and capabilities (i.e., ISR enablers).
App A	OV-1	Ensure high-level intelligence system connectivity and interoperability are accurately and adequately illustrated. Ensure the OV-1 illustration is consistent with the CONOPS described in Para 3. Provide citations to all applicable references. At a minimum, the CJCS 3170.01 series, CJCS 3312 series, DIAD 5000.02, and DIAD 5000.200 will be included in all JROC Interest and Joint Integration JCIDS documents.
App B	References	
App C	Acronym List	
		No additional requirements beyond those stated in the CJCS 3170.01 series (references a and b).

Table E-1. Initial Capabilities Document Intelligence Considerations

Turning to CDDs and CPDs, the level of discussion and analysis will be much more refined and must address specific support requirements for each capability (or capabilities) discussed in the CDD or CPD. As a program or capability document progresses from Phase 1 to Phase 2 review, and more substantially as that program or capability progresses from CDD to CPD, sponsors will be responsible for ever-increasing levels of refinement and analysis relating to intelligence supportability and shortfalls. General considerations for CDD and CPD intelligence support and detailed guidance on developing paragraph 9 ("Intelligence Supportability") are provided in subparagraph 6 below. As a reminder, note that sponsors are required to completely address intelligence supportability requirements and shortfalls in JCIDS documents.

Para	Title	CDD and CPD Considerations
1	Capability Discussion	<p>a. Identify and discuss the capability(ies) presented by the program document being reviewed.</p> <p>b. Ensure the capability gap(s) is/are adequately addressed in terms of detail and scope to allow sufficient supportability analysis, including (among other things): mission area, relevant range of military operations, and appropriate development and production timeframe considerations (development schedules, IOC, etc.).</p>
2	Analysis Summary	Ensure the summary of analysis includes the alternatives considered, objectives, criteria assumptions, conclusions, and overall recommendation. To the fullest extent possible, ensure the proposed approach does not duplicate existing or other developing joint capabilities.
3	CONOPS Summary	Address whether there are any key intelligence support capabilities required to enable the program or capability's operational status within the context of the CONOPS. Ensure the CDD/CPD addresses the employment of the proposed solution within the context of the CONOPS.
4	Threat Summary	Provide a general description of the expected operational environment in which the capabilities will be expected to operate -- include specific threat capabilities, the nature of the threat, and threat tactics (both existing and anticipated, if available, and both lethal and non-lethal threats). For all ACAT ID programs, ensure the most current versions of DIA-validated threat documents are used to support JCIDS analysis and documentation. For all other programs, ensure the most current DIA- or Service-validated threat documents have been used to support threat analysis. Ensure judgments or extrapolations regarding adversarial capabilities are appropriate, logical, and consistent with existing DIA- and Service-validated assessments. Provide references to all applicable threat documents, and ensure current DIA-validated threat documents are provided (contact DIA/DWO as needed for specific guidance). Note: Threats are factors that an adversary can control and direct, or will be able to direct; threats are not environmental or natural factors such as weather or terrain.
5	Program Summary	Address whether the program or capability 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 program, capability, or increment. Of particular interest are essential intelligence enablers or relevant shortfalls created by underdeveloped/undeveloped, unfunded/under-funded, and/or deactivated/retiring legacy systems. Also address the dependency upon other systems in the FoS or SoS.
6	System Capabilities Required	<p>a. Identify attributes and Key Performance Parameters (KPP) that are dependant upon or enabled by intelligence resources or support. Ensure that objective and threshold values for attributes are supported by adequate information and analysis.</p> <p>b. Ensure the rationale for each KPP complies with the analysis and findings of the applicable JROC-approved intelligence ICDs.</p>
7	FoS/SoS Synch	For capabilities that are part of a FoS/SoS (Family of Systems/Systems of Systems), ensure this section cites related JCIDS documents and existing capabilities. Ensure dependencies between these capabilities are defined (e.g., information exchange) and are consistent with the related documents. Ensure the CDD/CPD accurately captures the desired capabilities described in applicable ICDs.
8	IT & NSS	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.
9	Intel Support-ability	Refer to the information that follows for detailed format and content recommendations for developing paragraph 9.
10	E3 & Spectrum Support	If there are potential issues regarding Electromagnetic Environmental Effects (E3) interference from threat emitters, ensure these issues are identified in this section. Ensure this section is consistent with the threat discussion in paragraph 4 or in the related System Threat Assessment Report (STAR). For clarity, refer back to paragraph 4 or to the appropriate STAR.
11	Assets Req'd for IOC	No additional requirements beyond those stated in the CJCS 3170.01 series (references a and b).
12	Schedule for IOC	Ensure all timeframes for any enabling or program-required/dependent intelligence capabilities (existing and future) are consistent with the program or

		capability's development schedule and anticipated/desired IOC.
13	DOTMLPF Considerations	Ensure all DOTMLPF considerations have been identified and analyzed. If any intelligence-related DOTMLPF considerations have been identified through related ISP processes or during analysis done for paragraph 9, ensure these are addressed in this paragraph (or in paragraph 9).
14	Other 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), ensure appropriate information assurance measures have been considered and are in place prior to operational testing and fielding of the program or capability.
15	Program affordability	No additional requirements beyond those referenced in the CJCS 3170.01 series (references a and b).
App A	Architecture Graphics	
OV-1	Ensure high-level intelligence systems connectivity and interoperability are accurately and sufficiently illustrated. Ensure the OV-1 illustration is consistent with the CONOPS described in Paragraph 3.	
OV-2	Ensure that intelligence systems are identified as specifically as possible considering program maturation, that applicable needlines are drawn, and that information attributes (as discussed in the DODAF) for each exchange are included.	
OV-4	Ensure key intelligence contributing or receiving organizations are represented.	
OV-5	Ensure key intelligence activities are represented. Ensure the intelligence support requirements addressed in paragraph 9 are consistent with these activities.	
OV-6C	Ensure activity sequencing and timing for key intelligence support functions are addressed. Ensure a joint ISR context is represented, regardless of direct interfaces with intelligence nodes.	
SV-2	Ensure the system nodes, systems, and system items, including their related communications lay-downs, are shown.	
SV-4	Ensure any specific systems tied to the intelligence information needs identified in the OV-2 are represented.	
SV-5	Ensure key intelligence activities from the OV-5 are represented in the SV-5 matrix.	
SV-6	Ensure specific exchange and data details for intelligence information (from systems) are addressed. Be as specific as possible with regard to content, format, accuracy, units of measurement, periods of performance/updates, timeliness, and security with respect to	

	Enclosure C guidelines for intelligence information. If “SCI” is listed as a security level, ensure security considerations per Director of Central Intelligence Directives (DCIDs) 6/3 and 6/9 are addressed within the text of the CDD/CPD.	
No other guidance	For guidance on the TV-1, NCOW (Net-Centric Operations and Warfare) Reference Model Compliance Statement, Initial Interconnectivity and Interoperability Capability Profile, NR-KPP statement, and Key Interface Profile Declaration, see the CJCS 3170.01 series.	
IA	Ensure an Information Assurance Statement of Compliance is included.	
As needed	OV-7, SV-11, TV-2 (for specific guidance, see the CJCS 3170.01 series)	
App B	References Ensure all threat references are current DIA-validated references, as required, and that the appropriate intelligence ICDs are listed. For all documents, include the CJCS 3170.01 series and CJCSI 3312.01 as references.	
App C	Acronym List	No additional requirements beyond those stated in the CJCS 3170.01 series (references a and b).

Table E-2. CDD and CPD Intelligence Considerations

6. Guidance on Developing CDD and CPD Paragraph 9, “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 the program or capability in one, comprehensive section of the CDD or CPD. If intelligence support requirements or shortfalls are addressed in other areas of the document, then refer to that section and provide a reference in the applicable subparagraph of the intelligence supportability paragraph. It is the responsibility of the sponsor to ensure that all requirements of this instruction are satisfied. The following suggestions and general outline are provided to assist sponsors in this task, and should be considered and tailored to meet program-specific support requirements.

a. Level of Detail. The level of detail, refinement, and specificity of analysis in the intelligence supportability paragraph will usually increase as an acquisition program or capability proceeds from the initial (phase 1) of the Milestone B CDD to the final phase of the Milestone C CPD. This refinement and specificity will better enable sponsors to identify intelligence support requirements and shortfalls early in the JCIDS process.

b. Scope. Sponsors must identify, analyze, and discuss their program or capability's current and projected requirements for intelligence support (e.g., manpower, resources, and processes); its impact on joint intelligence strategy, policy, and architecture planning; and intelligence support shortfalls, if any. The intelligence supportability paragraph (and the analysis behind it) should be based on representative, validated scenarios and operational environments; sponsors are not expected to address all possible contingencies or possibilities. Moreover, this paragraph must address all requirements for intelligence support to a program or capability, regardless of whether the intelligence support required will be unique to the program or capability. Over time, as concepts are refined and revised, intelligence support requirements and shortfalls and/or threats applicable to a given program or capability may change. Sponsors must account for these changes as a program or capability progresses through the JCIDS process. It is essential that sponsors identify known intelligence requirements (and associated supportability issues) and address intelligence requirements and issues that may impact their program but which cannot be reasonably assessed given the information available during the drafting of the CDDs and CPDs. In addition, sponsors must continually update their JCIDS documents to account for changes to existing threats or the emergence of new threats to their program or capability.

c. Recommended Analytical Approaches. There are a number of analytical tasks that should be completed to ensure a program or capability's intelligence support requirements and shortfalls, if applicable, are adequately identified, defined and analyzed. These tasks include:

(1) Leverage work done for the ISP. Review the completed or ongoing analysis from the program or capability ISP Information Needs Discovery and Analysis Process. Depending on the maturity and completeness of the ISP analysis, some elements discussed below may have already been started or accomplished.

(2) Review the architecture graphics for intelligence requirements based on information needs. Determine whether these information needs are addressed adequately to allow a thorough assessment of intelligence supportability (as defined in enclosures C and E). Likewise, if the graphics appear incomplete with regard to intelligence support issues, then revise the graphics to ensure intelligence information needs are appropriately reflected.

(3) Carefully examine operational performance requirements in CDD and CPD paragraph 6 ("System Capabilities Required for the Current Increment"). Ensure that all intelligence requirements are captured within the appropriate architecture graphics (in sufficient detail to assess supportability). Sponsors must identify intelligence support requirements for each capability. For all intelligence requirements identified, address what intelligence infrastructure (e.g., platforms, systems, software, facilities) and resources (e.g.,

10 June 2010

manpower, funding) will be required to collect, compile, store, analyze, and disseminate the intelligence required. (Note: Sponsor is not expected to “reverse analyze” the entire intelligence cycle back to the source collection; rather, sponsor must 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.)

(4) Analyze the program or capability’s projected progression throughout all phases of a program, and identify all likely intelligence support requirements and shortfalls from the “pre-operational” phases (such as development, testing, and training) to the operational and sustainment phases of the acquisition life cycle.

d. Classification. As with all operational and warfighting analysis, ensure all information is appropriately classified, marked, and handled via appropriate security channels and systems.

e. General Considerations for Developing Paragraph 9. As stated above, sponsors should consider whether each of the stated support categories listed in Enclosure C will be available, suitable, and sufficient throughout all phases of a given program’s acquisition life cycle, not just any particular phase of the acquisition life cycle. In developing paragraph 9, consider the following list of intelligence support considerations and address each that applies.

Manpower: Have intelligence manpower requirements been addressed? Will this program have an effect on intelligence manning? (The effect on manning may be Service-specific or across the joint spectrum.)

Resource Allocation: Have all required intelligence resources been appropriately considered, and will such resources be available to be allocated to support development of the program? (Consider whether necessary resources are currently available and if such resources are funded, unfunded, or under-funded.)

Collection Management: Will there be appropriate collection management resources and infrastructure available to support the requirements resulting from the program? Note: Collection management support may include the allocation and use of collection assets that often address multi-level (tactical to national) intelligence concerns.

Signature Support: If appropriate, have all signature support (to include coverage, timeliness, content, fidelity, security, and scalability) and denial and deception support been considered and addressed?

GI&S/GEOINT Support: If appropriate, have all GI&S/GEOINT support requirements been considered and addressed (to include coverage, timeliness, security, scale, information format, and delivery to end user[s])?

Targeting Support: If appropriate, have requirements for targeting support been considered and addressed (to include target development, mission planning support, precise positioning support, battle damage assessment support, munitions effects assessment support, and weaponizing support)? Note: Targeting support often implicates aspects of collection management, signatures, and GEOINT support and affects resource allocation; thus, each should be considered in this area of analysis. Also note that that targeting will affect not only munitions (both kinetic and non-kinetic), but programs that rely upon munitions needing targeting support.

Combat Search and Rescue/Personnel Recovery (CSAR/PR) Intelligence Support: If appropriate, have requirements for CSAR/PR intelligence support been considered and addressed (to include infrastructure, coverage, timeliness, security, and scale of GI&S/GEOINT products)? Note: CSAR/PR support implicates GEOINT support, and often times requires collection management, signatures, and targeting support, and affects resource allocation, thus each should be considered in this area of analysis.

JIPOE/IPOE Support: If appropriate, have requirements for (JIPOE/IPOE) support been considered and addressed (to include coverage, timeliness, security, scale, and accuracy)?

Indications and Warning (I&W) Support: What, if any, requirements for I&W will be required, and has I&W support been considered and addressed (to include coverage (periodic or persistent), timeliness, security, form of support necessary (e.g., SIGINT, MASINT, etc.) and accuracy)? Note: I&W support often implicates collection management, signatures, and GEOINT support, and affects resource allocation. Therefore, each should be considered in this area of analysis.

Space Intelligence Support: If appropriate, have requirements for space intelligence support been considered and addressed (to include coverage (periodic or persistent), timeliness, security, form of support necessary (e.g., MASINT, etc.) and accuracy)?

Counter Intelligence (CI) Support: If applicable, have requirements for counter intelligence support to research and information protection efforts been considered and addressed? Note: CI support requirements will affect manpower and collection management.

Intelligence Training: Have intelligence training requirements (manpower, materials, facilities, equipment, increases in intelligence personnel with

existing skill sets, development of new skill sets) for initial program/capability standup been considered and addressed? Note: This will require consideration of manpower and resource allocation.

Intelligence Support to Training: Will intelligence support to training (and the associated infrastructure and effort) be required, and has it been considered and addressed? Note: This may require consideration of manpower and resource allocation.

DOTMLPF Considerations: Is the program expected to require new, unique, and unplanned support, or will it place additional burdens on the existing and projected intelligence architecture? If yes, then consider and address what, if any, DOTMLPF changes are needed to address these requirements.

Dissemination of Intelligence: Have dissemination support requirements (interoperability, connectivity, networks, systems, software, manpower, security) been addressed? Note: If the program will require or transmit TS/SCI information, then appropriate physical security concerns (accreditation and use of a SCIF) will need to be considered and addressed. Note: This may require addressing resource allocation (particularly with respect to finite resources, e.g., certain overhead collection platforms).

Intelligence Systems: If the program will require the use of TS/SCI traffic systems, then:

(1) Will the end-to-end capability be compliant with all applicable security directives?

(2) Will the communications interface be technically compatible and compliant with DODIIS and all other applicable standards?

Coalition Interoperability: Does the program expect to use or will it require systems that interface with foreign or Coalition information systems? If yes, then has management and control of sensitive or classified information been addressed?

Intelligence Accreditation: For programs using systems that have intelligence authorities as designated accrediting authorities, have security testing considerations been addressed in interoperability testing plans?

Measures of Effectiveness: If the program will provide or enable intelligence collection, tasking, processing, exploitation, dissemination or production, consider whether required attributes of each capability are defined using appropriate measures of effectiveness (e.g., time, distance, effect [including scale]) and obstacles to overcome.

General Considerations: Consider whether each of the anticipated intelligence support categories will be available, suitable, and sufficient throughout all phases of the acquisition life cycle of the program or capability, not just any particular stage of the acquisition life cycle.

f. Content and Format of Paragraph 9. As stated earlier, the content and organization of this paragraph should be tailored to best fit the nature of the program or capability and drafting style used in the document. With this in mind, the following provides a recommended, general format for the intelligence supportability paragraph. The recommendations below should be answered in light of the considerations above, and should be supplemented with the sponsor's unique knowledge and insight about the program.

7. Intelligence Supportability. Introduce the paragraph with a general description of the types and level of intelligence support required to enable the program's warfighting capability. For all requirements below, be as specific as possible, and include as many qualitative and quantitative attributes as possible (see Enclosure C for a specific attributes for each support category). If details regarding required qualitative or quantitative attributes are unknown due to program maturity (such as instances where sponsor is awaiting source selection) or otherwise, state what is not known and why. It is essential that sponsors identify all intelligence support needed and how those needs will be fulfilled by the intelligence community; alternatively, state what the anticipated shortfalls in support will be (i.e., address the considerations in the above subparagraph 6(e) – "General Considerations for Developing Paragraph 9.") Discussions related to intelligence support and shortfalls must address whether 1) the necessary or desired intelligence is available; 2) the available intelligence is suitable; and/or 3) the available intelligence is sufficient (i.e., with respect to quantity required -- for example, when dealing with data points or similar technical/MASINT collection or intelligence). If requirements are discussed in other places within the document, provide cross-references to those paragraphs.

a. Intelligence Support to Development and Testing. This subparagraph should reference intelligence threat and threat warning support that will be necessary for the program's development and testing, and should refer to Paragraph 4 of the CDD or CPD as appropriate. Using the above subparagraph 6(e) -- "General Considerations for Developing Paragraph 9" -- as a guide, the sponsor must address all program development and testing intelligence support requirements. Sponsor must ensure that intelligence information or services required for the effective operation of the program or capability can be tested in its anticipated or intended operational environment.

b. Intelligence Training. Consider and address what intelligence training requirements may be required for personnel supporting the program or capability as a result of developing and fielding the program or capability.

Sponsor should address unique training requirements, if any, that the program 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, special access program requirements, etc.). Refer to subparagraph 6(e), “General Considerations for Developing Paragraph 9,” for general guidance.

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

d. Intelligence Support to Operations. Using the above subparagraph 6(e), “General Considerations for Developing Paragraph 9,” and Enclosure C as guides, address all requirements for intelligence support that will be necessary to ensure successful operation and sustainment of the program or capability.

e. Intelligence Security Requirements. Identify all security requirements or considerations that the program or capability will require, and address how those security considerations are satisfied (e.g., classification levels; information sharing or releasability; certifications, and facility implications for receiving, using, and storing SCI; and all other security considerations that the program or capability will require [e.g., compliance with DCID 6/3 and DCID 6/9, references n and o]).

f. Potential Intelligence Support Shortfalls. Consider and address known, projected, or potential intelligence support shortfalls that result from, or may result from, the development, testing, operation, and/or the sustainment of the program or capability (to include manpower, training, doctrine, processes, or systems). As used in this subparagraph, “shortfalls” may include shortfalls related to the program or capability, those caused by the program or capability that affects other (existing or planned) programs, or which may exacerbate currently known shortfalls. Particular focus should be placed on shortfalls that could affect or delay development, testing, or fielding the program or capability, or those shortfalls that may degrade the operational effectiveness or sustainment of the program or capability. Sponsor must also consider and address the cause of these shortfalls (such as technological capability shortfalls, undefined common intelligence data/metadata standards, scheduling problems, or funding issues) and, if possible, estimate the magnitude of the shortfall in terms of scheduling delays, vulnerability, materiel, resources, training, manpower, and any other relevant criteria. (Note: Information related to intelligence shortfalls may be, or may become, classified information when associated with a shortfall; therefore, sponsors must ensure that all necessary security procedures are complied with.)

10 June 2010

g. Proposed Solutions. Identify, analyze, and discuss any and all possible solutions for shortfalls identified. Include key issues that must be resolved concerning each shortfall. Provide a plan to address such shortfalls and provide a schedule or deadline to remedy each shortfall. If the solution lies outside the control of the program office, or is deemed to be unobtainable under the existing intelligence infrastructure, manpower, etc., provide a recommendation on how to address the shortfall, and identify the organization with the authority and responsibility to address the shortfall.

8. Information Support Plan Document Development

a. The goal in developing and reviewing ISPs is to identify and resolve materiel (acquisition or procurement) and non-materiel (DOTMLPF issues) interoperability and supportability considerations related to DOD IT and NSS resources. To further this goal, DODI 4630.8 (reference h) charges the Under Secretary for Defense for Acquisition, Technology, and Logistics (USD(AT&L)) with managing the acquisition process of major defense acquisition program-related IT and NSS resources, and evaluating and ensuring that such systems are interoperable and supportable. The Joint Staff contributes to this process through intelligence (J-2) and interoperability (J-6) reviews or certifications.

b. ISP reviews will focus on evaluating intelligence-related systems for security and intelligence interoperability and supportability standards. (Note: J-6's review of ISPs will be a separate, but related, interoperability certification.) The table that follows identifies (by paragraph) specific areas within the ISP that sponsors should consider and address concerning ISP intelligence reviews.

Ch	Title	ISP Consideration
1	Intro- duction	<p>a. Overview. Address how the capability relates to the BA integrated architecture, or other intel support elements of other Joint Field Activity/Joint Force Commander (JFAs/JFCs) (like targeting sub-architectures as part of the Force Application JFA/JFC). Address whether the desired capabilities described relate to any of the key intelligence CRDs or MA ICDs.</p> <p>b. Program Data. Address any program related acquisition scheduling issues that have precluded conducting full intelligence information need and supportability analysis. For example, system level detail may not be available until prime contractor selections have been made, or until the functional solution has been more refined.</p>
2	Analysis <i>(Steps correspond with steps in the Information Needs and Discovery Process described in reference 1)</i>	<ul style="list-style-type: none"> ▪ Ensure the warfighting missions or enterprise business domain functions are consistent with the operational capabilities required IAW the associated CDD or CPD. (Step 1) ▪ Ensure intelligence information needs are completely addressed, clearly related to the missions or functions identified in Step 1 and include required qualitative and quantitative attributes as discussed in Enclosure C of this instruction. (Steps 2, 4, 5 and 6) ▪ Ensure the scope of analysis for and declaration of intelligence information needs includes all stages of acquisition (to include development, testing, training, and operation). (Step 13) ▪ Ensure the supportability assessment adequately considers the ability of the current/projected joint intelligence architecture to both quantitatively and qualitatively satisfy the intelligence information needs. (Step 8) ▪ Ensure the analysis in this section is consistent with intelligence information needs discussed in the associated CDD or CPD (primarily paragraph 9).
3	Issues	Ensure intelligence related shortfalls, issues, and associated mitigation strategies or resolution paths have been addressed. Ensure this section is consistent with paragraph 9 of the associated CDD or CPD.
App A	Refs	Ensure the Battlespace Awareness Joint Functional Concept is cited if applicable. Ensure the currency of any relevant DIA or Service-validated threat references used.
App E	SV-6	Ensure intelligence nodes and systems/subsystems have been adequately represented in the Systems Information Exchange Matrix (SV-6). Ensure specific exchange and data details for intelligence information (from systems) are addressed. Be as specific as possible with regard to content, format, accuracy, units of measurement, periodicity, timeliness, and security WRT Enclosure E guidelines for intelligence information. If "SCI" is listed as a security level, ensure security considerations per Director of Central Intelligence Directives (DCIDs) 6/3 and 6/9 are addressed within the text of the CDD/CPD.
App C	N/A	N/A (Interface Control Agreements)
App D	Acronyms	Ensure appropriate intelligence-related acronyms are included for clarity.

Table E-3. ISP Intelligence Considerations

(INTENTIONALLY BLANK)

ENCLOSURE F

REFERENCES

- a. CJCSI 3170.01 series, "Joint Capabilities Integration and Development System"
- b. CJCSM 3170.01 series, "Operation of the Joint Capabilities Integration and Development System"
- c. CJCSI 5123.01 series, "Charter of the Joint Requirements Oversight Council"
- d. CJCSI 6212.01 series, "Interoperability and Supportability of Information Technology and National Security Systems"
- e. DODD 5000.1, 12 May 2003, "The Defense Acquisition System"
- f. DODI 5000.2, 12 May 2003, "Operation of the Defense Acquisition System"
- g. DODD 4630.5, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- h. DODI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- i. DODD 5105.21, 18 February 1997, "Defense Intelligence Agency (DIA)"
- j. DIAI 5000.002, 30 March 2005, "Intelligence Threat Support for Major Defense Acquisition Programs"
- k. DIAD 5000.200, 19 January 2005, "Intelligence Threat Support for Major Defense Acquisition Programs"
- l. Acquisition Knowledge Sharing System (AKSS), "Acquisition Deskbook," <http://asks.dau.mil/jsp/default/jsp>.
- m. DODD 8500.1, 24 October 2002, "Information Assurance (IA)"
- n. Director of Central Intelligence Directive (DCID) 6/3, 5 June 1999, "Protecting Sensitive Compartmented Information within Information Systems"

10 June 2010

- o. DCID 6/9, 18 November 2002, “Physical Security Standards for Sensitive Compartmented Information Facilities”
- p. ICPM 2005-700-1, 1 December 2005, “Intelligence Community Update to Director of Central Intelligence (DCID) 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)”
- q. ICPM 2005-700-1, Attachment 1, 1 December 2005, “Annex D, Part I, Portable Electronic Devices in Sensitive Compartmented Information Facilities”
- r. ICPM 2005-700-1, Attachment 2, 1 December 2005, “Sample Table, Portable Electronic Device (PED) Mitigation”
- s. DODD 8100.1, 19 September 2002, “Global Information Grid (GIG) Overarching Policy”
- t. JP 2-01.2, 7 May 2002, “Joint Doctrine, Tactics, Techniques, and Procedures for Counter Intelligence Support to Operations”
- u. JP 2-01.3, 16 June 2009, “Joint Intelligence Preparation of the Operational Environment
- v. JP 2-03, Geospatial Intelligence Support to Joint Operations, March 22, 2007
- w. JP 2-0, Joint Intelligence, 22 June 2007
- x. JP 2-01, 7 October 2004, “Joint and National Intelligence Support to Military Operations”
- y. JP 2-01.1, 9 January 2003, “Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting”
- z. JP 3-50.2, 26 January 1996, “Doctrine for Joint Combat Search and Rescue”
- aa. JP 3-14, 9 August 2002, “Joint Doctrine for Space Operations”
- bb. CJCSI 3170.01 series, “Joint Capabilities Integration and Development System”
- cc. CJCSM 3500.04 series, “Universal Joint Task List (UJTL)”
- dd. Interim Defense Acquisition Guidebook (formerly DOD Regulation 5000.2-R, 5 April 2002), 30 October 2002

10 June 2010

- ee. Intelligence Community Policy for Metadata and Metadata Markup, 15 April 2003, Intelligence Community Chief Information Officer Executive Council
- ff. DOD Architecture Framework Version 1.0, Volume II, Product Descriptions, 9 February 2004
- gg. CJCSI 3137.01 series, “The Functional Capabilities Board Process”
- hh. JROCM 095-04, 14 June 2004, “Capstone Requirements Documents (CRDs) Conversion Guidance”
- ii. DODD 5200.39, 10 September 1997, “Security, Intelligence, and Counter Intelligence Support to Acquisition Program Protection”
- jj. JROCM 124-04, 9 July 2004, “Common Data Standards and Format to Enable Horizontal Integration (HI)”
- kk. DCID 1/8, 21 March 2001, “Management of National Imagery, Imagery Intelligence, Geospatial Activities, and Related Information”
- ll. DoDD 5105.60, July 29, 2009, NGA
- mm. DODD 5200.37, 18 December 1992, “Centralized Management of Department of Defense Human Intelligence (HUMINT) Operations”
- nn. DODD 5100.20, 23 December 1971 (Administrative Reissuance Incorporating Through Change 4, June 24, 1991), “The National Security Agency and the Central Security Service”
- oo. JSM 5100.01 series, “Organization of the Joint Staff”
- pp. DOD Indications and Warning System Operations Manual, J2M-0177-01-96, January 1997
- qq. CJCSI 3901.01B, 15 July 2004 (current as of 22 August 2007), “Requirements for Geospatial Information and Services”
- rr. CJCSI 3160.01, 13 February 2009, “No-Strike and the Collateral Damage Estimation Methodology”

(INTENTIONALLY BLANK)

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ACAT	acquisition category
AoA	analysis of alternatives
AMA	analysis of material/non-materiel approaches
BA	battlespace awareness
BA FCB	Battlespace Awareness Functional Capability Board
BAWG	battlespace awareness (FCB) working group
BDA	battle damage assessment
C2	command and control
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
C4ISP	command, control, communications, and intelligence support plan
CDD	capability development document
CIC	critical intelligence category
CIO	chief information officer
CPD	capability production document
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CONOPS	concept of operations
CRD	capstone requirements document
CRM	comment resolution matrix
CSAR	combat search and rescue
CSS	Central Security Service
DAB	Defense Acquisition Board
DCID	Director, Central Intelligence Directive
DCGS	Distributed Common Ground System
DIA	Defense Intelligence Agency
DIA/DR	Director, Defense Intelligence Agency
DISA	Defense Information Systems Agency
DJ-2	Director for Intelligence, Joint Staff
DOD	Department of Defense
DODI	Department of Defense instruction
DODIIS	Department of Defense Intelligence Information System
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel and facilities

FAA	functional area analysis
FNA	functional needs analysis
FSA	functional solutions analysis
FCB	Functional Capabilities Board
GDIP	General Defense Intelligence Program
GEOINT	geospatial intelligence
GI&S	geospatial information and services
GIG	Global Information Grid
HUMINT	human intelligence
IA	information assurance
IC	Intelligence Community
ICD	initial capabilities document
ICMR	Intelligence Community Metadata Registry
ICWG	intelligence certification working group
IMINT	imagery intelligence
INFOSEC	information security
IPB	intelligence preparation of the battlespace
IRCO	Intelligence Requirements Certification Office
ISP	information support plan
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
ITWA	initial threat warning assessment
JCD	joint capabilities document
JCPAT-E	Joint C4I Program Assessment Tool-Empowered
JCS	Joint Chiefs of Staff
JFA	joint field activity
JIIB	Joint Intelligence Interoperability Board
JIPB	joint intelligence preparation of the battlespace
JITC	Joint Interoperability Test Command
JP	Joint Publication
JPD	joint potential designator
JROC	Joint Requirements Oversight Council
JSBA	joint systems baseline assessment
JWICS	Joint Worldwide Intelligence Communications System
J-2	Directorate for Intelligence, Joint Staff
J-2S	Directorate for Intelligence Assessments, Joint Staff
J2S-4/IRCO	Intelligence Requirements Certification Office, Joint Staff
KM/DS	knowledge management/decision support tool
MA ICD	mission area initial capabilities document
MASINT	measurement and signatures intelligence

MDA	milestone decision authority
MDAP	major defense acquisition program
MEA	munitions effects assessment
MER	manpower estimation report
METOC	meteorological and oceanographic
MIP	military intelligence program
MNS	mission need statement
MTI	moving target indicator
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NIP	National Intelligence Program
NSP	National Signatures Program
NSA/CSS	National Security Agency/Central Security Service
NSS	National Security System
ORD	operational requirements document
OSD	Office of the Secretary of Defense
POC	point of contact
SIGINT	signals intelligence
SIPRNET	Secret Internet Protocol Router Network
TTP	tactics, techniques, and procedures
USD(AT&L)	Under Secretary for Defense for Acquisition, Technology, and Logistics
VDJ-2	Vice Director for Intelligence, Joint Staff

DEFINITIONS

acquisition category (ACAT). Categories established to facilitate decentralized decision-making, and execution and compliance with statutorily imposed requirements. The ACAT category determines the level of review, decision authority, and applicable procedures. The following is a general list of ACAT levels I-III:

ACAT I -- Programs are Major Defense Acquisition Programs (MDAPs). An MDAP is defined as a program estimated by the USD(AT&L) to require eventual expenditure for research, development, test, and evaluation of more than \$365 million (FY 00 constant dollars) or procurement of more than \$2.19 billion (FY 00 constant dollars), or those designated by the USD(AT&L) to be ACAT I. ACAT I programs have two subcategories, and the USD(AT&L) designates programs as ACAT ID or ACAT IC.

ACAT ID -- The Milestone Decision Authority (MDA) is USD(AT&L). The “D” refers to the Defense Acquisition Board (DAB), which advises the USD(AT&L) at major decision points.

ACAT IC -- The MDA is the DOD component head or, if delegated, the DOD component acquisition executive (CAE). The “C” refers to component.

ACAT IA -- programs are Major Automated Information Systems (MAISs) or programs designated by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) to be ACAT IA. A MAIS is an Automated Information System (AIS) program that is (1) designated by the ASD (C3I) as a MAIS; or (2) estimated to require program costs in any single year in excess of \$32 million (FY 00 constant dollars), total program in excess of \$126 million (FY 00 constant dollars), or total life cycle costs in excess of \$378 million (FY 00 constant dollars). MAISs do not include highly sensitive classified programs (as determined by the Secretary of Defense) or tactical communication systems). For the purpose of determining whether an AIS is a MAIS, the following shall be aggregated and considered a single AIS: (1) the separate AISs that constitute a multi-element program; (2) the separate AISs that make up an evolutionary or incrementally developed program; or, (3) the separate AISs that make up a multi-component AIS program.

ACAT IA programs have two sub-categories (ASD(C3I) designates programs as ACAT IAM or ACAT IAC):

ACAT IAM -- The MDA is the chief information officer (CIO) of the Department of Defense, the ASD(C3I). The “M” (in ACAT IAM) refers to a Major Automated Information System (MAIS).

ACAT IAC -- The DOD CIO has delegated milestone decision authority to the CAE or component CIO. The "C" (in ACAT IAC) refers to component.

ACAT II -- programs are defined as those acquisition programs that do not meet the criteria for an ACAT I program, but do meet the criteria for a major system. A major system is defined as a program estimated by the DOD component head to require eventual expenditure for research, development, test, and evaluation of more than \$140M in FY 00 constant dollars, or for procurement of more than \$660M in FY 00 constant dollars or those designated by the DOD component head to be ACAT II. The MDA is the DOD CAE.

ACAT IIA -- Programs are AIS programs that do not meet the criteria for ACAT IA, but are designated by the Army Acquisition Executive or Army Chief Information Officer for PM management and Army Major Automated Information System Review Council (MAISRC) review. (Army only.)

ACAT III -- Programs are defined as those acquisition programs that do not meet the criteria for an ACAT I, an ACAT IA, or an ACAT II. The MDA is designated by the CAE and shall be at the lowest appropriate level. This category includes less-than-major AISs.

acquisition life cycle. The total expected period of time that a program or capability will be in active development, production, operation, and sustainment. This timeframe includes the JCIDS process and extends to the complete retirement of the substance/object of a program or capability.

all-source intelligence. 1. Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked.

analysis of alternatives. An analysis that illuminates the relative advantages of the alternatives being considered. The analysis of alternatives aids in judging if the proposed alternatives offer sufficient military or economic benefit to be worth the cost.

analysis of material/non-materiel approaches (AMA). The Joint Capabilities Integration and Development System analysis to determine the best approach or combination of approaches to provide the desired capability or capabilities. Though the AMA is similar to an analysis of alternatives (AoA), it occurs earlier

in the analytical process. Subsequent to approval of an initial capabilities document, which may lead to a potential acquisition category I/IA program, program analysis and evaluation provides specific guidance to refine this initial AMA into an AoA.

architecture. The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

availability. In the context of this instruction, a determination that the intelligence information, infrastructure, or resources are, or are expected to be, available to support the operational system or program throughout all phases of its acquisition life cycle. This assessment takes into consideration the operational requirements and acquisition schedule of the system or program, current and proposed defense and national intelligence support infrastructures, C4I architectures, funding levels and allocations, and other materiel and non-materiel issues.

battlespace. The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces, facilities, weather, terrain, the electromagnetic spectrum, and the information environment within the operational areas and areas of interest.

battlespace awareness. Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate assessments, in order to successfully apply combat power, protect the force, and/or complete the mission.

capability. The ability to achieve a desired effect under specified standards and conditions by performing a task or set of tasks. It is defined by an operational user and expressed in broad operational terms in the format of a joint capabilities document, initial capabilities document or a joint doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) change recommendation. In the case of materiel proposals, the definition will progressively evolve to DOTMLPF performance attributes identified in the capability development document and the capability production document.

collection management. The process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required.

capability development document (CDD). A document that captures the information necessary to develop a proposed program or programs, normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable, and technically mature capability.

capability production document (CPD). A document that addresses the production elements specific to a single increment of an acquisition program.

capstone requirements document (CRD). A document that contains capabilities-based requirements that facilitate the development of CDDs and CPDs by providing a common framework and operational concept to guide their development.

capstone threat assessments. Comprehensive, authoritative assessments of foreign threats in major warfare areas. CTAs project the threat environment in a given warfare area out 20 years and constitute the DOD Intelligence Community position with respect to those warfare areas.

certification. A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process.

comment priorities. Assessors will designate their comments according to the issues or problems addressed by the comment. Below is a short synopsis of comment types.

a. Critical -- Indicates nonconcurrency with the document, for both the Phase 1 (O-6 or planner-level) and Phase 2 (general/flag officer) review, until the comment is satisfactorily resolved.

b. Substantive -- Provided because a section in the document appears to be or is potentially unnecessary, incorrect, misleading, confusing, or inconsistent with other sections.

c. Administrative -- Corrects what appears to be a typographical, format, or grammatical error.

concept of operations. A verbal or graphic statement, in broad outline, of a commander's assumptions or intent with regard to an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in

succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose.

counter intelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Includes any representations such as characters or analog quantities to which meaning is or might be assigned.

dissemination. In intelligence usage, the delivery of intelligence to users in a suitable form.

DOD component. The DOD components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, DOD field activities, and all other organizational entities within the Department of Defense.

electromagnetic environmental effects. The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms.

electronic intelligence. Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.

evolutionary acquisition. Preferred DOD strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing up front the need for future capability improvements.

functional area. A broad scope of related joint warfighting skills and attributes that may span the range of military operations. Specific skill groupings that make up the functional areas are approved by the Joint Requirements Oversight Council.

Functional Capability Board. A permanently established body that is responsible for the organization, analysis, and prioritization of joint warfighting capabilities within an assigned functional area.

gatekeeper. The Vice Director, J-8, is the individual that makes the initial joint potential designation of JCIDS proposals. The gatekeeper will also make a determination of the lead and supporting FCBs for capability proposals. The gatekeeper is supported in these functions by USJFCOM, J-6, J-7, and the FCB Working Group leads.

geospatial information and services. The concept for collection, information extraction, storage, dissemination, analysis, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. Geospatial information is information produced by multiple sources to common interoperable data standards, which data are used for military planning, training, and operations including navigation, mission planning, mission rehearsal, modeling, simulation and precise targeting. This information provides the basic framework for battlespace visualization, and may be presented in the form of printed maps, charts, and publications; in digital simulation and modeling databases; in photographic form; or in the form of digitized maps and charts or attributed centerline data. Geospatial services include tools that enable users to access and manipulate data. They also include instruction, training, laboratory support, and guidance for the use of geospatial data.

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

indications and warning. Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or Coalition military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied and/or Coalition nations; hostile reactions to U.S. reconnaissance activities; terrorist attacks; and other similar events.

human intelligence. A category of intelligence derived from information collected and provided by human sources.

increment. A militarily useful and supportable operational capability that can be effectively developed, produced or acquired, deployed, and sustained. Each increment of capability will have its own set of threshold and objective values set by the user. Spiral development is an instance of an incremental

development strategy where the end state is not known. Technology is spiraled to maturity and injected into the delivery of an increment of capability.

imagery intelligence. Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors, such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media.

information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

information technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

initial capabilities document (ICD). Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects and time. The ICD summarizes the results of the DOTMLPF analysis and describes why non-material changes alone have been judged inadequate in fully providing the capability.

information operations (IO). Actions taken to affect adversary information and information systems while defending one's own information and information systems.

information support plan (ISP). The ISP provides a mechanism to identify and resolve implementation issues related to an acquisition program's information technology (IT) and National Security Systems information infrastructure support and information interface requirements. It identifies IT and information (including intelligence) needs, dependencies, and interfaces for programs in all acquisition categories, focusing on net-readiness, interoperability, information supportability, and information sufficiency concerns.

information technology (IT). Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a component directly, or used by a contractor under a contract with the component, which (1) requires the use of such equipment; or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “IT” also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term “IT” does not include any equipment that is acquired by a federal contractor incidental to a federal contract. The term “IT” includes National Security Systems.

intelligence. The product (information) resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity that results in the product (information) and to the organizations engaged in such activities.

intelligence certification. The affirmation that requirements for intelligence support have been completely and adequately declared and identified; adequately assessed for projected supportability; that critical intelligence supportability or threat-related issues identified during coordination of program documents have been addressed; and that any projected shortcomings in intelligence support will be dealt with in an appropriate manner. This certification occurs as a prerequisite for the Joint Capabilities Integration and Development System and defense acquisition processes, and occurs at each acquisition milestone.

intelligence requirements. For the purposes of this CJCSI, intelligence requirements refer to requirements for intelligence information, infrastructure, or systems (as opposed to intelligence collection requirements).

intelligence supportability. The availability, suitability, and sufficiency of intelligence information and capabilities to support the requirements or system defined in program documents.

intelligence, surveillance, and reconnaissance. An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated and collaborative intelligence and operations function.

interoperability. The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information technology and National Security Systems interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment.

interoperability certification. A J-6 certification process that parallels the intelligence certification process, in which DIA and J-2 are assessor and contributing organizations. (See CJCSI 6212.01, reference d for further details.)

joint capabilities document (JCD). The JCD is an overarching document that identifies a set of capabilities supporting a defined mission area that is identified in the Family of Joint Future Concepts, concept of operations (CONOPS), or Unified Command Plan-assigned missions. The capabilities are identified by analyzing what is required across all functional areas to accomplish the mission. The gaps or redundancies are then identified by comparing the capability needs to the capabilities provided by existing or planned systems. The JCD will be used as a baseline for one or more initial capabilities documents, but cannot be used for the development of capability development or capability production documents. The JCD will be updated as changes are made to the Family of Joint Future Concepts, CONOPS or assigned missions.

Joint C4I Program Assessment Tool-Empowered (JCPAT-E). A tool set that DISA operates and maintains for the Joint Staff and OASD(NII)/DOD CIO that provides a collaborative work area, automated mail and distribution function, and an archival capability.

Joint Intelligence Preparation of the Operational Environment. The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's (JFC's) decision-making process. It is a continuous process that involves four major steps: 1) defining the total operational environment; 2) describing the impact of the operational environment; 3) evaluating the adversary; and 4) determining and describing adversary potential courses of action (COAs), particularly the adversary's most likely COA and the COA most dangerous to friendly forces and mission accomplishment. The JIPOE process assists JFCs and their staffs in achieving information superiority by identifying adversary centers of gravity (COGs), focusing intelligence collection at the right time and place, and analyzing the impact of the operational environment on military operations.

joint potential designator (JPD). A designation assigned by the gatekeeper to determine the JCIDS validation and approval process and the potential requirement for certifications/endorsements.

a. “JROC interest” designation will apply to all acquisition category (ACAT) I/IA programs and ACAT II and below programs where these capabilities have a significant impact on joint warfighting or have a potentially significant impact across Services or interoperability in allied and Coalition operations. This designation may also apply to intelligence capabilities that support DOD and national intelligence requirements. These documents will receive all applicable certifications, including a weapon safety endorsement when appropriate, and be staffed through the JROC for validation and approval. An exception may be made for ACAT IAM programs without significant impact on joint warfighting (i.e., business oriented systems). These programs may be designated either Joint Integration, Joint Information, or Independent.

b. “Joint Integration” designation will apply to ACAT II and below programs where the capabilities and/or systems associated with the document do not significantly affect the joint force and an expanded review is not required. Staffing is required for applicable certifications (IT and National Security Systems interoperability and supportability and/or intelligence), and for a weapon safety endorsement, when appropriate. Once the required certification(s)/weapon safety endorsement are completed, the document may be reviewed by the FCB. “Joint Integration” documents are validated and approved by the sponsoring component.

c. “Joint Information” designation applies to ACAT II and below programs that have interest or potential impact across Services or agencies but do not have significant impact on the joint force and do not reach the threshold for JROC Interest. No certifications or endorsements are required. Once designated “Joint Information,” staffing is required for informational purposes only and the FCB may review the document. “Joint Information” documents are validated and approved by the sponsoring component.

d. “JCB Interest” designation applies to any program deemed by the Director of the Joint Capabilities Board requiring Joint Staff review.

Joint Worldwide Intelligence Communications System (JWICS). The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing.

key performance parameter (KPP). Those attributes or characteristics of a system that are considered critical or essential to the development of an

effective military capability, and those attributes that make a significant contribution to the key characteristics as defined in the Joint Operations Concept. KPPs are validated by the Joint Requirements Oversight Council (JROC) for JROC interest documents, and by the DOD component for Joint Integration or Independent documents. Capability development and capability production document KPPs are included verbatim in the acquisition program baseline.

knowledge management/decision support tool (KM/DS). A tool set that replaced the legacy system JCPAT for processing, coordinating, and storing functions for JCIDS documents. KM/DS is a J-8 system and facilitates staffing and commenting functions for JROC Interest and Joint Impact documents.

material solution. Correction of a deficiency, satisfaction of a capability gap or incorporation of new technology that results in the development, acquisition, procurement, or fielding of a new item (including ships, tanks, self-propelled weapons, aircraft, etc., and related software, spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without disruption as to its application for administrative or combat purposes. In the case of family of systems and system of systems approaches, an individual materiel solution may not fully satisfy a necessary capability gap on its own.

measurement and signature intelligence. Intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted.

military deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

milestone. Major decision points that separate the stages of an acquisition program. In the context of this instruction, there are three milestones in the JCIDS process (milestones A, B, and C) and each milestone culminates with a final intelligence certification review and an intelligence certification letter (if appropriate per this instruction).

National Security Systems. Telecommunications and information systems operated by the Department of Defense -- the functions, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities

related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

net-centric. Exploitation of advancing technology moving from an applications-centric to a data-centric paradigm -- that is, providing users the ability to access applications and services through Web services, an information environment comprised of interoperable computing and communication components.

net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables user access and use of resources both collaboratively and asynchronously, regardless of time and place. It is the ability of a program or system to integrate with, offer services to, and exploit the services of a net-centric environment. Net-centricity provides substantial improvement to military situational awareness and significantly shortened decision-making cycles.

net-ready. DOD IT/NSS that meets required information needs, information timeliness requirements, has information assurance accreditation, and meets the attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. DOD IT/NSS that is net-ready enables warfighters and DOD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata and collaboration to provide an environment that promotes unifying actions among all participants. See reference d, the current version of the CJCSI 6212.01 series, for more information.

Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP assesses information needs, information timeliness, information assurance and net-enabled attributes required for information exchange and use. The NR-KPP consists of measurable and testable characteristics and/or performance metrics required for the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP consists of the following elements: compliance with DODD 5200.39 Net-Centric Operations and Warfare Reference Model (reference ii); compliance with applicable Global Information Grid key interface profiles; verification of compliance with DOD information assurance requirements; and supporting

integrated architecture products required to assess information exchange and use for a given capability.

non-materiel solution. Changes in doctrine, organization, training, materiel, leadership and education, personnel, facilities or policy (including all human systems integration domains) to satisfy identified functional capabilities. The materiel portion is restricted to commercial or non-developmental items that may be purchased commercially, or by purchasing more systems from an existing materiel program.

objective value. The desired operational goal associated with a performance attribute, beyond which any gain in utility does not warrant additional expenditure. The objective value is an operationally significant increment above the threshold. An objective value may be the same as the threshold when an operationally significant increment above the threshold is not significant or useful.

operational view (OV). The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DOD missions. DOD missions include both warfighting missions and business processes. The OV contains graphical and textual products identifying the operational nodes and elements, assigned tasks and activities, and information flows required between nodes. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges.

signals intelligence (SIGINT). 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation SIGINT, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals.

sufficiency. In the context of this CJCSI, an assessment of whether the intelligence information, infrastructure, and/or resources are, or are expected to be, sufficient to support the operational capability, system, or program. This assessment takes into consideration the operational requirements and acquisition schedule of the system or program and determines the minimum requirements for the current and proposed defense and national intelligence support infrastructures, C4I architectures, funding levels and allocations, and other materiel and non-materiel activities.

suitability. In the context of this instruction, an assessment of whether the intelligence information, infrastructure and/or resources are, or are expected to be, suitable to support the operational system or program. This assessment considers the operational requirements and acquisition schedule of the system

or program, and determines if the current or proposed defense and national intelligence support infrastructures, C4I architectures, and funding levels and allocations are, or are expected to be, suitable to satisfy the operational need.

sponsor. The DOD component, principal staff assistant, or domain owner responsible for all common documentation, periodic reporting, and funding actions required to support the capabilities development and acquisition process for a specific JCIDS capability proposal.

supportability. In the context of this instruction, an assessment of whether intelligence support will be available, suitable, and sufficient to support a program or capability. Assessing supportability requires a comparison of the sponsor's stated or derived intelligence support requirements with the expected intelligence support capabilities, as anticipated throughout a program or capability's life cycle.

sustainment. The supply and delivery of personnel, training, logistic, and other support required to maintain and prolong operations or combat until successful accomplishment or revision of the mission or of the national objective.

system of systems (SoS). A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole. The development of a SoS solution will involve trade space between the systems as well as within an individual system performance. An example of a SoS would be a combat aircraft. While the aircraft may be developed as a single system, it could incorporate subsystems developed for other aircraft. For example, the radar from an existing aircraft may be incorporated into the aircraft being developed rather than developing a new radar. The SoS in this case would be the airframe, engines, radar, avionics, etc. that make up the entire combat aircraft capability.

System Threat Assessment Report (STAR). The basic authoritative threat assessment, tailored for and focused on a particular (single) U.S. major defense acquisition program. It describes the threat to be countered and the projected threat environment. Mandatory elements of the STAR are included in the enclosed STAR Guidance and Format. In some references, the STAR is referred to as the System Threat Assessment (STA). Production centers and commands will draw from CTAs in the appropriate warfare areas and focus threat intelligence on the specific U.S. weapons system or systems supported by the STAR.

systems view. An architecture view that identifies the kinds of systems, how to organize them, and the integration needed to achieve the desired operational

capability. It will also characterize available technology and systems functionality.

target. 1. An area, complex, installation, force, equipment, capability, function, or behavior identified for possible action to support the commander's objectives, guidance, and intent. Targets fall into two general categories: planned and immediate. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. 3. An area designated and numbered for future firing. 4. In gunfire support usage, an impact burst that hits the target.

targeting. The process of selecting and prioritizing targets and matching the appropriate response to them, taking account of operational requirements and capabilities.

technical view. An architecture view that describes how to tie the systems together in engineering terms. It consists of standards that define and clarify the individual systems technology and integration requirements.

threat. The sum of the potential strengths, capabilities, and strategic objectives of any adversary which can limit or negate U.S. mission accomplishment or reduce force, system, or equipment effectiveness.

threat validation. The substantiation of threat documentation for appropriateness and completeness of the intelligence, reasonableness of the judgments, consistency with existing intelligence positions, and logic of extrapolations from existing intelligence.

threshold value. A minimum acceptable operational value below which the utility of the system becomes questionable.

validation. The review of documentation by an operational authority other than the user to confirm its operational capability. Validation is a precursor to approval.

weaponneering. The process of determining the quantity of a specific type of lethal or nonlethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapons effect, munitions delivery accuracy, damage criteria, probability of kill, and weapon reliability.

^[3] Please note that ISPs have changed from “*Intelligence* Support Plans” that contained a formal intelligence support section, to “*Information* Support Plans” that no longer have a formal intelligence section. ISPs are now focused on identifying, explaining, and depicting (with graphics) a program’s IT and NSS architecture, connectivity, and interoperations.

(INTENTIONALLY BLANK)