



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6

DISTRIBUTION: A, B, C, J

CJCSI 6212.01C
20 November 2003

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure O

1. Purpose. This instruction

- a. Establishes policies and procedures for the J-6 interoperability requirements and supportability certification and validation of Joint Capabilities Integration and Development Systems (JCIDS) Acquisition Category (ACAT) programs cited in references a and b, and for all non-ACAT and fielded systems.
- b. Provides detailed instructions for the implementation of information technology (IT) and National Security Systems (NSS) interoperability and supportability certifications as referenced in CJCSI 3170.01 Series, DODD 4630.5, DODI 4630.8, and DODD 8100.1 (references a, b, e, g and y, respectively).
- c. Details the Net-Ready Key Performance Parameter (NR-KPP) in lieu of the Interoperability KPP (I KPP) discussed in CJCSI 3170.01C and CJCSM 3170.01. The NR-KPP shall be used to assess information needs, information timeliness, information assurance, joint interoperability and supportability, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP shall consist of measurable, testable or calculable characteristics and performance metrics required for the timely, accurate and complete exchange and use of information.
- d. Establishes policies and procedures for Joint Interoperability Test Command (JITC) system interoperability test certification.
- e. Provides additional guidance for development of Information Support Plans (ISPs) and establishes procedures for certification of ISPs

for all programs, including ACAT, non-ACAT, and fielded systems with regard to the J-6 interoperability requirements and supportability certification. The ISP replaces the Command, Control, Communications, Computers and Intelligence Support Plan (C4ISP) originally in the DOD 5000 series directives.

2. Cancellation. CJCSI 6212.01B, 8 May 2000, Interoperability and Supportability of National Security Systems, and Information Technology Systems is canceled.

3. Applicability

a. This instruction implements the policies and procedures for developing, evaluating and providing interoperability and supportability certification in support of the JCIDS, which replaces the Requirements Generation System for ACAT, non-ACAT and fielded capabilities. This instruction applies to Services, combatant commands, Joint Staff, Defense agencies, and joint and combined activities. This instruction also applies to other agencies preparing and submitting JCIDS documents in accordance with references d and e.

b. This instruction is applicable to all IT and NSS (systems or services) acquired, procured or operated by any component of the Department of Defense, to include:

(1) All ACAT programs, non-ACAT activities and procurements, and fielded systems. ACAT programs include all DOD 5000-Series IT and NSS acquisition systems. Non-ACAT activities and procurements include all defense technology IT and NSS projects, IT and NSS pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations (ACTD), Advanced Technology Demonstrations (ATD), and Joint Warrior Interoperability Demonstrations (JWID) when selected for acquisition or procurement), joint experimentations, Joint Tests and Evaluations (JTE); non-DOD 5000 Series IT and NSS acquisitions or procurements (e.g., the Combatant Commander Command and Control Initiative Program (C2IP), Combatant Commander Initiatives Fund (CCIF), Combatant Commander Field Assessments, military exploitation of reconnaissance and technology programs, and tactical exploitation of national capabilities programs). Fielded systems are post-acquisition IT and NSS operational systems.

(2) All inter- and intra- component IT and NSS that exchange and use information to enable units or forces to operate effectively in joint, combined, coalition, and interagency operations and simulations.

(3) All IT and NSS acquired, procured, or operated by DOD intelligence agencies, DOD component intelligence elements, and other DOD intelligence activities engaged in direct support of DOD missions. This instruction recognizes that special measures may be required for protection and/or handling of foreign intelligence or counterintelligence information, or other need to know information. Accordingly, implementation of this instruction must be tailored to comply with separate and coordinated Director of Central Intelligence (DCI) directives and intelligence community policies.

(4) All DOD IT and NSS external information exchange interfaces with other US government departments and agencies, combined and coalition partners, and multinational alliances (e.g., North Atlantic Treaty Organization).

c. The overall objective of this policy decision is to develop, acquire, and deploy IT and NSS that (1) meet the essential operational needs of US forces; (2) are interoperable with existing and proposed IT and NSS; (3) are supportable over the existing and planned global information grid; and (4) are interoperable with allies and coalition partners.

d. This instruction applies to any organization that supports the Joint Requirements Oversight Council (JROC) in its role to advise the Chairman of joint interoperability between existing and future IT and NSS.

e. All classified programs will comply with this instruction, but processes will be tailored to account for special security considerations.

f. This instruction does not preclude the need to refer to basic guidance and direction on defense acquisition and interoperability (references a through e and g).

4. Scope

a. This instruction addresses the interoperability and supportability of IT and NSS. This policy applies to all ACAT, Non-ACAT and fielded programs. IT and NSS are defined in Part II of the Glossary. Intelligence supportability is addressed in a separate, but related, process conducted by the J-2. Information assurance (IA) accreditation is addressed through the references d, f and r through w; IA accreditation for sensitive compartmented information (SCI) systems is addressed in references z, aa and bb.

b. This document removes most references to automated information systems (AIS) as defined in Part II of the Glossary. The generation and

implementation of AIS requirements involve unique circumstances and the user is directed to use the basic process in reference d. When modifications are absolutely essential to accommodate the unique aspects of a particular capability or system, they will be accomplished with approval of the Validation Authority.

6. Policy

a. It is DOD policy that all IT and NSS and major modifications to existing IT and NSS will be compliant with the Clinger-Cohen Act, DOD interoperability regulations and policies, and the most current version of the DOD Information Technology Standards Registry (DISR). Establishing interoperability and supportability in a DOD system is a continuous process that must be managed throughout the lifecycle of the system. The NR-KPP is comprised of the following elements: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM), applicable Global Information Grid (GIG) Key Interface Profiles (KIP), DOD information assurance requirements, and supporting integrated architecture products required to assess information exchange and use for a given capability.

b. This document explains the processes necessary to implement full-spectrum interoperability from an integrated and net-centric approach. To accomplish this, consideration will be placed on information needs, information timeliness, information assurance and net-enabled concepts using integrated architectures for a given capability. The NR-KPP is a mandatory element of all JCIDS documents and is required to receive interoperability certification.

c. Formats and processes in this instruction are mandatory for all ACAT, non-ACAT and other fielded capabilities. In most cases, this document will refer to references a and b for formats of capability documents. This document will provide additional information as it applies to supportability certification.

d. The J-6 certification process is an integral part of the JCIDS process. Interoperability requirements certifications granted under the former requirements generation system remain valid except as detailed below:

(1) The I-KPP contained in capstone requirements documents (CRDs) and Operational Requirements Documents (ORDs), already approved or directed by the JROC prior to JCIDS implementation, will continue to be valid until superseded by completed integrated architectures. The new JCIDS supports new CRDs directed by the JROC. Those new CRDs will develop their NR-KPP in accordance with

(IAW) the procedures documented in Enclosure D. The I-KPP currently cited in CJCSI 3170.01C and CJCSM 3170.01 has been superseded by the NR-KPP and meets the intent of JROC direction.

(2) Mission Needs Statement (MNSs) that have initiated staffing in the Joint C4I Program Assessment Tool will continue through the normal staffing process; however, J-6 will assess MNS but will not certify for interoperability requirements certification. J-6 will only concur or nonconcur based upon interoperability concerns and implications. IAW references a and b, no new MNS will be accepted for staffing.

(3) IAW references a and b, ORDs will be accepted for staffing IAW the current CJCSI 3170.01B, dated 15 April 2001, for 6 months after signing CJCSI 3170.01C, i.e., until 24 December 2003, unless otherwise extended by the JROC. Therefore, I KPP for those documents will be IAW CJCSM 3170.01M Enclosures B and H. Enclosure H will be superseded automatically upon the termination of ORDs on 24 December 2003.

(4) All JCIDS documents submitted for review and interoperability certification will be submitted into the J-8 Knowledge Management/Decision Support (KM/DS) tool. Users should contact the J-8 at 703-695-7065 for details.

(5) All ISPs for all ACAT programs will be submitted into the OSD Joint C4I Program Assessment Tool (JCPAT) tool for review on the SIPRNET at <https://206.36.228.76>.

e. Unless declared unsuitable for information sharing due to national security considerations, for purposes of interoperability and supportability, all IT and NSS developed for use by US forces are for joint, combined, and coalition use. The term “joint force” throughout this document refers to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander (JP 1-02 and references e and g). Interoperability and supportability of IT and NSS requirements for ACAT programs will be determined during the JCIDS validation process (references a through e and g) and this instruction and will be updated as necessary throughout the acquisition period, deployment and operational life of a system. Interoperability and supportability of IT and NSS requirements for non-ACAT and fielded programs will be determined by the requirements authority IAW references c, d, e and g and this instruction and will be updated as necessary throughout the acquisition period, deployment, and operational life of a system.

7. Implementation and Supplementation. Upon implementation of this instruction, the interoperability and supportability certification process for all IT and NSS (classified SECRET and below) will use the J-8 Knowledge Management/Decision Support (KM/DS) tool for JCIDS document staffing and the Joint C4I Program Assessment Tool (JCPAT) for Information Support Plan staffing. Documents established in staffing at the time of implementation of this instruction will convert to KM/DS at the next key-staffing milestone. The Web site for KM/DS is <https://siprweb1.js.smil.mil/pls/jrcz>. JCPAT is the integrated tool used by J-6 and DISA for managing the interoperability and supportability certification, testing, and validation process end-to-end and involves system and/or program registration, standards development, capability interconnectivity, and interoperability analysis, testing, certification, and validation. This instruction will not be supplemented without the prior approval of the Vice Chairman of the Joint Chiefs of Staff or his delegated representative.

8. Waivers. Submit waivers or requests for exceptions to the provisions of this instruction to the Joint Staff. Statutory requirements shall only be waived if the statute specifically provides for doing so. All JCIDS documents and ISPs submitted 6 months after publication of this instruction shall contain the NR-KPP defined in this instruction. Legacy Requirements Generation System (RGS) documents and CRDs will continue to contain the legacy I KPP. When the NR-KPP requirement is waived, an alternate J-6 approved source of interoperability requirements information will be specified by J-6.

9. Summary of Changes

a. This revision reflects a complete rewrite of the document to reflect changes in the overall acquisition and new capability based methodology. The revision also reflects a new NR-KPP and other changes that support an integrated view of architectures.

b. This revision reflects recent changes from the DOD 5000-series, DODD 4630.5, DODI 4630.8, and CJCSI 3170 (references a, c, d, e and g).

10. Reliability. This instruction is approved for public release and 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/doctrine/>. Copies are also available through the Government Printing Office on the Electronic Library CD-ROM.

11. Definitions. See Glossary.
12. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

Approved & Secured with


T. J. KEATING
VADM, USN
DIRECTOR, JOINT STAFF

Enclosures:

- A--Process Overview
- B--Responsibilities
- C--Procedures
- D--Capstone Requirements Document (CRD)
- E--Initial Capabilities Document (ICD)
- F--Net-Ready Key Performance Parameter for the Capability Development Document (CDD)
- G--Net-Ready Key Performance Parameter for the Capability Production Document (CPD)
- H--Requirements Generation System Documents
- I--Information Support Plan (ISP)
- J--Joint C4I Program Assessment Tool – Empowered (JCPAT-E)
- K--Interconnectivity and Interoperability Capability (IIC) Profile
- L--IT Standards Profile
- M--Joint Interoperability Testing and Test Certification Process
- N--IT and NSS System Specific Policies
- O--References
- GL--Glossary

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for. 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	H-A-1 thru H-A-6	O
i thru viii	O	I-1 thru I- 18	O
A-1 thru A-22	O	I-A-1 thru I-A-6	O
B-1 thru B-14	O	J-1 thru J-8	O
C-1 thru C-8	O	K-1 thru K-2	O
D-1 thru D-10	O	L-1 thru L-6	O
E-1 thru E-12	O	M-1 thru M-8	O
F-1 thru F-16	O	N-1 thru N-2	O
G-1 thru G- 16	O	O-1 thru O-4	O
H-1 thru H- 4	O	GL-1 thru GL-14	O

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	Page
ENCLOSURE A Process Overview	A-1
ENCLOSURE B Responsibilities	B-1
ENCLOSURE C Procedures	C-1
ENCLOSURE D Capstone Requirements Document (CRD).....	D-1
ENCLOSURE E Initial Capabilities Document (ICD).....	E-1
ENCLOSURE F Net-Ready Key Performance Parameter For The Capability Development Document (CDD)	F-1
ENCLOSURE G Net-Ready Key Performance Parameter For The Capability Production Document (CPD)	G-1
ENCLOSURE H Requirements Generation System (RGS)	H-1
ENCLOSURE I Information Support Plan (ISP)	I-1
ENCLOSURE J Joint C4i Program Assessment Tool – Empowered (JCPAT-E)	J-1
ENCLOSURE.K Interconnectivity And Interoperability Capability (IIC) Profile	K-1
ENCLOSURE L IT Standards Profile	L-1
ENCLOSURE M Joint Interoperability Testing And Test Certification Process	M-1
ENCLOSURE N IT And NSS Specific Policies.....	N-1
ENCLOSURE O References.....	O-1
ENCLOSURE GL Glossary.....	GL-1
Part I - Abbreviations and Acronyms	GL-1
Part II - Definitions.....	GL-6

(INTENTIONALLY BLANK)

ENCLOSURE A

PROCESS OVERVIEW

1. This enclosure provides an overview of the J-6 Interoperability and Supportability Certification and Interoperability Certification Testing Process. Detailed procedures are provided in Enclosure C.

2. Failure to meet Certifications

a. If a program/system fails to meet certification requirements, the J-6 will:

(1) Not validate the program.

(2) Recommend the program not proceed to the next milestone.

(3) Recommend that funding be withheld until compliance is achieved and the program and/or system is validated.

b. The J-6 will make this recommendation to the USD(AT&L), USDP, USD(C), ASD(NII), DOD Executive Agent for Space, the Military Communications-Electronics Board (MCEB), and the JROC. The J-6 will also request that the program and/or system be added to the DODI 4630.8, Interoperability Watch List (IWL).

3. Net-Ready Key Performance Parameter (NR-KPP)

a. The focus of the new interoperability and supportability certification process is the NR-KPP, which replaced the previous I KPP.

b. The NR-KPP assesses net-readiness; information assurance requirements; and both the technical exchange of information and the end-to-end operational effectiveness of that exchange. 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, documented in CRDs, Capabilities Development Document (CDD)s and Capabilities Production Document (CPD)s, shall be used in analyzing, identifying and describing IT and NSS interoperability, and test strategies in the Test and Evaluation Master Plan (TEMP).

c. The NR-KPP consists of the following elements:

(1) Information Assurance. Demonstrate achievement of Information Assurance within the GIG through a defense-in-depth approach that integrates the capabilities of personnel, operations and technology, and supports the evolution to network centric operations and warfare. Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DOD IT and NSS systems in accordance with 10 USC Section 2242, OMB Circular A-130 Appendix III, and references r through w; as well as references z, aa and bb for SCI and Special Access Programs. Interoperability and integration of IA solutions within or supporting the DOD shall be achieved through adherence to an architecture that will enable evolution to network centric operations and warfare by remaining consistent with the DOD Architecture Framework, and defense-in-depth approach.

(2) Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW RM). The NCOW RM, depicted in Figure A-1, describes the activities required to establish, use, operate and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest (COI) services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the GIG are realized. The NCOW RM represents the objective end-state for the GIG. (See reference n for details.) This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of military operations; DOD business operations; and Department-wide enterprise management operations.

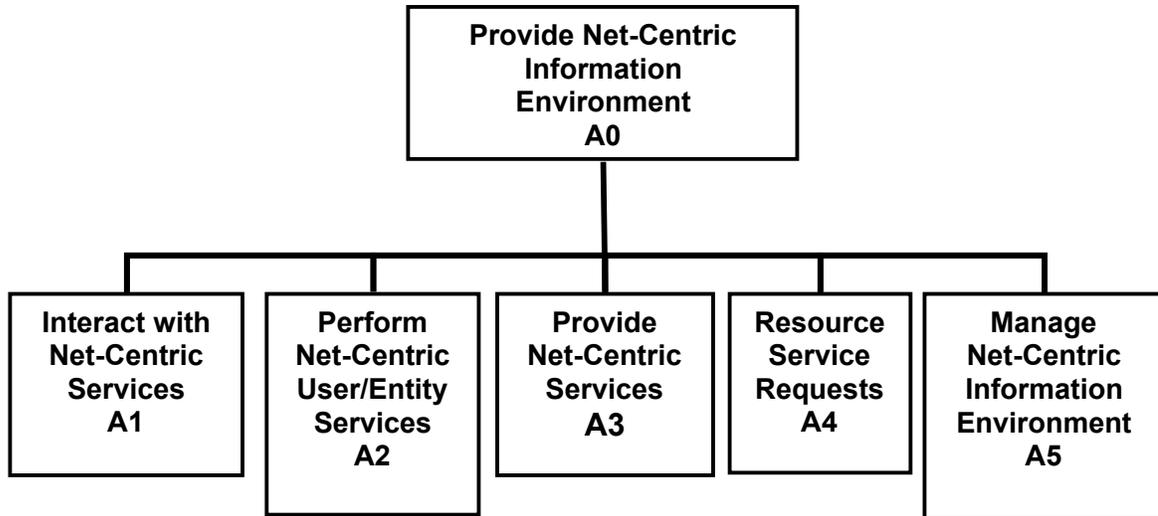


Figure A-1. Net Centric Operations Warfare Reference Model (NCOW RM)

(a) The NCOW RM serves as a common, enterprise-level, reference model for the DOD's Enterprise Architecture and for current and future acquisition programs to use in focusing and gaining net-centric support through the GIG. The NCOW RM enables a shared perspective of the enterprise information environment operations and is used to assist decision-makers in arriving at decisions that promote enterprise-wide unity of effort. The goal is to perform program development and oversight with a uniform Department-wide reference to which all net-centric IT-related issues can be addressed within individual programs and across the set of enterprise programs in a constructively consistent, coherent, and comprehensive manner. The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities core services, community of interest (COI) services, and environment control services, and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the GIG become realized.

(b) The NCOW RM represents the target viewpoint of the DOD GIG. This viewpoint is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of (1) military operations, (2)

DOD business operations, and (3) Department-wide enterprise management operations. Enterprise management operations extend from internally focused operations to externally focused operations in which the DOD is one component of the total US government enterprise. The NCOW RM will ultimately provide a common architectural construct for NCOW with a common language and taxonomy. The final version of the RM will include:

1. All Views (AV): AV-1 and AV-2
2. Operational Views (OV): OV-1, OV-2, OV-3, and OV-5
3. System Views (SV): SV-1, SV-2, SV-3, SV-4, and SV-5
4. Target Technical View

(c) The current version, NCOW RM v0.9, consists of the following architectural view products:

1. All Views: AV-1, AV-2
2. Operational Views: OV-1, OV-5
3. Target Technical View

(1) Compliance with applicable GIG Key Interface Profiles (KIPs). GIG KIPs provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. (See reference n for details.)

(a) A KIP is the set of documentation produced as a result of interface analysis which:

1. Designates an interface as key.
2. Analyzes it to understand its architectural, interoperability, test requirements, configuration management and security requirements.
3. Documents those characteristics in conjunction with solution sets for issues identified during the analysis.

(b) The profile consists of:

1. Refined operational and systems view products.

2. Interface Control Document/Specifications.
3. Engineering Management Plan.
4. Configuration Management Plan.
5. Technical Standards View (TV-1) with SV-TV Bridge.
6. Procedures for standards conformance and interoperability testing.

(a) DOD identified 17 key interfaces in reference cc for development and management at the enterprise level. DISA developed the GIG teleport KIP in November 2002.

(b) Relevant GIG KIPs, for a given capability, shall be documented in the CDD and CPD. Compliance with identified GIG KIPs shall be analyzed during the development of the ISP and TEMP, and assessed during DISA (JITC) joint interoperability certification testing. Since all of the GIG KIPs have not been developed, the following applies:

(c) The Chairman of the Joint Chiefs of Staff and DISA shall continue the development of the GIG KIPs.

(d) The Chairman of the Joint Chiefs of Staff shall continue the well-defined, phased implementation of the GIG KIPs, to be completed by FY 2006.

(e) DISA shall maintain completed GIG KIPs in the DOD DISR), an online database registry for standards and profiles.

(2) Supporting Integrated Architecture Products. The following integrated architecture products described in reference e shall, as a minimum, be incorporated in the NR-KPP and used to assess information exchange and use for a given capability:

Framework Products	Framework Product Name	General Description
AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
OV-2	Operational Node Connectivity Description	Operational Nodes, operational activities performed at each node, connectivity and information exchange need lines between nodes
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
OV-5	Operational Activity Model	Operational activities, relationships among activities, inputs and outputs. Overlays can show cost performing nodes, or other pertinent information.
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity sequence and timing – traces actions in a scenario or sequence of events and specifies

		timing of events.
SV-4	Systems Functionality Description	Functions performed by systems and the information flow among system functions, including information assurance functions
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to operational capabilities or of system functions back to operational activities.
SV-6	Systems Data Exchange Matrix	Provides details of systems data being exchanged between systems.
TV-1	Technical Standards Profile	Extraction of standards that apply to the given architecture, including information assurance functions.

Table A-1. Principal Integrated Architecture Products.

a. The NR-KPP for each type of document (CRD, CDD, CPD and ISP) is defined in the applicable enclosure in this document. Table A-2 provides a matrix of the JCIDS documents and the NR-KPP architecture products. As indicated above, at a minimum, the NR-KPP is comprised of:

- (1) Supporting Architecture products.
- (2) Compliance with the NCOW reference model.
- (3) Compliance with the KIP.
- (4) Information Assurance policies and procedures.

Document	Net-Ready Key Performance Parameter Products													NCOW RM	KIP Compliance	IA Compliance	LISI Profile		
	Supporting Architecture Products																		
	AV-1	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	SV-1	SV-2	SV-3	SV-4	SV-5	SV-6					TV-1	
ICD		X													X				
CDD	X		X		X	X	X				X	X	X	X	X	X	X	X	X Basic
CPD	X		X		X	X	X				X	X	X	X	X	X	X	X	X Complete
CRD		X		1		2									2	2	2		
ISP	3	3	3		3	3	3	3			3	3	3	3	3	3	3	3	3 Complete

Note: X = Required

(1) Old CRDs Updates

(2) New CRDs

(3) ACAT, NON ACAT and Fielded Systems. NR-KPP products produced for the CDD and CPD will be used in the ISP.

Table A-2. JCIDS Documents/NR-KPP Products Matrix.

b. All elements of the NR-KPP will be able to be measured, tested or evaluated.

4. Migration to the Net-Ready Key Performance Parameter. Just as was done with CJCSI 3170 regarding top down architectures, it is recognized that all the KIPs are not available, but the process must be put in motion for future system development.

a. Figure A-2 below depicts the migration timeline to the NR – KPP.

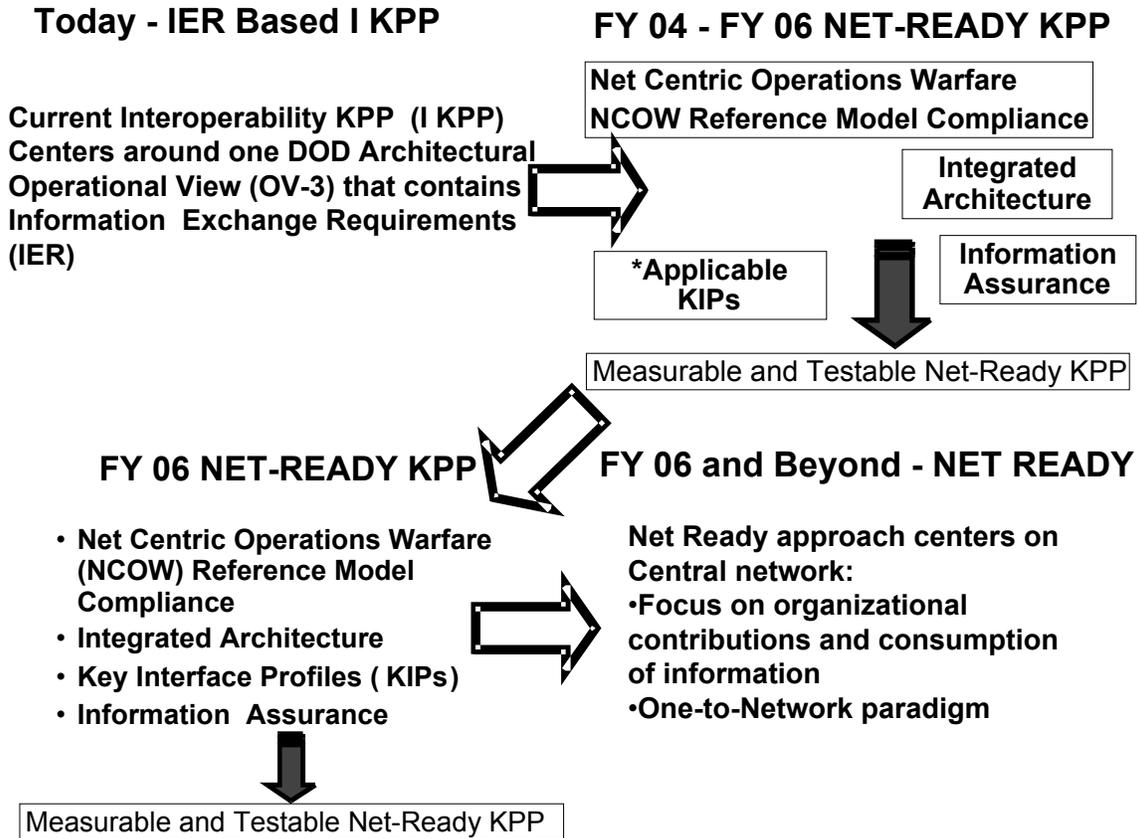


Figure A-2. Migration to the Net-Ready KPP

b. FY 04 to FY 06. Program managers will comply with three parts of the Net-Ready Key Performance Parameter:

(1) Architectures products. See Table A-2. Program Managers (PM) producing the Architectures Products, using the NCOW RM, should develop high-level interface information for becoming net ready and plan to be Key Interface compliant to the applicable KIPs as they become available.

(2) Net-Centric Operations Warfare Reference Model. NCOW RM provides the PM with a common lexicon for NCOW concepts and

terminology, supported by recognizable architectural descriptions. It describes net-centricity at the enterprise level for DOD Program Managers and other decision makers. It includes Overview And Summary Information (AV-1), Integrated Dictionary (AV-2), High-Level Operational Concept Graphic (OV-1), Activity Model (OV-5), and Target Technical View (TV-1).

(3) Information assurance. IAW DOD Directive 5000.1 (reference d, PMs shall verify compliance with the security requirements and evaluate vulnerabilities, for each lifecycle development activity where there is a corresponding set of security activities. PMs must provide J-6 documentation that each phase of the Defense Information Technology Security Certification and Accreditation Program (DITSCAP) process (Definition, Verification, and Validation) has been completed throughout the stages of the JCIDS/acquisition process.

(4) As key interfaces which have been profiled and made available through the DISR, PMs will comply with these KIPs, which will be published as an annex in DISR. KIP's will be distributed as an advisory as soon as they have been defined, and will be formally published on a priority basis. PM's are required to incorporate published KIP's in all new start or significantly modified systems acquisitions and/or pre-Milestone B designs immediately. For ongoing acquisitions beyond Milestone B and/or established systems, published KIPs will be included as objective capabilities immediately, and as threshold requirements within 12 months of publication through the systems evolutionary spiral block upgrade process.

c. FY 06 and beyond. PMs will be expected to comply with all parts of the NR-KPP.

5. This instruction must account for three categories of programs requiring certification: ACAT programs which enter into the JCIDS process (references a and b), Non-ACAT programs, and fielded systems. The following paragraphs provide an overview of the processes for conducting interoperability and supportability certification and testing certification for these three categories.

a. ACAT Programs. This paragraph provides policy for interoperability and supportability certification and for Joint System Interoperability Test Certification of ACAT programs.

(1) Interoperability and Supportability Certification and Validation Process for ACAT Programs. Figure A-1 depicts the interoperability and supportability certification process for ACAT

programs. This diagram illustrates three interoperability and two supportability certifications of capabilities and one validation of the completed systems tests against required capabilities and architectures discussed in the following paragraphs. The J-6 will certify capabilities interoperability and supportability for all IT and NSS for all ACAT.

(a) The J-6 interoperability and supportability certification and testing validation process is intended to manage, evaluate, and report IT and NSS interoperability and supportability over the life of the system.

(b) The J-6 will validate that the following have been accomplished: capabilities interoperability and supportability certification; JITC Joint System Interoperability Test Certification; and NR-KPP: NCOV Reference Model compliance, integrated architecture products compliance, KIPs compliance; and information assurance accreditation.

(2) The interoperability and supportability certification process for all IT and NSS (classified SECRET and below) will use the J-8 KM/DS tool for JCIDS document staffing and the JCPAT for ISP staffing. JCPAT is the integrated tool used by J-6 and DISA for managing the interoperability and supportability certification, testing, and validation process end-to-end and involves system and/or program registration, standards development, capability interconnectivity, and interoperability analysis, testing, certification, and validation. Figure A-3 depicts the interoperability and supportability certification, testing and validation process for ACAT programs.

(a) Developmental (CDD) interoperability requirements and supportability certification occurs prior to acquisition Milestone B. For space systems being acquired under reference dd, the CDD is required prior to PDR.

(b) Production (CPD) interoperability requirements certification and supportability certification occurs prior to acquisition Milestone C.

(c) PMs will submit JCIDS documents for interoperability certification into the J-8 KM/DS tool. PMs will submit ISPs for all ACAT, Non-ACAT and fielded systems for supportability certification into the OSD JCPAT tool for review. The ISP is submitted prior to key decision point (KDP-B) and update is submitted prior to KDP-C for space systems acquired under reference dd.

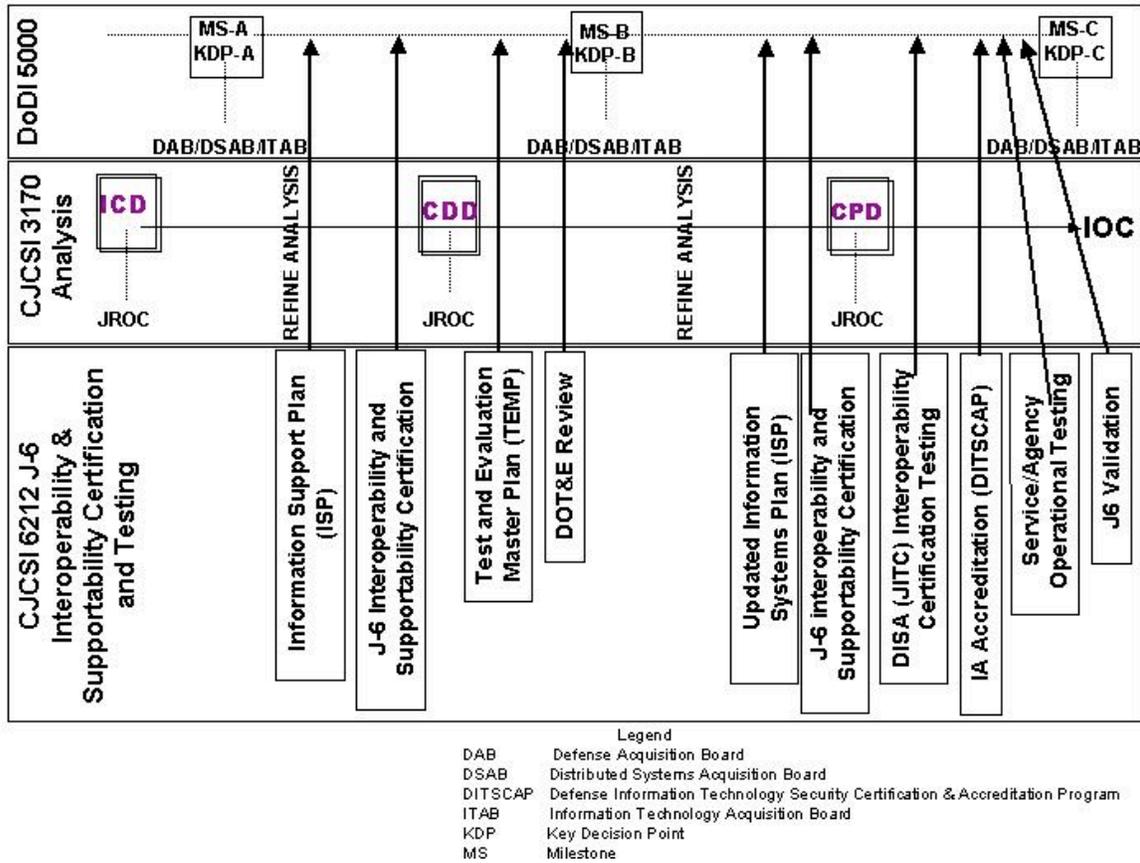


Figure A-3. J-6 Interoperability and Supportability Certification, Testing, and Validation Process for ACAT Programs

(d) During the review process, J-8 staffs JCIDS documents on KM/DS to OSD, combatant commands, Services, the Joint Staff and DOD agencies.

(e) ASD(NII) staffs ACAT I and OSD Special Interest ISPs and J-6 staffs all other ACAT ISPs on JCPAT to OSD, combatant commands, Services and DOD agencies.

(f) Only the J-6 will certify interoperability and supportability requirements for JCIDS documents and ISPs for all ACAT, to ensure conformance with policy, doctrine, and applicable interoperability and supportability standards for joint IT and NSS. J-6 reviews all interoperability and supportability related comments submitted into KM/DS and JCPAT as part of the certification process. All interoperability comments submitted to the KM/DS tool will be identified in the KM/DS Comment Matrix by inserting "Interoperability Comment"

as the first entry in the COMMENT column. Only comments so marked will be considered as part of the interoperability certification process.

(g) Combatant commanders are asked to review and provide comments on all ACAT programs during the interoperability and supportability certification process.

(h) US Joint Forces Command (USJFCOM), as the joint force integrator, will review and confirm sufficiency of NR-KPPs and integrated architectures for JCIDS documents regardless of ACAT. USJFCOM, as the Chairman's advocate for interoperability, may require selected programs and systems for interoperability demonstrations, using the Joint C4ISR battle center's (JBC) interoperability technology demonstration center (ITDC). Selection of the program or system may be made by the joint battle management command and control board of directors. These interoperability demonstrations do not replace the JITC system interoperability test certification. Demonstration results could be used or provided to JITC to assess the system for interoperability test certification.

(i) After completing the two-stage document review, sponsors will submit the adjudicated comment resolution matrix and updated ORD/ICD/CDD/CPD to J-8 KM/DS tool (for JCIDS documents) or adjudicated comments resolution matrix and updated ISP to JCPAT (for ISPs). Sponsors will upload these documents into KM/DS or JCPAT (respectively) and contact J-6 to request interoperability and/or supportability certification for all JCIDS and/or ISP documents not originally granted certification after the flag level and/or certification review.

(j) The J-6 will provide interoperability and supportability requirements certification for JCIDS documents (CRD, CDD, and CPD), regardless of ACAT level, designated as JROC Interest, Joint Impact, and Joint Integration. The J-6 will provide supportability certification for ISPs for all ACAT regardless of ACAT level. All inter- and intra-DOD component IT and NSS that exchange and use information to enable units or forces to operate effectively in joint, combined, and interagency operations shall be certified for interoperability and supportability. Programs categorized as independent (e.g., systems or capabilities that do not exchange or use external information) are returned to the submitter and do not require certification.

(k) In accordance with reference g, the PM for all ACAT programs will submit an ISP into the DOD JCPAT tool for review prior to Milestone B (Program initiation for ships) and an updated ISP prior to

Milestone C in accordance with DOD 5000.2-R or Acquisition Deskbook (as appropriate) guidance. The ISP shall describe system dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability requirements. The ISP shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of performance, and interoperability issues. Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD(NII)/DOD CIO) will coordinate the review of ACAT I and Special Interest ISPs. The J-6 will coordinate the review of ACAT II and below (non-Special Interest) ISPs.

(l) The J-6 provides supportability certification to ASD(NII)/DOD CIO and posts this certification onto JCPAT and KM/DS for all CPDs including all ACAT programs, regardless of ACAT level. This certification ensures that IT and NSS infrastructure requirements, the availability of bandwidth and spectrum support, and identify dependencies and interface requirements between systems are adequately addressed. This is done prior to Milestone C.

(m) In support of a Milestone C decision, J-6 will provide validation of status of interoperability and supportability requirements certification (JITC Joint System Interoperability Test Certification), adherence to the NCOW Reference Model, information assurance accreditation, and achievement of the NR-KPP, to the Milestone Decision Authority (MDA).

(n) In support of the J-6 JCIDS document certification, DISA JITC will review and confirm the measurability and testability of all NR-KPPs.

(3) IT and NSS Joint System Interoperability Test Certification for ACAT Programs.

(a) All ACAT IT and NSS must be evaluated and certified for Joint interoperability by DISA (JITC). When JITC is not the responsible testing organization, the system proponent will coordinate test plans, analysis, and reports with JITC to ensure sufficient information is available to support a certification determination. IT and NSS interoperability testing and evaluation shall be conducted as early as is practical to support scheduled acquisition or procurement decisions during the development phases and throughout a system's life. Testing may be performed in conjunction with other testing (i.e., Developmental Test & Evaluation (DT&E), Operational Test and Evaluation (OT&E), or

early user test) whenever possible to conserve resources. Enclosure M describes the Joint System Interoperability Test Certification process.

(b) All IT and NSS must have a J-6 certified NR-KPP prior to DISA (JITC) Joint System Interoperability Test Certification (see reference g). J-6 may waive the requirement for an NR-KPP on a case-by-case basis. (When waived, the source of interoperability requirements needs to be satisfied.)

(c) The table below provides the NR-KPP Threshold and Objective:

Net-Ready KPP	Threshold (T)	Objective (O)
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture**.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements in the Joint integrated architecture.

Table A-3. NR-KPP Threshold and Objective

* Data processing is defined as: the input, output, verification, organization, storage, retrieval, transformation and extraction of information from data.

** Joint integrated architecture: An integrated architecture that establishes the basis for rapidly acquiring affordable and evolving joint warfighting capabilities through collaborative planning, analysis, assessment and decision making.

(d) The MDAs and component acquisition executives (CAEs) must address IT and NSS interoperability evaluation and certification by DISA (JITC) as an integral part of the acquisition process prior to production and fielding approval of each increment.

(e) DISA (JITC) Joint System Interoperability Test Certification evaluation will include standards conformance evaluation and certification, where applicable. DISA (JITC), in conjunction with the PMs, will plan and conduct standards conformance evaluation, including compliance with applicable Key Interface Profiles (KIPs), during the development and acquisition procurement processes. DISA (JITC) will provide input to the DT and Operational Test Readiness Review (OTRR) processes on whether a system is ready for testing, from an interoperability perspective.

(f) DISA (JITC) Joint Interoperability re-Certification is required as follows:

1. When materiel changes (e.g., hardware, firmware, software modifications) affect interoperability.
2. Upon revocation of interoperability certifications or J-6 system validation.
3. Upon automatic expiration 3 years after the date of the certification.
4. When non-materiel changes (i.e., Doctrine, Operations, Training, Logistics, Personnel, or Facilities) occur that may affect interoperability.

(g) IT and NSS with significant interoperability may be placed on the Interoperability Watch List (IWL) to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

b. Non-ACAT Programs. This paragraph provides policy for Interoperability and Supportability Certification and for DISA (JITC) Joint System Interoperability Test Certification of non-ACAT programs.

(1) This process applies to IT and NSS under consideration for operational use, but being acquired or procured outside of the ACAT program processes described in DOD 5000 Series (reference d). Included in this category are all defense technology projects and pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations

(ACTDs), Joint Testing and Evaluations (JT&Es), and Joint Warrior Interoperability Demonstrations (JWIDs) that lead to acquisitions), the Combatant Commander Command and Control Initiative Program, Combatant Commander Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, Tactical Exploitation of National Capabilities Programs, DODIIS, post-acquisition (fielded) IT and NSS systems, and modifications to fielded IT and NSS capabilities.

(2) If the acquisition or procurement of non-ACAT IT or NSS or services transitions to an acquisition program, then it shall be managed and fielded per the DOD 5000 series guidance.

(3) Interoperability and Supportability Certification and Validation Process for Non-ACAT Programs

(a) Figure A-4 depicts the interoperability and supportability certification process and its linkage to the JCIDS process for Non-ACAT programs.

1. This diagram illustrates the Joint Staff interoperability and supportability review and certification of the ISP, JITC Joint Interoperability Test Certification, Information Assurance accreditation and a J-6 validation of the NR-KPP requirements for Non-ACAT programs (Certified ISP, IA Accreditation, and JITC Interoperability Certification).

2. The J-6 will certify interoperability and supportability capabilities for all Non-ACAT IT and NSS. The J-6 interoperability and certification and testing process is intended to manage, evaluate, and report IT and NSS interoperability and supportability over the life of the system.

3. The J-6 will validate that the following have been accomplished:

a. Interoperability and supportability requirements certification.

b. JITC Joint System Interoperability Test Certification. In support of the J-6 JCIDS documentation certification, DISA JITC will review and confirm the measurability and testability of all NR-KPPs.

c. Information assurance accreditation.

4. This interoperability and supportability certification process for all IT and NSS will use the Joint C4I Program Assessment Tool (JCPAT) and involves system/program registration, standards development, capability interconnectivity, and interoperability analysis and certification. Information assurance accreditation guidance is provided in reference u.

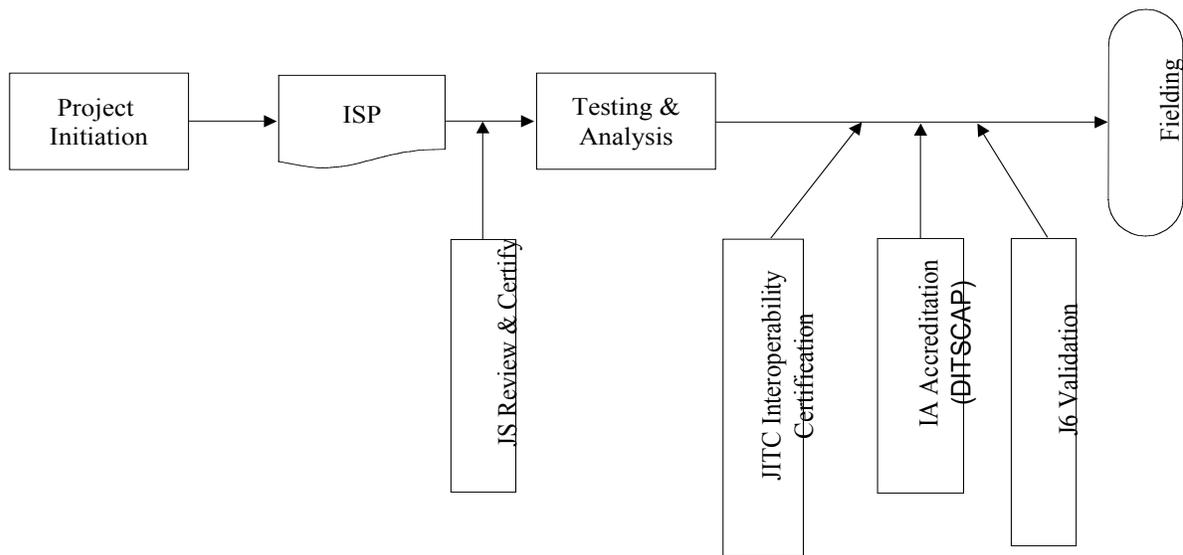


Figure A-4. Non-ACAT Interoperability and Supportability Certification Process

(b) Information Support Plan (ISP). In accordance with reference g, an ISP shall be developed for all non-ACAT acquisitions and procurements to document IT and NSS needs, dependencies, interface requirements and the NR-KPP. The plan shall describe system dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability requirements. The ISP shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of performance, and interoperability issues. The scope of the ISP shall be scaled to the relative size and funding profile for the program. The sponsoring or cognizant authority shall review, assess, and approve the ISP for non-ACAT acquisitions and procurements, and

forward any critical interoperability or supportability issues to the ASD (NII)/DOD CIO.

(c) IT and NSS Joint Interoperability Certification Evaluation for Non-ACAT Programs. All non-ACAT acquisitions and procurements shall be tested and evaluated for required interoperability.

1. The fielding authority must address IT and NSS interoperability evaluation and certification during the system interoperability test certification by DISA (JITC) as an integral part of the requirements validation and acquisition process prior to procurement, production or fielding approval of each increment.

2. IT and NSS interoperability testing shall be scaled, as necessary, based on the relative size and funding profile, criticality, and other risk factors for the program and may be performed in conjunction with other tests, exercises or demonstrations (e.g., component interoperability testing) to conserve resources.

3. DISA (JITC) will conduct an interoperability evaluation, based on JITC system interoperability testing of the NR-KPP or other submitted test results, and provide a system interoperability test certification.

4. Other than the source of interoperability requirements, the operational interoperability evaluation and certification process remains the same as for ACAT systems. (Enclosure M describes the Joint System Interoperability Test Certification and evaluation process.)

5. The sponsoring or cognizant authority shall review and consider IT and NSS interoperability test results prior to operational use or fielding decision. IT and NSS with significant interoperability deficiencies (as determined by the offices of the USD(AT&L), DPA&E, the ASD(NII)/DOD CIO, the DOT&E, DOD Executive Agent for Space, and the Chairman of the Joint Chiefs of Staff, and USJFCOM) may be placed on the IWL to ensure that sufficient attention is given toward achieving and maintaining interoperability objectives.

6. All IT and NSS must have a J-6 certified NR-KPP prior to DISA (JITC) Joint Interoperability System Certification.

c. Fielded Systems. This paragraph provides policy for interoperability and supportability certification and for certification testing of fielded systems.

(1) Interoperability and Supportability Certification and Validation Process for Fielded Systems. The sponsoring authority will verify that all proposed materiel and non-materiel remedies for fielded IT and NSS capabilities meet interoperability and supportability requirements. IT and NSS interoperability verification may be performed in conjunction with other activities such as joint tests and evaluations, operational tests and exercises, demonstrations or component interoperability testing to conserve resources.

(a) A CPD/ISP must be submitted for fielded systems in order to receive an interoperability/supportability review and certification.

(b) Systems that cannot provide the required documentation must obtain an Interim Certificate to Operate (ICTO), issued by the MCEB interoperability test panel (good for up to 1 year), in order to continue to operate until they provide the documentation.

(2) Figure A-5 depicts the interoperability process for addressing operational warfighting interoperability and supportability issues for fielded IT and NSS.

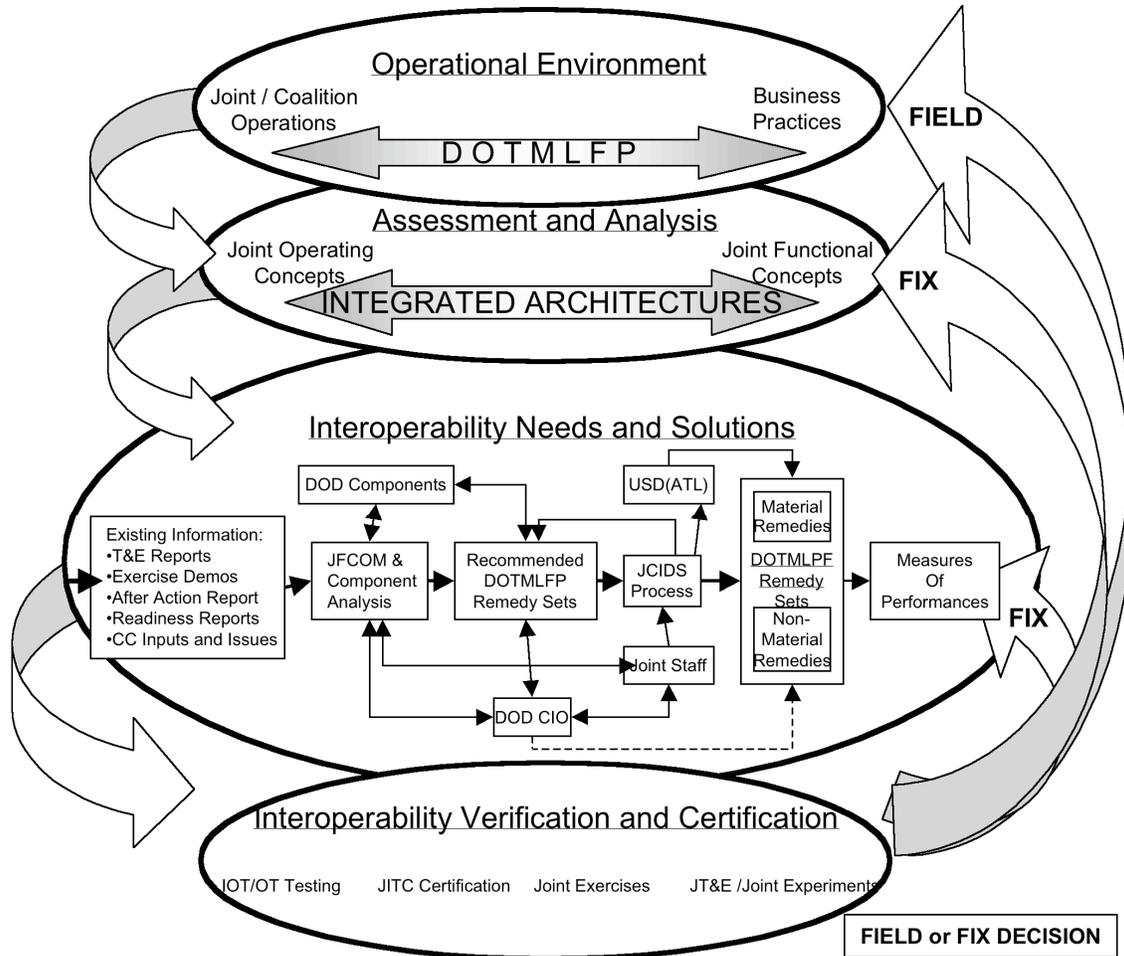


Figure A-5. Fielded (Legacy Systems) IT and NSS Interoperability Process

(3) IT and NSS Joint System Interoperability Test Certification for Fielded Systems. Other than the source of interoperability requirements,

the operational interoperability evaluation and certification process remains the same as for ACAT systems. (See Enclosure M for a description of the Joint Interoperability Certification test and evaluation process.)

(a) DISA (JITC) will conduct an interoperability evaluation, based on JITC system interoperability testing of the NR-KPP or other submitted test results, and provide a system interoperability test certification.

(b) The sponsoring authority for the materiel or non-materiel remedy shall review and consider IT and NSS interoperability test results prior to operational use or a fielding decision.

(c) IT and NSS with significant interoperability deficiencies (as determined by the offices of the USD(AT&L), the ASD(NII)/DOD CIO, the DOT&E, DPA&E, DOD Executive Agent for Space, the Chairman of the Joint Chiefs of Staff and the USJFCOM) may be placed on the IWL to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

(d) All IT and NSS must have a J-6 certified NR-KPP prior to DISA (JITC) Joint Interoperability System Certification.

6. Interoperability Test Panel

a. The MCEB Interoperability Test Panel (ITP) resolves issues in joint testing and interoperability certification.

b. The ITP in special situations may, on a case-by-case basis, grant a temporary certification from interoperability system testing certification in the form of an Interim Certificate to Operate (ICTO).

c. Submit requests for an ICTO to the ITP IAW reference h (or see the DISA (JITC)/ITP Web site: <http://jitc.fhu.disa.mil>).

d. ICTOs will not exceed 1 year.

7. Joint System Interoperability Test Certification Programming and Budgeting

a. Combatant commands, Services and agencies are responsible for funding interoperability testing for systems. This responsibility includes funding, scheduling, and coordination to ensure that external interfacing systems are available during interoperability testing. Required

interoperability testing and certification will normally impact schedule and program cost and will need to be added to POM and program cost estimates.

b. Combatant commands/Services/agencies (C/S/A) may designate and fund another C/S/A test organization to conduct interoperability testing.

(1) When DISA (JITC) is not the interoperability testing organization, interoperability test plans, test analysis, and test reports will be coordinated with DISA (JITC) to ensure sufficient information is available to allow DISA (JITC) to certify a system.

(2) DISA (JITC) schedules tests and certifications, balancing between the program manager's schedule, DISA (JITC)'s available test resources, organizational priorities, and functional priorities. Enclosure M provides more information.

7. Joint System Interoperability Testing and Certification Prioritization. Combatant commands/Services/agencies and participating test unit coordinator (PTUC) will incorporate interoperability testing into its overall testing plans in coordination with DISA (JITC).

a. DISA (JITC) uses the following organizational prioritization for testing, assessing and certifying interoperability:

(1) Joint IT and NSS systems that support the unified commands.

(2) Joint IT and NSS systems that are acquired by the Services.

(3) Systems that are acquired by the Defense agencies.

b. The order for functional prioritization is:

(1) Strategic warning and communication systems that support the unified commands, the Secretary of Defense and the Commander-in-Chief;

(2) Tactical systems that support the unified commands;

(3) C2 systems that support the unified commands;

(4) Combat service support systems that support the unified commands.

c. Interoperability testing and certification schedule conflicts will be submitted to the ITP for resolution. Issues that cannot be resolved by the ITP process will be submitted to the MCEB for resolution.

d. The prioritization process is not intended to impede, delay, or restrict milestone accomplishment. Should delays occur due to a lack of testing resources, the PM should submit an ICTO request to the ITP.

8. Information Technology Standards. New or modified IT and NSS systems should be capabilities-based. IT and NSS must comply with applicable information technology standards contained in the current DISR, and the latest versions of the OASD(NII) Net Centric Operations and Warfare Reference Model (NCOW RM) and the GIG Architecture. Compact Disc (CD) copies of the GIG Architecture and NCOW RM are available through ASD(NII)/DOD CIO until its Web site is established. Additionally, IT and NSS systems must comply with current Information Assurance policies and procedures.

9. IT and NSS System-specific Policies. Current and newly established interoperability related policies that impact J-6 certifications are listed in Enclosure N.

ENCLOSURE B

RESPONSIBILITIES

1. The Joint Staff, J-6, will:

- a. Conduct a capability interoperability certification of CDDs, CPDs and ISPs and other capabilities documents designated by the JROC, regardless of ACAT level.
- b. Conduct a J-6 Functional Capability Board (FCB) Working Group assessment of all ICDs through the C2 FCB.
- c. Conduct a J-6 FCB Working Group assessment of all Doctrine, Organization, Training, Material, Leadership, Personnel and Facility (DOTMLPF) Change Documents through the C2 FCB and other applicable FCBs.
- d. Conduct supportability certification of IT and NSS for all ACAT.
- e. Conduct interoperability system test validation of all IT and NSS for all ACAT, including Joint Interoperability System Certification, NCOW RM and KIP compliance and IA certification.
- f. Coordinate IT and NSS interoperability and supportability policies, procedures and programs.
- g. Monitor C2 R&D and acquisition of IT and NSS in collaboration with USD(AT&L), ASD(NII), and J-8 through the C2 FCB and other applicable FCBs.
- h. Convene the MCEB consisting of the senior Service and agency officials responsible for communications-electronics matters and act as chairman (references h and v). The MCEB will consider interoperability and supportability matters referred to it by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. The board will:
 - (1) Act as the senior resolution body for issues related to IT and NSS, standards, interoperability testing and NR-KPP issues. All interoperability issues not resolved by these instructions and the MCEB may be referred to the Interoperability Senior Review Panel (ISRP) for final resolution.

(2) Obtain coordination for issues presented to the board among DOD components, between the Department of Defense and other governmental departments and agencies, and between the Department of Defense and representatives of foreign nations.

(3) Coordinate and furnish advice, guidance, direction, and assistance among components for IT and NSS interoperability and supportability matters.

(4) Establish the following sub-panels whose duties in regards to this instruction are as defined:

(a) The ITP will oversee conduct of the interoperability certification testing process, resolve testing issues, and waive requirements for Joint Interoperability Certification IAW MCEB Pub 1.

(b) The Information Assurance Panel (IAP) will resolve information assurance (IA) interoperability issues.

(c) The Interoperability Panel (IP) of the MCEB will resolve issues directly related to or involving IT and NSS systems interoperability, and operational and procedural standards.

i. Designate a POC to act as executive agent of the J-6 Assessment Tool (see Enclosure J).

j. Ensure that USD(AT&L), ASD(NII), and other DOD components have the opportunity to participate in or review the analysis conducted early to ensure that processes adequately address a sufficient range of interoperability issues and material approaches.

2. Joint Staff, J-2, will:

a. Designate J-2 document assessor points of contact (POCs) for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor POCs are responsible for the following J-6 Assessment Tool actions:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

b. The Intelligence Certification (led by DIA/J-2) of JCIDS documents is conducted in a separate, but related process that examines intelligence support needs for completeness, supportability, and impact on joint intelligence planning. Collaboration and coordination between J-2 and J-6 regarding issues relating to intelligence information requirements is critical to the respective goals of both processes. In addition, to conserve resources, coordination and combined testing with DISA JITC is encouraged to support security intelligence certification tests that overlap.

3. Joint Staff, J-4, will:

a. Designate J-4 document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor POCs are responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

b. Procedures and criteria for J-4 Certification of Insensitive Munitions are distinct from the procedures and criteria in this instruction and can be obtained through consultation with the Joint Staff J-4.

4. US Joint Forces Command (USJFCOM). Serves as the joint force integrator of the Department of Defense. USJFCOM, as the Chairman's Advocate for interoperability, may require selected programs and systems for interoperability demonstrations, using the JBC ITDC. These demonstrations do not replace the JITC system interoperability test

certification. Demonstration results could be used or provided to JITC to assess the system for interoperability test certification.

a. USJFCOM will review and confirm the sufficiency of NR-KPPs and integrated architectures for all IT and NSS programs for all ACAT, Non-ACAT, and fielded systems. This evaluation will be based on the warfighter's perspective using a universal joint task list (UJTL)/joint mission-essential task list (JMETL) based assessment process.

b. Designate command document assessor POCs for the J-6 Assessment Tool (Enclosure J). The command must have one primary and one alternate document assessor POC. The document assessor is responsible for the following J-6 Assessment Tool actions:

(1) Identify the individuals within the organization who should review each document.

(2) Assist each document reviewer in obtaining a username and password for a read only user account.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated organization approved reviewer comment matrix in the proper format.

5. Combatant commanders will:

a. Review and comment on relevant programs during the J-6 interoperability and supportability certification process.

b. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

c. Participate, as appropriate, in IT and NSS interoperability testing programs by planning, programming, budgeting, executing and providing resources IAW agreed-to schedules and test plans. Required interoperability testing and certification will have some impact on schedules and costs of programs. These cost and schedule impacts will need to be added to POM and project cost estimates.

6. Military Services, Defense agencies and US Special Operations Command (USSOCOM) will:

a. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

b. Identify all Service or Agency systems that require external joint and combined interfaces with other Service or agency programs and systems.

c. Ensure the CPD NR-KPP along with other KPPs and critical technical and operational issues are used to develop the ISP and the TEMP.

d. Ensure the Program Managers' design includes all user required external joint and combined DOD DISR-compliant system interfaces when building new systems or modifying existing ones through coordination with all DOD components and allies.

e. Participate in configuration management (CM) of interface standards.

f. Participate in DOD efforts to influence development of non-government standards for supportability of all IT and NSS. Implement standards in candidate systems and test those implementations for conformance with the standards.

g. Participate in the MCEB and appropriate sub-panels.

h. In coordination with DISA (JITC), develop interoperability test and evaluation criteria for inclusion in acquisition documents, TEMP, and other test plan submissions. Prior to a Milestone C decision approval for all new or modified IT and NSS, the Services and Defense agencies, and participating test unit coordinators will ensure those systems undergo Joint Interoperability Certification test and evaluation IAW these criteria. This includes any limited or prototype IOC fielding. Services, Defense agencies, and participating test unit coordinators will ensure a TEMP is approved, prior to KDP-C for space systems being acquired under reference dd, to ensure the system will complete interoperability certification testing IAW these criteria. Actual certification testing will likely occur after KDP-C and prior to the first launch and/or prior to declaration of IOC.

i. Participate in IT and NSS Joint interoperability and accreditation testing programs by planning, programming, budgeting, executing and providing resources in accordance with agreed-to schedules and test plans. Required Joint interoperability testing and certification will have some impact on schedules and costs of programs. These cost and schedule impacts will need to be added to POM and project cost estimates.

(1) Resources include:

(a) Services and Defense agencies, such as DISA JTIC.

(b) Services and Defense agencies systems, equipment, and personnel, necessary to accomplish standards conformance testing and interoperability testing.

(2) For DISA JITC system interoperability test certification, the sponsor will:

(a) Coordinate funding with DISA (JITC) prior to the initiation of DISA (JITC) efforts. The System Program Office will coordinate with DISA (JITC) to determine funding required to support interoperability testing and certification. Once funding is identified, the Program Office will identify this requirement as an integrated facet of the program cost through the Service/agency POM process.

(b) Include funding the Service/Agency Participating Test Unit Coordinator (PTUC). The PTUC will be the point of contact (POC) for coordinating funding with DISA (JITC) prior to the initiation of DISA (JITC) efforts.

j. Provide direction to acquisition managers to ensure that all weapon systems that have or depend on IT and NSS capabilities are certified and tested for interoperability.

k. Provide guidance to all program managers to ensure that information assurance hardware and software capabilities (tools) are assessed for and meet interoperability requirements as established by the IAP.

l. Ensure all programs are compliant with current DOD information assurance directives and policies.

m. Provide guidance and direction to all program managers that all systems must be certified and accredited IAW applicable policy.

n. Provide systems engineering guidance to other components to implement IA solutions and to facilitate IA accreditation.

7. Director, Defense Information Systems Agency (DISA) will:

a. Participate in the technical assessment of all IT and NSS requirements and capability documents.

b. Exercise DISA's role as executive agent for coordinating and integrating the common operating environment (COE), GIG, and GIG Enterprise Services (GIG-ES) activities.

c. Exercise DISA's role as executive agent for coordinating and integrating the Department of Defense IT standards activities, and for integrating the DOD DISR tenets and their supporting infrastructure activities and capabilities.

d. Manage the IT and NSS Standards within the Defense Standardization Program to ensure that appropriate standards are available and used. Ensure that requirements for standards are identified, and related standards projects are planned, prioritized and properly resourced.

e. Provide guidance, assistance, profiling tools and information on appropriate use of standards including the applicability of standards to

DOD DISR Services (e.g., networking), Domains (e.g., combat support) and program phases (e.g., use of existing standards for imminent acquisitions and use of emerging standards for long-range program planning).

f. Ensure that the DOD standards profiles (TV-1) conform to DOD DISR standards for interoperability by requiring that standards profiles be generated through the use of the DISR online tool and an interoperability requirements profile generated by the Levels of Information System Interoperability (LISI) InspecQtor tool.

g. Provide an assessment of the suitability of standards identified in IT and NSS programs submitted under this instruction. Standards issues that cannot be resolved will be forwarded by DISA to the MCEB.

h. Provide systems engineering and developmental interoperability testing assistance to system developers to help ensure maximum interoperability and minimum duplication.

i. Review all available Test and Evaluation Master Plans and provide acquisition managers with recommended interoperability test and evaluation criteria, as well as accreditation testing (reference u), for inclusion in acquisition documents and test plans. Coordinate with NSA regarding the inclusion of IA standards.

j. Establish and conduct, in collaboration with other DOD components, the JITC joint interoperability test and evaluation and certification program for IT systems, including NSS.

k. Forward Joint Interoperability System Test Certification results to the J-6 for validation IAW the NR-KPP validation.

l. Certify interoperability and standards implementation or compliance to the MCEB ITP and to the developmental and operational testing organizations of DOD components.

m. Publish an annual report to the Joint Staff J-6, USD(AT&L), ASD (NII/DOD CIO), DOT&E, DOD Executive Agent for Space, and USJFCOM containing a summary of system interoperability test certification status of functional areas.

n. IAW MCEB Pub 1, provide a semi-annual update in the status of DISA JITC interoperability testing to the MCEB.

o. Serve as executive agent for the MCEB ITP (reference h).

p. Coordinate with DIA in matters of networking and communications services for the DOD Intelligence Information System (DODIIS).

q. Facilitate joint interoperability across the DOD global, theater, and tactical network boundaries.

r. Provide systems engineering, planning, and program guidance to the DOD components and agencies to implement solutions and to facilitate joint interoperability.

s. Assist NSA/CSS in coordinating and defining tactical signals intelligence (SIGINT) standards and processes and promote security, integration, interoperability, and data sharing among systems. Additionally, in coordination with NSA, review and define information assurance standards.

t. Provide test tools and procedures, and support systems in support of interoperability and standards conformance testing. Validate test tools and procedures (including those developed by other organizations) for interoperability and standards conformance testing.

u. Designate a central office to act as system manager of the J-6 Assessment Tool (see Enclosure J).

v. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer obtain a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

w. Coordinate with the National Security Agency (NSA), for any DOD system that collects, stores, transmits, or processes unclassified or classified information, to ensure security-testing considerations are addressed in interoperability testing.

x. Establish and maintain an automated process to track system status, monitor certification status, document ICTO information, and track uncertified systems.

y. Exercise DISA's role as executive agent for the Joint Interoperability of Tactical Command and Control Systems (JINTACCS), Information Technology standardization program and conformance to current message implementations for all inter and intra DOD component IT and NSS that exchange and use information to enable units/forces to operate effectively in Joint, Coalition and interagency operations."

8. Community Functional Lead for Cryptology (CFLC) - Director, National Security Agency (NSA)/Chief Central Security Service (CSS), will:

a. As the executive agent for approving and enforcing tactical SIGINT architectures and standards, approve all SIGINT investment programs and provide standards compliance and interoperability assessment reports to assist MDAs in production decisions.

b. Ensure that DOD cryptologic/cryptographic programs and US Signals Intelligence Directives (USSIDs) comply with interoperability and supportability policy (e.g., DCID 6/1 and 6/3).

c. Ensure IA and IA-enabled products comply with National Security Telecommunications and Information Systems Security Policy 11 (NSTISSP 11).

d. Ensure, in coordination with other DOD components, that requirements for cryptologic/cryptographic systems interoperability are satisfied through the design and development of technical, procedural, and operational interfaces between IT and NSS systems and those intelligence systems processing foreign intelligence and foreign counterintelligence information.

e. Perform CM for cryptologic systems; perform CM jointly with DISA for the interface between cryptologic systems and IT and NSS systems.

f. Provide information assurance guidance and assistance to the development of information technology architectures, incorporation of information assurance related standards in the DOD Information Technology Standards Registry (DISR), and in certification and accreditation activities.

g. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

9. Director, National Geospatial-Intelligence Agency (NGA), will:

a. Ensure that National System for Geospatial Intelligence (NSGI) standards and specifications established by NIMA for geospatial intelligence support the interoperability of IT and NSS via coordination with the Military Services, DISA and the unified commands.

b. Set standards for all geospatial intelligence systems and interfaces, including to the Net Centric Enterprise Services and their accompanying KIPs.

c. Ensure NSGI standards and specifications incorporate imagery and geospatial information release or disclosure decisions.

d. Ensure that commercial and non-governmental standards used for imagery and geospatial systems and applications are open-systems based and conform to Defense Information Infrastructure (DII) and DOD DISR tenets for interoperability across the geospatial intelligence user community.

e. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

10. Director, Defense Intelligence Agency (DIA), will:

a. Ensure that standards and specifications established for measurement and signature intelligence (MASINT) under the US MASINT System (USMS) support the interoperability of IT and NSS systems via coordination with the Military Services.

b. Ensure that commercial and non-governmental standards used for MASINT systems and applications are open-systems based and conform to DII and DOD DISR tenets for interoperability.

11. Program Managers from combatant commands, Military Services and Defense agencies, when building new, or modifying existing systems, will ensure that they are:

a. Compliant with the Clinger-Cohen Act of 1996, as amended (sections replaced by Pub L 102-217).

b. Compliant with the latest version of the DOD Information Technology Standards Registry (DISR).

c. Certified and accredited IAW current DOD Information Assurance directives and policies.

d. Interoperable with other DOD, Joint and Coalition systems, unless security requirements prohibit or limit the sharing of information.

e. Properly evaluated and certified for interoperability by DISA or obtain an Interim Certificate to Operate (ICTO) IAW MCEB Pub 1, as required, until system interoperability test certification is complete.

f. Compliant with LISI profiles requirements.

12. DOD Executive Agent for Space. As the DOD executive agent for Space, the Under Secretary of the Air Force, will review and confirm the sufficiency of NR-KPPs and integrated architecture products for all National Security Space Programs for all ACAT, non-ACAT and fielded

systems. This evaluation will be based on ensuring architectures are in compliance with approved space architectures.

13. Other DOD Components. Coordinate on interoperability certification and supportability documents developed by other sponsors to identify opportunities for cross-component utilization, Joint Integration and harmonization of capabilities. Make recommendations to the J-6 on whether staffing documents contained in ICD, CDD, CPD, ISP proposals meet recognized standards.

(INTENTIONALLY BLANK)

ENCLOSURE C

CAPSTONE REQUIREMENTS DOCUMENT (CRD)

1. General. The Joint Staff J-6 performs interoperability requirements certification, supportability certification and interoperability system validation for both the development and production of IT/NSS systems/programs. Documents submitted by Military Services and Defense agencies shall follow the format contained in CJCSM 3170.01 and shall include JCPAT system registration, LISI profiles (Enclosure K) and DISR online profiles (Enclosure L).

a. J-6 Capabilities Interoperability Certification. This certification occurs prior to each acquisition milestone.

(1) Initial Capabilities Document (ICD) certification occurs prior to Milestone A. ICD certification occurs prior to KDP-A for space systems being acquired under reference dd.

(2) Developmental Capabilities Interoperability Certification occurs prior to Milestone B usually in a CDD. Developmental certification allows the sponsor to adjust the KPP values in the next level document (typically, the CPD). For example, the timeliness fields within the IER matrix maybe "TBD" due to technology and spiral development. CDD certification occurs prior to KDP-B for space systems being acquired under reference dd.

(3) Production Capabilities Interoperability Certification occurs prior to Milestone C usually in a CPD. Production certification is more stringent than developmental certification. A complete design analogous to an ISP with all of the technical information and specifications is mandatory to ensure complete capabilities interoperability certification. CPD certification occurs prior to KDP-C for space systems being acquired under reference dd.

(4) The J-6 certifies the NR-KPP derived from a set of top-level requirements, capability documents and programs for all ACAT, non-ACAT, and fielded systems for conformance with policy, doctrine and applicable interoperability standards for joint IT and NSS. The J-6 forwards interoperability certification to the JROC or to the sponsoring DOD component via KM/DS.

(5) As part of the review process, J-8 staffs all JCIDS documents (to include JROC Interest, Joint Impact and Joint Integration) on KM/DS to OSD, combatant commanders, the Services, the Joint Staff and DOD agencies.

(6) USJFCOM, as the joint force integrator, will review ICDs, CDDs, CPDs and Information Support Plans (ISPs). USJFCOM, as the Chairman's Advocate for interoperability, may require selected programs and systems for interoperability demonstrations, using the JBC ITDC. Selection of the program or system may be made by the Joint Battle Management Command and Control Board of Directors. This does not replace the JITC system interoperability test certification and the demonstration results could be used or provided to JITC to assess the system for interoperability test certification.

(7) J-6 will forward unresolved interoperability issues to the MCEB or MIB for resolution. The MCEB or MIB will return resolved interoperability issues to the lead DOD component to complete the JROC approval process. The MCEB and MIB will ensure that unresolved issues resulting from interoperability assessments are presented to the JROC for resolution (see Figure C-1).

b. Supportability Certification. The J-6 certifies to ASD(NII) that IT and NSS programs for all ACAT, adequately address infrastructure requirements, the availability of bandwidth, spectrum support, and identify dependencies and interface requirements between systems. PMs will submit the applicable CDD/CPD along with the ISP into the JCPAT tool for supportability certification review.

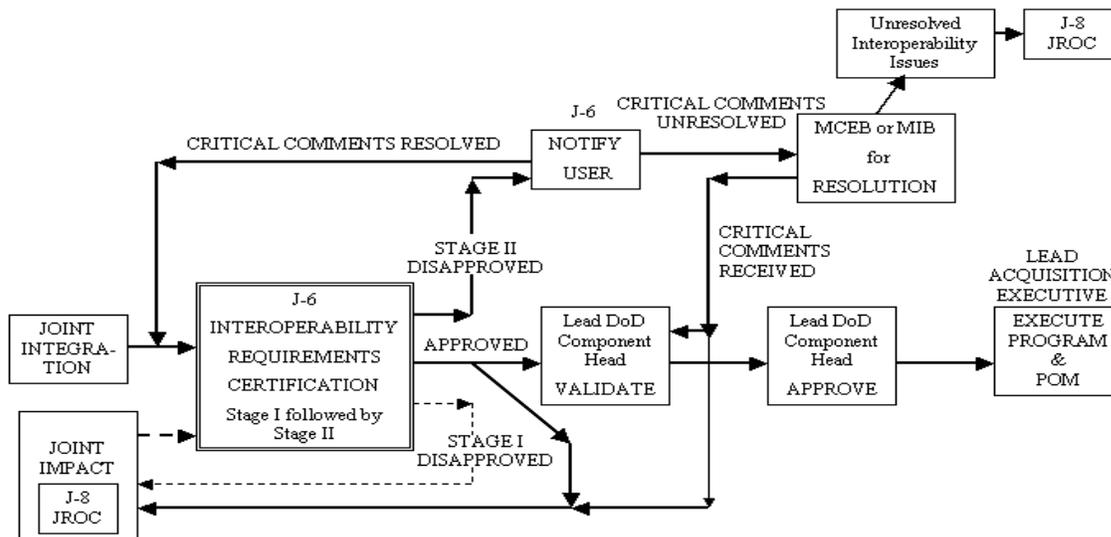


Figure I-1. Critical Comment Resolution Process

c. J-6 Interoperability System Validation. The J-6 validation is intended to provide total lifecycle oversight of warfighter capabilities interoperability. The J-6 validates the DISA (JITC) interoperability system test certification, which is based upon a joint certified NR-KPP, approved in the CDD, CPD and ISP. The validation will occur after receipt and analysis of the DISA (JITC) interoperability system test certification. The J-6 will issue an interoperability system certification memorandum to the respective Services, agencies and developmental and operational testing organizations.

2. Assessment Procedure Overview. Documents submitted by combatant commands/Services/agencies will be evaluated early in the lifecycle of a system and at all acquisition milestones to help the developer ensure that a system or program will successfully achieve system test certification and eventual fielding.

a. To support the interoperability certification process, J-6 requests technical assessments from DISA, Services and other DOD agencies.

b. USJFCOM, as the joint force integrator, will review all ICDs, CDDs, CPDs and ISPs.

c. Combatant commanders are invited to review and comment on all JCIDS documents during the J-8 (JROC) formal review. During this review, combatant commanders should review these documents for interoperability concerns and include interoperability related comments in the response to J-8. All interoperability comments submitted to the KM/DS tool will be identified in the KM/DS Comment Matrix by inserting "Interoperability Comment" as the first entry in the COMMENT column. Only comments so marked will be considered as part of the interoperability certification process.

d. J-8 staffs JCIDS documents using the J-8 KM/DS tool IAW references a and b. J-6 and OASD(NII) use a DISA-managed electronic tool, the ISP Program Assessment Tool in JCPAT, for the staffing, coordination, and compilation of assessment comments for ISPs. Enclosure J provides more information on the J-6 Assessment Tool.

e. J-6 interoperability certifications of capabilities and capability documents and programs are conducted in four distinct stages.

(1) O-6 Level Review is the draft assessment for all types of documents.

(2) Flag Level Review (for JROC Interest and Joint Impact JCIDS documents and OSD Special Interest ISPs) or Certification Review Stage (Joint Integration JCIDS documents and all non-OSD Special Interest ACAT ISPs) review is the final assessment.

(3) FCB Draft (JROC Interest and Joint Impact JCIDS documents) or Final stage (for Joint Integration JCIDS documents and all ISPs). Interoperability and supportability certifications will be issued upon successful adjudication of all comments from the previous two review stages. PMs will submit the final or FCB Draft document along with the adjudicated comments resolution matrix to the J-8 KM/DS tool (JCIDS documents) or JCPAT (ISPs) for review and certification by J-6.

(4) Upon receipt of the interoperability or supportability certification, PMs will post the completed and JROC/FCB or MDA approved document to KM/DS (JCIDS documents) or JCPAT (ISPs) for archival.

f. The suspense for completing Stage I documents for certification is normally 25 sequential days from the transmittal date from the J-8 RAD Action Officer (for JROC Interest and Joint Impact designated programs) for staffing in the J-8 KM/DS Tool. The suspense date for Joint Integration will normally be 25 sequential days from the date the Joint Potential Designator (JPD) is set by the JCIDS Gatekeeper (references a and b). DISA will download the applicable documents from KM/DS for all JROC Interest, Joint Impact and Joint Integration programs for interoperability and supportability review. The actual suspense date will be posted in the J-6 Assessment Tool.

g. The Stage II suspense is normally 21 sequential days.

h. The Stage III suspense is normally 15 sequential days after JROC or MDA approval.

i. All DOD ISP originators and assessors (combatant commanders, Services, agencies) will use the ISP Assessment Tool on JCPAT to submit ISP documents and assessor comments to J-6 for all ISPs.

j. During Stages I and II, assessors will submit comments in the following categories.

(1) CRITICAL. A critical comment indicates non-concurrence with the document until the comment is satisfactorily resolved. Prior to submitting a critical comment for flag-level review, a commenter is required to contact and coordinate with the document submitter and the comment will require a planner level approval for submission.

(2) SUBSTANTIVE. A substantive comment is provided because a section in the document appears to be or is potentially unnecessary, incorrect, misleading, confusing, or inconsistent with other sections. A substantive comment not resolved in Stage I could result in a critical comment during

Stage II. Additionally, multiple substantive comments could result in a critical comment and non-certification of the document.

(3) ADMINISTRATIVE. An administrative comment addresses what appears to be a typographical, format, or grammatical error.

k. Formal comments will indicate the page and paragraph numbers from the document and provide a rewrite recommendation and a rationale.