



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6

DISTRIBUTION: A, B, C, J, S

CJCSI 6212.01D

8 March 2006

Directive current as of 14 March 2007

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure F.

1. Purpose. This instruction

a. Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs.

b. Establishes procedures to perform I&S Certification and J-6 System Validation of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems cited in references a and b.

c. Establishes procedures to perform I&S Certification and J-6 System Validation of Information Support Plans (ISPs) for all non-ACAT and fielded programs/systems (references c and d).

d. Defines the four elements of the Net-Ready Key Performance Parameter (NR-KPP).

e. Provides guidance for NR-KPP development and assessment.

f. Establishes procedures for Joint Interoperability Test Command (JITC) Joint Interoperability Test Certification.

2. Cancellation. CJCSI 6212.01C, 20 November 2003, "Interoperability and Supportability of Information Technology and National Security Systems" is canceled.

3. Applicability. This instruction applies to:

a. The Joint Staff, Services, combatant commands, Defense agencies and joint and combined activities. This instruction also applies to other agencies preparing and submitting JCIDS documents in accordance with references a and b.

b. 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 (references e and f) IT and NSS acquisition systems. Non-ACAT activities and procurements include all defense IT and NSS projects, IT and NSS pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations (ACTD), Advanced Technology Demonstrations (ATD), and Coalition Warrior Interoperability Demonstrations (CWID) 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); and post-acquisition (fielded) IT and NSS 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.

(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 Director of National Intelligence (DNI) 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).

(5) All DOD component IT and NSS supporting business areas and domains within the Department of Defense.

c. Any organization that supports the J-6 in its role to perform I&S Certification of IT and NSS.

4. Policy. It is Joint Staff policy to assure that DOD components 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; (4) are interoperable with allies and coalition partners; (5) are net-ready; and (6) allow US forces to protect mission essential data; detect and respond to network intrusion/system compromise; and restore mission essential data.

a. All IT and NSS and major modifications to existing IT and NSS will be compliant with DOD regulations and policies contained in references c through i. The NR-KPP is a mandatory element of Capability Development Documents (CDDs), Capability Production Documents (CPDs) and Information Support Plans (ISPs) except for those that do not communicate with external systems. Establishing and maintaining interoperability and supportability in a DOD system is a continuous process that must be managed throughout the lifecycle of the system.

b. Interoperability and Supportability Certification shall be accomplished through an assessment of adherence to the NR-KPP and other applicable IT and NSS specific policies/guidance to include Spectrum Supportability (references i through k) and Selective Availability Anti-Spoofing Module (SAASM) (reference l) compliance.

c. An NR-KPP, consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

d. The four NR-KPP elements include: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM) (reference m), supporting integrated architecture products (references n and o) required to assess information exchange and operationally effective use for a given capability, compliance with applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) (<http://kips.disa.mil>), and verification of compliance with DOD information assurance requirements (references p through u).

e. The Joint Staff Interoperability and Supportability (I&S) Certification process is an integral part of the JCIDS process. I&S Certifications granted under the former requirements generation system remain valid; however, all capabilities documents supporting a Milestone B or Milestone C decision will include the NR-KPP elements applicable to the program. See National Security Space Acquisition Policy 03-01 (reference v), for space program key decision points (KDPs).

CJCSI 6212.01D
8 March 2006

f. Secret and below ISPs shall be submitted to the OSD ISP (C4ISP) Assessment Tool for review via the Secret Internet Protocol Router Network (SIPRNET) Joint C4I Program Assessment Tool-Empowered (JCPAT-E) (URL: <https://jcpat.disa.smil.mil>) or Non-secure Internet Protocol Router Network (NIPRNET) JCPAT-E (URL: <https://jcpat.disa.mil>). TS and/or SCI ISPs will be posted on the Joint World Wide Intelligence Communications System (JWICS) by the sponsoring entity. SCI and SAP document submissions parallel the KM/DS process – specific submission instructions can be obtained from J-8. DODI 4630.8 provides specific ISP preparation, review procedures, formats and timelines.

g. Interoperability and Supportability of IT and NSS.

(1) Interoperability and Supportability of IT and NSS capabilities for ACAT programs will be determined during the JCIDS process (references a through d, f, g and this instruction) and will be updated as necessary throughout the acquisition process, deployment and operational life of a system.

(2) Table 1 summarizes the I&S Certification and J-6 System Validation of IT and NSS. The entries in the table also include the reference that contains the detailed procedures.

| IT&NSS Program | | JCD | ICD | CDD | CPD | ISP*** | Joint Interoperability Test Certification Complete |
|---|--------------------|--|-----|-----|-----|--------|--|
| JCIDS JPD | JROC Interest | | | C2 | C2 | N1 | V3 |
| | Joint Integration | | | C2 | C2 | N1 | V3 |
| | Joint Information* | | | | | N3 | V3 |
| | Independent | | | | | N3 | V3 |
| OSD Special Interest** | | | | | | C1 | V1 |
| Non-ACAT | | | | | | C3 | V3 |
| Fielded Systems | | | | | | C3 | V3 |
| Requirement C: I&S Certification V: J-6 System Validation N: NR-KPP Certification * Joint Information JPD per JROCM 100-05 may be elevated to JROC Interest or Joint Integration **OSD ISP Special Interest per OSD Memorandum (ACAT II or III) *** Tailored ISP Contains Fewer Arch Products, but Still Requires the Appropriate Certification and Validation | | Governing Directive 1: DODI 4630.8 2: CJCSI 3170.01 and CJCSI 6212.01 3: CJCSI 6212.01 | | | | | |

Table 1. Interoperability and Supportability Certification and Validation Summary

(3) I&S of IT and NSS capabilities for non-ACAT and fielded systems will be determined by the approving authority IAW references c, d, f, h and this instruction and will be updated as necessary throughout the acquisition period, deployment, and operational life of a system. J-6 certifies the NR-KPP to ASD(NII)/DOD CIO in the form of an I&S certification of the ISP for these programs/systems.

(4) Joint Interoperability Test Certification is provided by the JITC upon completion of testing and is valid for three years from the date of the certification or when subsequent program modifications change components of the NR-KPP or supportability aspects of the system. This includes: when materiel changes (e.g., hardware or software modifications, including firmware) and similar changes to interfacing systems affect interoperability; upon revocation of joint interoperability test certifications or JS J-6 System Validation; and non-materiel changes (i.e., DOTLPF) that may affect interoperability.

(5) J-6 System Validation occurs upon completion of both the I&S Certification and the Joint System Interoperability Test Certification. The Validation expires 3-years from the date of the Test Certification or when subsequent program modifications change components of the NR-KPP or supportability aspects of the system.

5. Definitions. See Enclosure GL, Part II.

6. Responsibilities. See Enclosure B.

7. Summary of Changes. This revision:

a. Reflects a significant change and restructuring to reflect lessons learned from implementation of the NR-KPP.

b. Introduces and provides guidance for the Tailored ISP (TISP).

c. Provides additional data strategy guidance IAW references w and x.

d. Adds the following architecture products: OV-7, SV-2, SV-11 and TV-2 to the NR-KPP.

e. Updates policy regarding the Key Interface Profiles (KIPs).

f. Explains the requirements to support the IA certification and accreditation (C&A) process and spectrum supportability requirements.

g. Addresses combatant command, Service, and Agency (CC/S/As) needs for Organization Unique Standards (OUSs) to be identified in JCIDS and ISP documents.

CJCSI 6212.01D

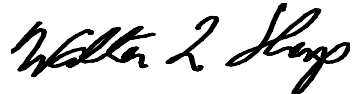
8 March 2006

h. Deletes requirements associated with the Levels of Information Systems Interoperability (LISI) and Interconnectivity and Interoperability Capability (IIC) Profiles.

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. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This document is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:



WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Enclosures:

- A – Life Cycle Process Overview
- B – Responsibilities
- C – Staffing Process and Procedures
- D – Determining Interoperability, Supportability, and Net-Readiness
- E – Joint Interoperability Testing and Certification Process
- F – References
- GL – Glossary

CJCSI 6212.01D
8 March 2006

DISTRIBUTION

Distribution A, B, C, and J plus the following:

| | <u>Copies</u> |
|--|---------------|
| Secretary of State..... | 2 |
| Secretary of Defense..... | 2 |
| Director of National Intelligence | 2 |
| Under Secretary of Defense for Acquisition, Technology And Logistics | 2 |
| Undersecretary of Defense (Comptroller)..... | 2 |
| Under Secretary of Defense for Personnel and Readiness..... | 2 |
| Under Secretary of Defense for Policy | 2 |
| Under Secretary of Defense for Intelligence | 2 |
| Assistant Secretary of Defense (Health Affairs)..... | 2 |
| Assistant Secretary of Defense (Networks & Information Integration)/DOD CIO | 2 |
| Director, Program Analysis and Evaluation | 2 |
| Director of Operational Test and Evaluation | 2 |

CJCSI 6212.01D
8 March 2006

(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 6 | O | D-1 thru D-24 | O |
| i thru viii | O | D-A-1 thru D-A-6 | O |
| A-1 thru A-8 | O | D-B-1 thru D-B-6 | O |
| B-1 thru B-12 | O | D-C-1 thru D-C-14 | O |
| C-1 thru C-8 | O | E-1 thru E-22 | O |
| C-A-1 thru C-A-4 | O | F-1 thru F-4 | O |
| C-B-1 thru C-B-2 | O | GL-1 thru GL-20 | O |

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

CJCSI 6212.01D
8 March 2006

RECORD OF CHANGES

| Change No. | Date of Change | Date Entered | Name of Person Entering Change |
|------------|----------------|--------------|--------------------------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

| | Page |
|--|----------|
| ENCLOSURE A Life Cycle Process Overview | A-1 |
| ENCLOSURE B Responsibilities | B-1 |
| ENCLOSURE C Staffing Process And Procedures..... | C-1 |
| ENCLOSURE D Determining Interoperability, Supportability and Net- Readiness | D-1 |
| ENCLOSURE E Joint Interoperability Testing And Certification Process..... | E-1 |
| ENCLOSURE F References | F-1 |
| ENCLOSURE GL Glossary | GL-1 |
| FIGURE | Page |
| A-1 DOD Acquisition, JCIDS and I&S Certification Process Relationship..... | A-4 |
| A-2 ASD(NII)/DOD CIO ISP Submission Process (Pilot Program) | A-5 |
| C-1 J-6 Critical Comment Resolution Process | C-4 |
| C-2 Sample Comment Resolution Matrix for JCIDS Documents..... | C-6 |
| D-1 NCOW RM Top Level Activity Model Decomposition | D-6 |
| D-2 Architecture Linkage to NR-KPP Attributes | D-12 |
| D-3 KIP Development Process | D-17 |
| E-1 Joint Interoperability Test Certification Process | E-6 |
| TABLE | Page |
| 1-Interoperability and Supportability Certification and Validation Summary | 4 |
| A-1 Interoperability and Supportability Internet Resources..... | A-7 |
| C-1 Staffing Timelines | C-4 |
| D-1 NR-KPP Products Matrix..... | D-3 |
| D-2 NR-KPP Compliance Statement..... | D-4 |
| D-3 Architecture Products Descriptions | D-12 |
| D-4 KIP Consumer and Provider Responsibilities..... | D-15 |
| D-A-1 NR-KPP Compliance Statement | D-A-2 |
| D-A-2 Example KIP Declaration Table | D-A-6 |
| D-C-1 Interoperability and Supportability Assessor's Checklist..... | D-C-1 |

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

ENCLOSURE A

LIFE CYCLE PROCESS OVERVIEW

1. This enclosure provides an overview of this instruction and its relationship to other Joint Staff and DOD policies and processes that require, affect, or contribute to achieving and maintaining interoperability and supportability throughout the lifecycle of DOD IT and NSS systems.

2. Relationship between this instruction and related DOD and Joint Staff policies and processes.

a. Clinger-Cohen Act. The Clinger-Cohen Act (CCA) (reference y), along with its many amendments, resides in Subtitle III (information Technology Management) of title 40, United States Code and defines IT and NSS. Section 2223 of title 10, includes the responsibility of the DOD CIO to ensure the interoperability of IT and NSS throughout DOD.

b. E-Government Act. The E-Government Act (Public Law 107-347), Title III, Federal Information Security Management Act of 2002 (reference z) requires Federal agencies to (i.e., DOD and its components) develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source and; ensure that information security is addressed throughout the life cycle of each agency information system.

c. DOD 5000 Series, National Security Space Acquisition Policy 03-01, and Defense Acquisition Guidebook. DODD 5000.1 prescribes DOD Policy for the Defense Acquisition System. DODI 5000.2 provides instructions for acquisition of non-space systems and National Security Space Acquisition Policy 03-01 provides additional policy and instructions for acquisition of space systems. Moreover, the Defense Acquisition Guidebook (reference aa) and the Defense Acquisition University (DAU) is a primary source of acquisition guidance. CJCSI 6212.01 supports these acquisition policy and instruction documents by providing I&S Certification at key milestones through its interface with the JCIDS (references a and b) and the JCPAT-E.

d. DOD 4630 Series. The DOD 4630 Series publications prescribe policy for establishing and maintaining interoperability and supportability for all IT

CJCSI 6212.01D

8 March 2006

and NSS throughout their lifecycle. DODI 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" introduces and establishes the requirement for an Information Support Plan (ISP) for all Acquisition Category (ACAT), non-ACAT, and fielded systems, and that the ISP be maintained and updated over the lifecycle of all IT and NSS systems. CJCSI 6212 implements the DOD 4630 policy to ensure all non-ACAT, ACAT, and fielded systems are interoperable and supportable throughout their lifecycle.

(1) For ACAT programs, the ISP should be developed in conjunction with the associated Joint Capabilities Integration and Development System (JCIDS) documentation and results of the ISP analysis included in the appropriate supportability sections of the CDD and Capability Production Document (CPD) (see CJCS 3170 Series paragraph).

(2) For non-ACAT and fielded systems, including pre-acquisition demonstrations described in references c and d, the J-6 will provide an interoperability and supportability certification based on the NR-KPP within the ISP as ready to support JITC Interoperability and Standards conformance testing.

e. CJCS 3170 Series Documents. CJCSI 3170.01 and CJCSM 3170.01, "Joint Capabilities Integration and Development System," prescribe policy and procedures for the Joint Capabilities Integration and Development System (JCIDS). The JCIDS supports the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Requirements Oversight Council (JROC) in identifying, assessing and prioritizing joint military capability needs. The JCIDS provides the Chairman's advice and assessment for acquisition programs in support of the Defense Acquisition Process. CJCSI 6212 details how the J-6 performs I&S certification and validation of JCIDS documents for acquisition programs supporting milestone decisions and other programs as required/requested through the JCIDS process.

f. DODD 8320.2. DODD 8320.2, "Data Sharing in a Net-Centric Department of Defense," establishes policies and responsibilities for implementing data sharing within the GIG. Included in this policy is that data shall be visible, accessible, and understandable. Data assets will be tagged, discoverable, searchable and retrievable using DOD-wide capabilities. This instruction outlines the policy for data sharing as part of the Interoperability and Supportability Certification.

g. DOD and Joint Staff Information Assurance (IA) Policies (references p through s, u and bb through dd; references ee and ff for SCI and Special Access Programs). Information Assurance is one of the four NR-KPP elements. Like the 4630 Series, IA policies and processes apply to the entire lifecycle of IT and NSS. CJCSI 6212.01 does not duplicate existing IA policies and processes;

rather it synchronizes IA efforts with the verification of interoperability and supportability of IT and NSS over the lifecycle and is consistent with DOD critical infrastructure policies. IA policies and procedures such as DITSCAP accreditations are prerequisites for J-6 I&S Certification.

h. DODD 4650.1, "Policy for Management and Use of the Electromagnetic Spectrum" (reference j) and the National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management" (reference k). Spectrum supportability is an assessment as to whether the electromagnetic spectrum necessary to support the operations of a spectrum-dependent equipment or system is, or will be, available. The spectrum supportability assessment requires, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation from Host Nations, and a consideration of electromagnetic compatibility aspects. Policy requires that the DOD components developing or acquiring spectrum-dependent equipment or systems take certain actions to obtain spectrum supportability. For spectrum-dependent equipment or systems being developed, efforts to obtain spectrum supportability shall be initiated as early as possible during the concept and/or technology development phase and that no spectrum-dependent off-the-shelf or other non-developmental system shall be purchased or procured without a spectrum supportability determination. Requests for spectrum supportability assessments shall include identification of those Host Nations into which deployment is likely or planned. A spectrum supportability determination must be obtained prior to a Milestone B decision for ACAT programs. For non-ACAT systems, a spectrum supportability determination must be completed prior to fielding. This instruction outlines the policy for spectrum supportability as part of the Interoperability and Supportability Certification.

i. DODD 3222.3, "Department of Defense Electromagnetic Environmental Effects (E3) Program" (reference i). This directive provides policies and responsibilities to ensure mutual EMC and effective E3 control among ground, air, sea, and space-based systems, subsystems, and equipment, including ordnance. The directive requires E3 control requirements to be defined early during the concept and technology development phase and included in the pertinent acquisition documentation (such as the CDD, CPD, ISP, TEMP, SOW, and contract specification) and verified throughout the acquisition process.

j. DOD IT and NSS Specific Policies. CJCSI 6212.01 includes, in the I&S Certification processes, a review of compliance with DOD IT and NSS related policies (i.e., JTRS/radio acquisition policy (reference gg), SAASM (reference l), etc.).

k. Figure A-1 illustrates the general relationship between the DOD acquisition, JCIDS, and I&S Certification processes and documentation. Figure A-2 illustrates the ASD(NII) Pilot ISP program.

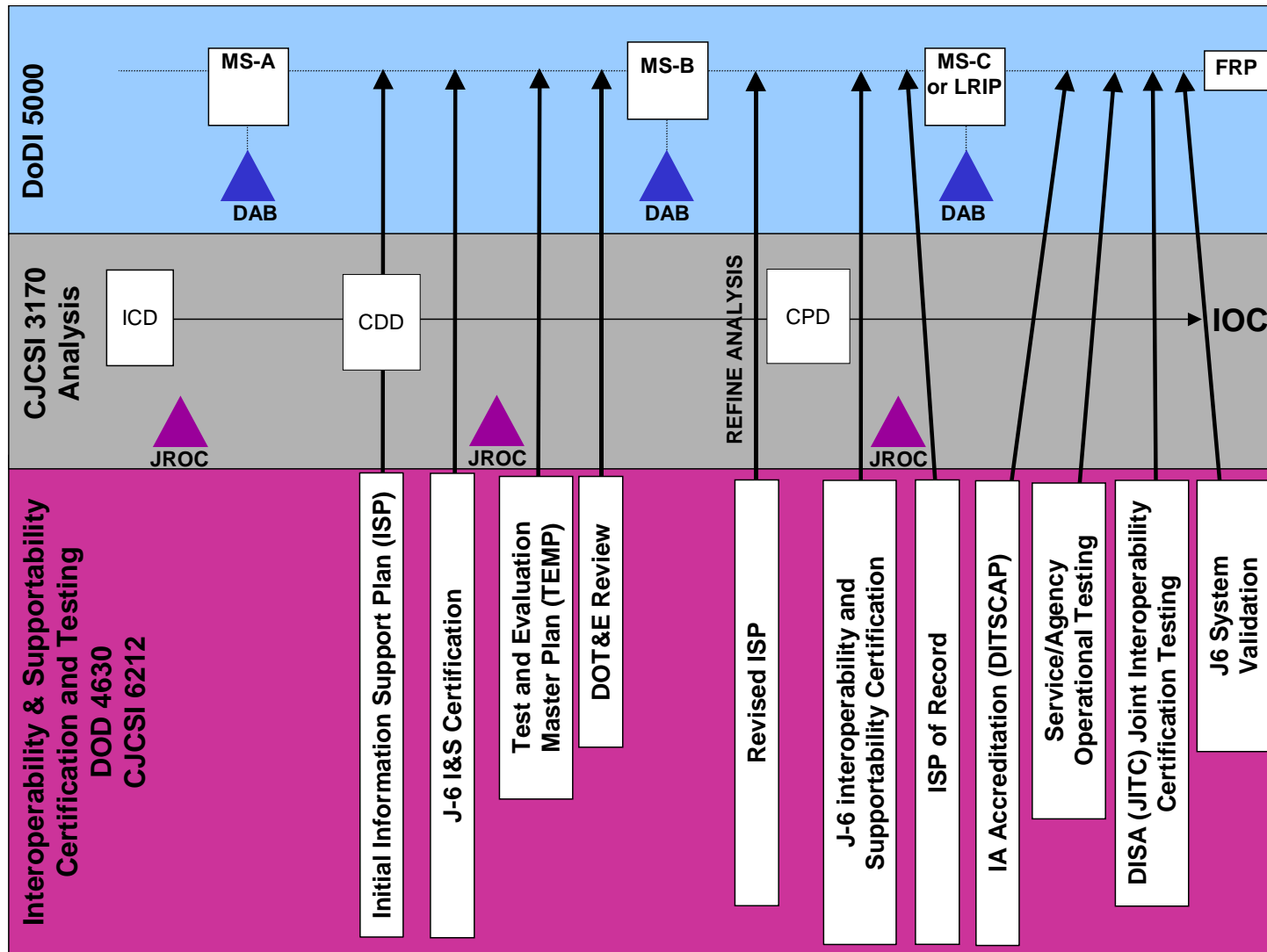


Figure A-1. DOD Acquisition, JCIDS and I&S Certification Process Relationships

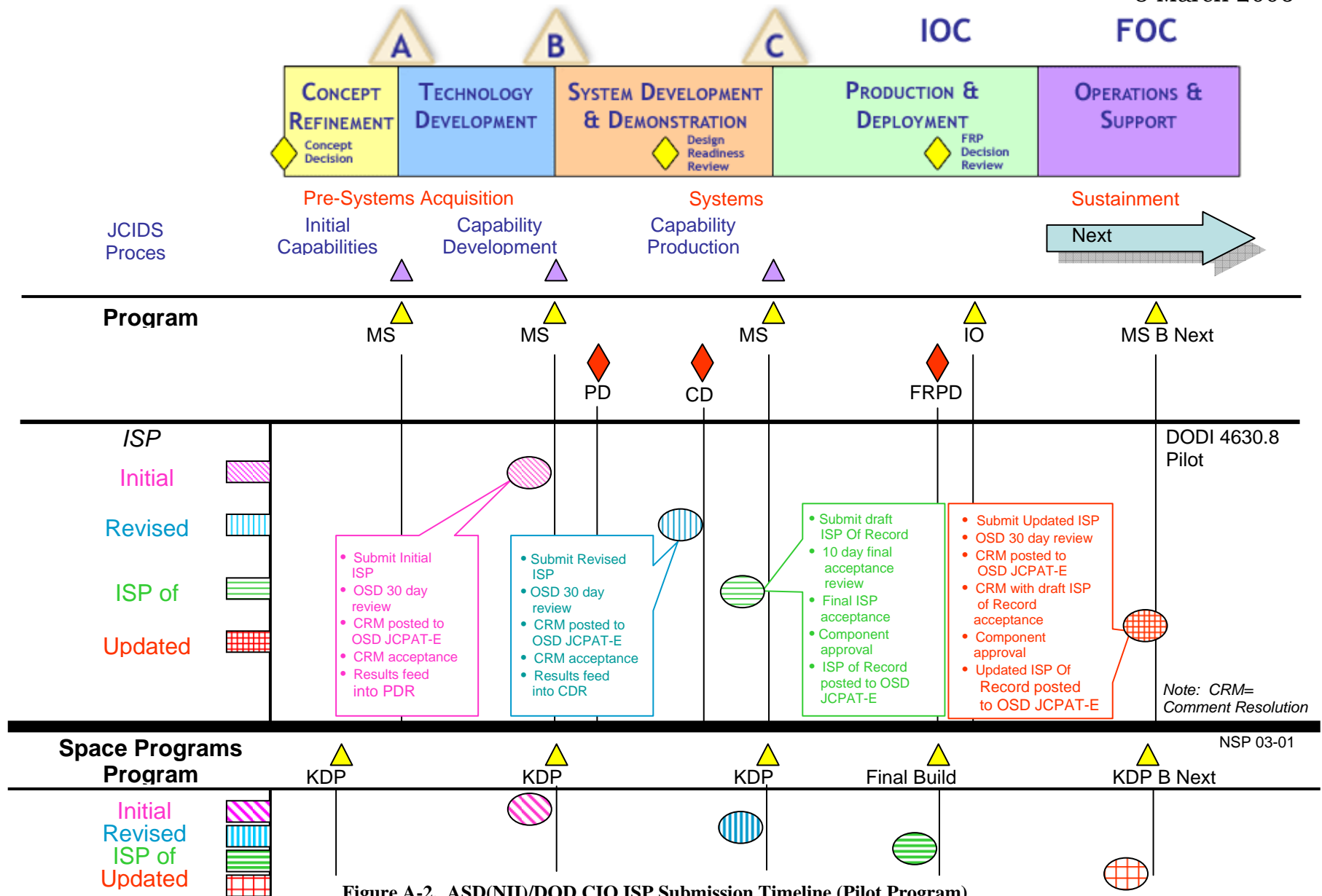
CJCSI 6212.01D
8 March 2006

Figure A-2. ASD(NII)/DOD CIO ISP Submission Timeline (Pilot Program)

CJCSI 6212.01D

8 March 2006

1. Programs following the traditional three stage ISP review process are not required to submit an ISP draft for review in advance of their Critical Design Review (CDR). Under the ASD(NII) ISP Pilot Program, the ISP review prior to the CDR is intended to give the PM another opportunity to influence system design and identify information related issues that can be resolved before the final development phase as well as provide a corresponding joint review prior to the Milestone C decision. Under the Pilot ISP Program, PMs still submit ISPs at Milestones B and C (IAW DODI 5000.2 and DODI 4630.8). The two-fold benefit of the Pilot ISP Program timing is to influence the CDR and to forestall late ISP submissions, which restrict comprehensive review prior to the Milestone C decision.

CJCSI 6212.01D
8 March 2006

m. The following table lists URLs for Interoperability and Supportability Internet resources:

| NIPR/ SIPR | Website | Topic |
|-----------------------|---|---|
| N | http://learn.dau.mil | Defense Acquisition University Continuous Learning (NR-KPP Module Under Construction) |
| N | https://learn.dau.mil/html/clc/Clc.jsp (Case Sensitive) | Defense Acquisition University Continuous Learning Browse Mode (NR-KPP Module Under Construction) |
| N | http://akss.dau.mil/dag | Defense Acquisition Guide Book |
| N | http://akss.dau.mil/jsp/default.jsp | AT&L Knowledge Sharing System |
| S | http://disronline.disa.smil.mil/a/DISR | DISRonline (SIPRNET) (Also resides on JWICS) |
| N | http://gesnew.dod.mil/obtainPKI.html | DOD PKI Client Certificate Assistance |
| N | http://jitc.fhu.disa.mil | JITC Public Web Site/MCEB Pub 1 |
| N | http://kips.disa.mil | KIPs (CAC Card Required) |
| N | http://www.defenselink.mil/nii/org/cio/doc/recmgnt.html | DODD 8320.2, Data Sharing in a Net-Centric Department of Defense |
| N | http://www.defenselink.mil/nii/doc/DoD_AF_v1_Volume_Deskbook.pdf | DODAF Deskbook |
| N | http://www.defenselink.mil/nii/doc/DoD_AF_v1_Volume_I.pdf | DOD Architecture Framework Volume I: Definitions and Guidelines |
| N | http://www.defenselink.mil/nii/doc/DoD_AF_v1_Volume_II.pdf | DOD Architecture Framework Volume II: Product Descriptions |
| N | http://www.dsc.osd.mil | Joint C4ISR Decision Support Center |
| N | http://www.dtic.mil/cjcs_directives | CJCS Directives Home Page |
| N | https://dars1.army.mil | DOD Architecture Repository System (DARS) |
| N | https://standmgt.disa.mil/restricted/ncow.html | DOD Global Information Grid Architectures (NCOW RM) |
| N | https://disronline.disa.mil | DISRonline (NIPRNET) |
| N | https://gesportal.dod.mil/sites/COIdirectory | DOD COI Directory/Guidance (CAC Card Required) |
| N | https://jcpat.disa.mil | JCPAT-E (NIPRNET) |
| S | https://jcpat.disa.smil.mil | JCPAT-E (SIPRNET) |
| S | https://jrockmds1.js.smil.mil/guestjrcz/guesthome | KM/DS |
| N | https://stp.fhu.disa.mil | JITC System Tracking Program (Select JITC for computer settings if link does not open) |
| N | https://www.dadms.navy.mil | DOD Information Technology Portfolio Registry (DITPR) (CAC Card Required) |
| N/S | Select ISP(C4ISP) Assessment Tool from JCPAT-E Link (NIPR or SIPR) | ISP (C4ISP) Assessment Tool on JCPAT-E |
| N | http://jitc.fhu.disa.mil/itp/isp_info.html | Tailored ISP (TISP) |
| N | http://diides.ncr.disa.mil/mdregHomePage/mdregHome.portal | DOD Metadata Registry Home Page |

Table A-1. Interoperability and Supportability Internet Resources

3. Organization of remaining enclosures

a. Enclosure B. Responsibilities. This enclosure outlines the stakeholder responsibilities in the interoperability and supportability policy and processes described within this instruction.

b. Enclosure C. Staffing Process and Procedures. This enclosure describes, in more detail, the processes for submission of documentation for interoperability and supportability review and certification/validation for all ACAT, non-ACAT and fielded IT and NSS. The appendices include the ISP(C4ISP) Assessment Tool and more detailed information on the Tailored ISP.

c. Enclosure D. Determining Interoperability, Supportability and Net Readiness. This enclosure describes the technical aspect of determining interoperability and supportability, including the NR-KPP, spectrum supportability, and compliance with DOD IT and NSS specific policies. It also includes an NR-KPP format, guidance on creating the TV-1 and TV-2, and an I&S Certification Assessor's Checklist.

d. Enclosure E. Joint Interoperability Test Certification Process. This enclosure details the policy and processes for joint interoperability test certification of IT and NSS over the lifecycle.

ENCLOSURE B

RESPONSIBILITIES

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

a. Perform IT and NSS Interoperability and Supportability (I&S) Certifications, NR-KPP Certifications, and System Validations IAW Table 1.

(1) Submit I&S Certifications to the Knowledge Management/Decision Support (KM/DS) tool for all CDDs and CPDs IAW references a and b.

(2) Provide an NR-KPP Certification to ASD(NII)/DOD CIO for ACAT I programs and programs designated as OSD Special Interest IAW reference f or in which the ASD(NII)/DOD CIO has indicated a special interest IAW reference d.

(3) Provide I&S Certification for Non-ACAT and fielded systems to the sponsoring DOD component.

(4) Validate system I&S by posting the J-6 System Validation information in the JCPAT-E after the completion of the I&S Certification and the JITC Joint Interoperability Test Certification.

b. Via the NC FCB, attend all Joint Capability Boards and Joint Requirement Oversight Council meetings to provide Interoperability and Supportability Certification results.

c. Coordinate IT and NSS Interoperability and Supportability policies, procedures and programs with CC/S/As.

d. Conduct MCEB Pub 1 responsibilities (references hh and ii).

e. Designate a POC to act as executive agent of the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) (see Appendix B to Enclosure D).

f. Ensure that USD(AT&L), ASD (NII)/DOD CIO, and other DOD components have the earliest opportunity to participate in or review JCIDS documents and ISPs for Interoperability and Supportability of IT and NSS.

g. Review legacy systems for the NR-KPP.

2. Joint Staff, J-2, will:

CJCSI 6212.01D

8 March 2006

a. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure D.

b. IAW reference jj, conduct the Intelligence Certification of JCIDS documents in a process that is separate, but related to the JCPAT-E process, that examines intelligence support needs for completeness, supportability, and impact on joint intelligence planning. This certification also considers the sufficiency of horizontal integration in accordance with reference kk.

c. Coordinate for combined testing with DISA (JITC) (encouraged to support intelligence certification tests that overlap).

3. Combatant Commanders will:

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

b. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure D.

c. Participate in or support, as appropriate, IT and NSS joint interoperability testing programs (of those which the combatant commander has title 10 Authority) 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 shall be added to the Program Objective Memorandum (POM) and project cost estimates.

d. In coordination with DISA (JITC), develop joint interoperability test and evaluation criteria and/or measures of requirements for inclusion in system acquisition documents, Test and Evaluation Master Plans (TEMP) (Enclosure E), and other test plan submissions.

e. Provide input for the Interoperability Watch List (IAW reference d) based on the observations of the Executive Agent (EA) staff and the Theater Joint Tactical Networks Configuration Control Board (TJTN-CCB) during reviews of the proposed acquisition of systems that must interoperate within the Operational Area Network (OAN) and by monitoring fielded-system and software modifications during the exercise of their configuration-management function.

f. Participate, as appropriate, in the MCEB.

4. US Joint Forces Command (USJFCOM) as the DOD joint force integrator will:

a. Provide IT and NSS Interoperability and Supportability comments to the Joint Staff/J-6 from the warfighter's perspective.

b. Request interoperability demonstrations of selected programs, using the Joint Systems Integration Command (JSIC). These demonstrations do not replace the JITC system interoperability test certification. Demonstration results could be used or provided to JITC to support the Joint Interoperability Test Certification requirements. It may also use Executive Agent for Theater Joint Tactical Networks (EA-TJTN) venues (Joint Users' Interoperability Communications Exercise (JUICE)), Coalition Warrior Interoperability Demonstration (CWID), and DOD Interoperability Communications Exercise (DICE) for system or program interoperability assessments. The Joint Battle Management Command and Control Board of Directors may make selection of the program or system. This does not replace the JITC issued joint interoperability test certification. However, JITC as the Joint interoperability test certifier may elect to use demonstration results to issue the Joint Interoperability Test Certification.

5. US Strategic Command (USSTRATCOM) will:

a. Review programs which will/may interface with national C2 architecture.

b. Review any programs planned to support global strike (kinetic, both nuclear and non-nuclear, and non-kinetic), missile defense, intelligence, surveillance and reconnaissance, information operations, and space operations.

c. As the Joint Task Force for Global Network Operations (JTF-GNO), assist the DISA and NSA review and define information assurance standards.

d. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure D.

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

a. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure D.

b. Document interoperability and supportability needs by developing JCIDS documentation, which includes the NR-KPP as specified in this instruction.

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

- d. Ensure the Program Manager's design conforms to all required DISR mandated GIG KIPs identified in the program's KIP declaration.
- e. Ensure all IT or NSS systems are compliant with current DOD information assurance directives and policies.
- f. Provide guidance to acquisition managers to consider IA certification and accreditation (C&A) requirements early.
- g. Ensure the CDD and CPD NR-KPPs along with other KPPs are used to develop and refine the ISP and the Test and Evaluation Master Plan (TEMP). Further, critical technical and operational issues developed during the CDD/CPD development shall be included in the ISP analysis and defined in the issues Chapter of the ISP as well as considered in the TEMP.
- h. Comply with the requirement for IT and NSS Joint interoperability testing across a system's life cycle 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 shall need to be added to the POM and project cost estimates.
- i. In coordination with DISA (JITC), develop interoperability test and evaluation criteria, measures, and requirements for inclusion in acquisition documents, TEMP, and other test plan submissions. Prior to a fielding decision for all new or modified IT and NSS (regardless of the JPD), the Military Services, Defense Agencies, USSOCOM, and participating test unit coordinators will ensure those systems undergo joint interoperability test and evaluation IAW these criteria. This includes any limited or prototype initial operational capability (IOC) fielding.
- j. For DISA (JITC) standards conformance and Joint Interoperability Test Certification:
 - (a) Coordinate funding with DISA (JITC) 2-3 years prior to a test event (initiation of DISA (JITC) efforts). 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 for 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.
- k. Ensure a TEMP is approved, prior to Key Decision Point B (KDP-B) for space systems being acquired under reference v, to ensure the system will complete interoperability certification testing IAW these criteria. Actual

CJCSI 6212.01D

8 March 2006

certification testing may occur after KDP-B and prior to the first launch and/or prior to declaration of IOC.

l. Provide direction to acquisition managers to ensure that all IT and NSS are certified and tested for interoperability IAW Table 1.

m. Provide guidance to all program managers and Operational Test Agencies (OTAs) to ensure that information assurance hardware and software capabilities are assessed for and meet interoperability and supportability requirements as established by DODI 8500.2 (reference q) and CJCSI 6510.01D (reference ll).

n. Plan funding for I&S Re-Certification.

o. Plan funding for incorporating the NR-KPP for legacy systems into ISPs.

p. Include Mission Area ICD (i.e., GIG MA ICD) requirements that may pertain to the system being developed (search the KM/DS tool for MA ICDs or JCDs). Coordinate with the applicable Functional Capability Board representatives for additional assistance.

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

a. Participate in the technical assessment of all IT and NSS capability documents and/or Information Support Plans.

b. Exercise DISA's role as the DOD executive agent for IT standards (reference mm) including integrating the DISR tenets and their supporting infrastructure activities and capabilities.

c. Ensure that DISR tenets give preference to the use of industry and non-governmental open standards, and that system technical standards profiles (TV-1s) be generated and published through the use of the DISRonline tool on the SIPRNET.¹

d. Update the DISRonline tool to be Core Architecture Data Model (CADM) conformant.

e. Review the technical standards forecast, TV-2, to ensure emerging relevant technologies have been considered.

f. Review Organization Unique Standards (OUSs) to ensure there is no conflict with Joint DISR standards and that they are identified for single-Service use only.

¹ Technical Standards Forecast (TV-2) will be published on line in 2006.

CJCSI 6212.01D

8 March 2006

- g. Provide an assessment of the suitability of standards identified in IT and NSS programs submitted under this instruction.
- h. Establish and conduct, in collaboration with other DOD components, the JITC Joint Interoperability Testing and Certification program for applicable IT and NSS.
- i. Provide developmental interoperability testing assistance to DOD components, agencies and system developers to implement solutions and ensure maximum interoperability and minimum duplication.
- j. Review all available Test and Evaluation Master Plans and provide acquisition managers with recommended interoperability test and evaluation measures; and security certification and accreditation criteria for inclusion in acquisition documents and test plans. Coordinate with National Security Agency (NSA) regarding the inclusion of IA standards.
- k. Post Joint Interoperability Test Certification results to the JCPAT-E in support of the J-6 System Validation.
- l. Provide Interoperability Test Certification results to the MCEB ITP, post these results in the System Tracking Program (STP) and the JCPAT-E.
- m. Notify the J-6 NLT 180 days prior to any Test Certification expiration.
- n. Publish an annual report to the Joint Staff J-6, USD (AT&L), ASD (NII)/DOD CIO, DOT&E, DOD Executive Agent for Space, USJFCOM, Military Services, and Program Offices containing an executive summary of systems tested for IT and NSS interoperability by functional area.
- o. Provide end-to-end (E2E) systems engineering, implementation and technical guidance to identify end-to-end issues and solutions required by individual acquisition programs and have those solutions specified as part of key interfaces to the enterprise infrastructure (e.g. GIG-BE, Teleport). This system engineering provides the specific design guidance needed to ensure that the independently developed component programs of the GIG work in concert to provide an enterprise information environment.
- p. Assist NSA/Central Security Service (CSS) in coordinating and defining tactical signals intelligence (SIGINT) standards and processes and promote security, integration, interoperability, and data sharing among systems.
- q. In coordination with NSA, review and define information assurance standards.

CJCSI 6212.01D

8 March 2006

r. Assist NGA in coordinating and defining Geospatial Intelligence (GEOINT) standards and processes and promote integration, interoperability and data sharing among systems.

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

t. Designate a central office to act as system manager of the JCPAT-E (see Appendix B to Enclosure D).

u. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure C.

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

w. Establish and maintain an automated process to track IT and NSS joint interoperability test and certification status, document Interim Certificate to Operate (ICTO) information, and track uncertified systems.

x. Allocate resources to manage and develop GIG KIPs and testing infrastructure in support of the ASD(NII)/DOD CIO and the Chairman of the Joint Chiefs of Staff.

8. Director, National Security Agency (NSA)/Chief, Central Security Service will:

a. Serve as the Community Functional Lead for Cryptology and coordinate with the appropriate DOD components on matters involving IT and NSS Interoperability and Supportability of Cryptologic systems including US Signals Intelligence Directives (USSIDs).

b. Serve as the DOD Lead for approving and enforcing tactical Signals Intelligence (SIGINT) architectures and standards, coordinate with DOD components and the US Special Operations Command to develop tactical SIGINT architectures and provide standards compliance and interoperability assessment reports to assist Milestone Decision Authorities (MDAs) in acquisition decisions.

c. Ensure that industry and non-governmental standards used for SIGINT and SIGINT systems and applications are open-standards based, and conform to the DISR tenets for interoperability.

- d. Ensure that NSA/CSS IT and NSS programs are certified for standards conformance and IT and NSS interoperability and supportability.
- e. Develop policy and procedures for interoperable and supportable IT and NSS IA and information releasability for joint, combined, and coalition forces and US Government Departments and Agencies.
- f. Ensure that interoperable and supportable IA products are available for the security of NSS.
- g. In cooperation with DISA, identify, evaluate, and select IA and related standards for inclusion in the DISR.
- h. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure D.
- i. Ensure interoperability, supportability, and security of NSA/CSS IT and NSS with those systems that provide direct support to the combatant commanders.
- j. Establish and maintain interoperability and supportability requirements within the IA Component of the GIG Architecture, and ensure their satisfaction through design and development of technical, procedural and operational interfaces between IT and NSS.
- k. Ensure that technical, procedural and operational interfaces are specified and configuration managed in coordination with other DOD components so that US DOD, non-DOD and coalition Cryptologic/Cryptographic systems can interoperate with DOD IT and NSS.

9. Director, National Geospatial-Intelligence Agency (NGA), as the Functional Manager for Geospatial Intelligence (GEOINT) standards, will:

- a. Ensure that National System for Geospatial-Intelligence (NSG) standards and specifications established by NGA for geospatial intelligence support the interoperability and supportability of IT and NSS.
- b. Assist DIA in coordinating and defining (Measurement and Signature Intelligence (MASINT) standards and processes and promote security, integration, interoperability, and data sharing among systems.
- c. Prescribe and mandate standards for all geospatial-intelligence systems and interfaces, including to the Net-Centric Enterprise Services and their accompanying KIPs.

- d. Ensure NSG standards and specifications require imagery and geospatial information to be tagged with metadata containing release or disclosure decisions.
- e. Ensure imagery and geospatial information is tagged with metadata containing release or disclosure decisions in accordance with National System for Geospatial-Intelligence (NSG) standards and specifications.
- f. Ensure that commercial and non-governmental standards used for imagery and geospatial systems and applications are open standards based and conform to DISR mandated standards for interoperability across the NSG.
- g. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure D.

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

- a. Ensure that standards and specifications established for Defense Human Intelligence (HUMINT) support the interoperability and supportability of IT and NSS via coordination with the Military Services and other DOD components, as appropriate.
- b. Assist NGA in coordinating and defining geospatial-intelligence standards and processes and promote security, integration, interoperability, and data sharing among systems.
- c. 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 via coordination with the Military Services and other DOD components, as appropriate.
- d. Ensure that commercial and non-governmental standards used for MASINT systems and applications are open standards based and conform to the GIG and DISR tenets for interoperability.

11. Program Managers from Combatant Commands, Military Services and Defense Agencies, when building new, or modifying existing IT and NSS, will ensure that they are:

- a. Compliant with the NR-KPP (IAW Enclosure D).
- b. Compliant with applicable standards mandated in the DISR and relevant active OUSs identified in the DISRonline.
- c. Identifying and including OUSs within the DISRonline and in the IT Standards profile generated and published through the use of DISRonline.

- d. Compliant with current DOD Information Assurance directives and policies.
 - e. Interoperable with other DOD, Joint and Coalition systems, fully implementing Data Strategy policy, including participating in all applicable Communities of Interest, within security constraints.
 - f. Properly evaluated and certified for interoperability by DISA (JITC) (unless they have obtained an ICTO IAW MCEB Pub 1, as required, until Joint Interoperability Test Certification completion).
 - g. Working with the respective Service Frequency Management Office by submitting an Application for Equipment Frequency Allocation (DD Form 1494) to the Service Frequency Management Office to obtain a spectrum supportability determination for all spectrum dependent equipment (reference j).
 - h. Assessed for overall operational effectiveness prior to the milestone decisions for acquisition programs.
12. Department of the Air Force. As the DOD executive agent for Space, the Under Secretary of the Air Force will review and confirm the sufficiency of the NR-KPP for all for all ACAT, non-ACAT and fielded National Security Space Program systems.
13. DOD Executive Agent for Theater Joint Tactical Networks (EA-TJTN) (Army Chief Information Officer (CIO) G6) will:
- a. IAW reference nn convene and chair the TJTN-CCB).
 - b. Provide a venue for the joint communications community to evaluate the interoperability of proposed tactical networked-communications products, making available assessment vehicles and the ability to conduct coordinated laboratory experiments.
 - c. Review and provide recommendations on the release of new software versions and equipment upgrades to systems to ensure that items affecting interoperability attain or maintain their mutually supporting functionality and do not degrade interoperability conditions.
 - d. Evaluate and provide recommendations on the necessity and extent of interoperability testing required for the certification and integration of approved changes to networked communications and network management system software, hardware, interfacing equipment, or related systems.
 - e. Establish access to the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) in accordance with Appendix B to Enclosure D.

CJCSI 6212.01D
8 March 2006

14. Other DOD Components will:

a. Coordinate on Interoperability and Supportability certification of IT and NSS developed by other sponsors to identify opportunities for cross-component utilization, Joint Integration and harmonization of capabilities.

b. Make recommendations to the J-6 on whether interoperability and supportability capability requirements contained in CDD, CPD, and ISP proposals meet recognized standards.

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

ENCLOSURE C

STAFFING PROCESS AND PROCEDURES

1. General. The Joint Staff J-6 performs an Interoperability and Supportability (I&S) Certification and J-6 System Validation for all IT and NSS programs. CC/S/As submit JCIDS documents to KM/DS IAW CJCSM 3170.01, register the system in the DOD IT Portfolio Repository (DITPR); and develop the program's IT Standards Profile and Forecast (TV-1, TV-2, and OUS) in DISRonline. CC/S/As submit ISPs IAW DODI 4630.8 to the JCPAT-E, register the system in the DITPR; and develop the program's IT Standards Profile and Forecast (TV-1, TV-2, and OUS) in DISRonline.

a. J-6 Interoperability and Supportability Certification

(1) JCIDS Documents. J-8 staffs all JCIDS documents on KM/DS to the CC/S/As. The J-6 reviews the NR-KPP and other IT or supportability related requirements and provides a certification recommendation to the J-8 via the KM/DS tool. J-6 I&S Certification occurs prior to acquisition Milestones B and C. Figure A-1 illustrates the general J-6 Interoperability and Supportability Certification process alignment with JCIDS document coordination and the DOD Acquisition Process.

(2) Information Support Plans (ISPs). IAW the DOD 4630 series, the Joint Staff shall review, certify, and validate sufficiency of the NR-KPP. The J-6 accomplishes this by providing an NR-KPP certification to ASD (NII)/DOD CIO.

b. J-6 System Validation. The J-6 System Validation is intended to provide total lifecycle oversight of warfighter IT and NSS Interoperability and Supportability capabilities. The System Validation occurs after Milestone C upon receipt of JITC's Joint Interoperability Test Certification (valid for three years from date of the test certification letter). The J-6 will update the JCPAT-E to indicate J-6 System Validation.

2. Staffing Process. Documents submitted by CC/S/As 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 achieves J-6 Interoperability and Supportability Certification. To support the I&S certification process, J-6 requests technical assessments from DISA, Services, and other DOD agencies.

a. JCIDS Documents. J-6 Interoperability and Supportability certification is not required for JCDs or ICDs. J-6 certifies IT and NSS CDDs and CPDs for

CJCSI 6212.01D

8 March 2006

Interoperability and Supportability (JROC Interest, Joint Integration). The JITC bases the Joint Interoperability Test Certifications on these certifications. The J-6 staffing process flow follows:

- (1) J-8 staffs JCIDS documents using the J-8 KM/DS tool IAW references a and b.
- (2) DISA transfers JCIDS documents to the JCPAT-E.
- (3) J-6 uses the JCPAT-E to staff the document for Interoperability and Supportability Certification recommendations.
- (4) J-6 compiles these results and posts the I&S Certification on the JCPAT-E.
- (5) DISA posts the I&S Certification on KM/DS.

b. J-6 ISP Staffing Process. CC/S/As upload ISPs in the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) for all ACAT, non-ACAT, and fielded programs IAW references c and d; and this instruction. J-6 provides the appropriate certification (See Table 1) to the ASD(NII)/DOD CIO or sponsoring DOD Component. The sponsoring component will submit the certified ISP to the JCPAT-E.

(1) OSD Special Interest, Non-ACAT, and Fielded IT and NSS ISPs. The process is the same as for the JCIDS documents above, except sponsors submit the ISP to the JCPAT-E vice the KM/DS tool and the final J-6 I&S Certification resides on the JCPAT-E (not KM/DS).

(2) ACAT IT and NSS ISPs. J-6 reviews these ISPs as needed but will not staff or certify ISPs for ACAT programs with associated CDDs or CPDs. The CDD/CPD I&S Certification satisfies the requirement for J-6 ISP NR-KPP certification.

c. Comments

(1) J-6 conducts Interoperability and Supportability Certifications of capability documents in three distinct stages summarized in Table C-1 (references c and d describe the process for ISPs).

(a) O-6 Level Review is the first assessment of JROC Interest Joint Potential Designator (JPD) documents. The Stage I review is the first assessment for Joint Integration JPD documents. Flag or Stage II review will not be required if the adjudication of all comments is accepted by the submitter, J-6, and the Functional Capabilities Board (FCB).

(b) Flag Level Review (for JROC Interest JCIDS documents) or Stage II Review (Joint Integration JCIDS documents) is the second and final

assessment. Flag or Stage II review is not required when comment author, J-6, and the FCB accept the adjudication of all comments during the O-6 level review.

(c) FCB Draft (JROC Interest JCIDS documents) or Final stage (Joint Integration JCIDS documents). Interoperability and Supportability Certifications will be issued upon successful adjudication of all critical comments from the previous two review stages. Sponsors will submit the final or FCB Draft document along with the adjudicated comments resolution matrix (CRM) to the J-8 KM/DS tool (JCIDS documents) for J-6 I&S Certification. Sponsors must, at a minimum, denote whether each comment was accepted, partially accepted, or rejected with rationale for rejecting the comment, the POC name, contact information, and whether or not there was agreement with the program's adjudication. This information will be provided in the "comment" field of the CRM (see Figure C-2).

(2) Combatant commanders are invited to review and comment on all JCIDS and ISP documents during the formal staffing process. Combatant commanders should review these documents for interoperability concerns and include interoperability related comments in the response. 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 and Supportability Certification process.

(3) During the initial stages of a tactical program's introduction, the Theater Joint Tactical Networks Configuration Control Board (TJTN CCB) reviews the program for architectural suitability (reference nn).

(4) Comment Format. Comments should be prioritized as critical, substantive or administrative (see definitions in the Glossary). Convincing support for critical and substantive comments will be provided IAW Figure C-2. Class is short for Classification (codes include U for unclassified, C for confidential, and S for secret) and the Type delineates the comment priority (C for Critical, S for Substantive, and A for Administrative). All comments will include a rewrite recommendation and a rationale.

(5) Comment Resolution. J-6 forwards unresolved Interoperability and Supportability issues to the MCEB or MIB for resolution. The MCEB or MIB will return resolved I&S issues to the lead DOD Component to complete the JROC approval process. The MCEB and MIB ensure that unresolved issues resulting from I&S assessments are presented to the JROC for resolution via the appropriate FCB (see Figure C-1). Unresolved I&S issues will result in

withholding of Interoperability and Supportability Certification.

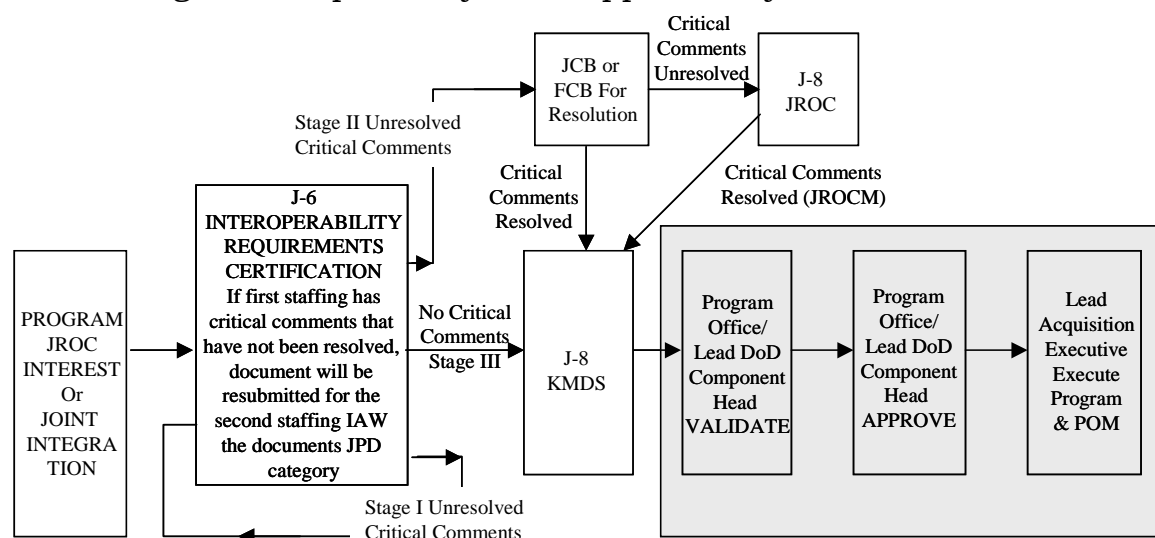


Figure C-1. J-6 Critical Comment Resolution Process

(6) Adjudication Timelines. Table C-1 details the timelines for reviews.

| Document Type | | Stage | Days | Reference | Level | Comments |
|---------------|-----------------------|-------|------|-----------------------|-------|---|
| JCIDS JPD | JROC Interest | I | 21 | CJCSM 3170, (C-7) | O6 | JROCM 100-05 Changes to 21 |
| | JROC Interest | II | 21 | CJCSM 3170, (C-7) | Flag | If Required |
| | JROC Interest | III | 10 | CJCSM 3170, (C-7) | Final | |
| | Joint Integration | I | 21 | CJCSM 3170, (C-10) | O6 | JROCM 100-05 Changes to 21 |
| | Joint Integration | II | 21 | CJCSM 3170, (C-10) | Flag | If Required, Level May be O6 |
| | Joint Integration | III | 10 | CJCSM 3170, (C-10) | Final | |
| | Independent | N/A | N/A | CJCSM 3170, (C-10) | N/A | Follow ISP Timelines |
| | Joint Information | I | 21 | JROCM 100-05 | O6 | If J-8 Directs Review |
| | Joint Information | II | 21 | JROCM 100-05 | Flag | If J-8 Directs Review, If Required |
| | Joint Information | III | 10 | JROCM 100-05 | Final | If J-8 Directs Review |
| ISP | ISP | I | 35 | DODI 4630.8, Page 72 | O6 | |
| | ISP | II | 21 | DODI 4630.8, Page 72 | Flag | |
| | ISP | Final | N/A | DODI 4630.8, Page 72 | Flag | |
| TISP | Tailored ISP | N/A | 30 | CJCSI 6212.01D | O6 | |
| ISP (Pilot) | Initial | N/A | 30 | ASD(NII)/DOD CIO Memo | N/A | Information Support Plan (ISP) Acquisition Streamlining Pilot Program, dated 26 August 2005 |
| | Revised | N/A | 30 | ASD(NII)/DOD CIO Memo | N/A | |
| | Final ISP of Record | N/A | 30 | ASD(NII)/DOD CIO Memo | N/A | |
| | Updated ISP of Record | N/A | 10 | ASD(NII)/DOD CIO Memo | N/A | |

Table C-1: Staffing Timelines

(a) The suspense for completing Stage I and Stage II JCIDS documents is 21 calendar days from the transmittal date to KM/DS. The suspense to J-6 will be posted in the JCPAT-E. Stage II reviews are not required if all comments are resolved during the Stage I review.

CJCSI 6212.01D

8 March 2006

(b) The FCB Draft and Final Stage (Stage III) suspenses are 10 working days following sponsor posting to KM/DS (JCIDS documents) or JCPAT-E (ISPs). In all cases, a minimum of ten working days prior to the FCB Decision brief is required to ensure adequate procedural time for staffing.

(7) Comment Format. Comments should be prioritized as critical, substantive or administrative (see definitions in the Glossary). Convincing support for critical and substantive comments will be provided IAW Figure C-2. Class is short for Classification (codes include U for unclassified, C for confidential, and S for secret) and the Type delineates the comment priority (C for Critical, S for Substantive, and A for Administrative). All comments will include a rewrite recommendation and a rationale.

3. Failure to meet Certification Requirements

a. If a program/system fails to meet or maintain Interoperability and Supportability Certification and/or Joint Interoperability Test Certification requirements, the J-6 may:

(1) Recommend the program not proceed to the next milestone (if currently in the DOD 5000 acquisition process).

(2) Recommend that appropriate funding be withheld until compliance is achieved.

(3) The J-6 will make its recommendation to the USD(AT&L), USD(P), USD(C), USD(I), ASD(NII)/DOD CIO, DOD Executive Agent for Space, the Interoperability Senior Review Panel (ISRP), the Military Communications-Electronics Board (MCEB), and the Joint Requirements Oversight Council (JROC). The J-6 may also request that the program and/or system be added to the ISRP's Interoperability Watch List (IWL) in accordance with reference d.

CJCSI 6212.01D
8 March 2006

| Org / Reviewer | Page # | Para # | Line # | Class (U,C,S) | Type (A,S,C) | Recommendation | Rationale | Comment |
|--|--------|--------|--------|------------------|-----------------|---|--|--|
| Joint Staff J-6 POC Name DSN: 999-9999 email@emailaddress.smil.mil or email@emailaddress.smil | 0 | 0 | 0 | U | C | Add sections 2, 3, 7, 9, and 14. Ensure all sections according to the instruction are titled correctly. | CJCSM 3170.01, Appendix A to Enclosure E. | Interoperability Comment: General: Several sections missing. |
| Joint Staff J-6 POC Name DSN: 999-9999 email@emailaddress.smil.mil or email@emailaddress.smil | 3 | 5.h | 405 | U | C | Include an SV-1 and narrative describing the systems and connectivity providing or supporting system functions. It should show how multiple systems link and integrate and identify key nodes including materiel system nodes, physical connections, association of systems to nodes, circuits, networks, warfighting platforms, and specific parameters. | CJCSI 3170; Mandatory contents of document | Interoperability Comment: Systems Interface Description (SV-1) is missing. |

Figure C-2. Sample Comment Resolution Matrix for JCIDS Documents

CJCSI 6212.01D

8 March 2006

4. Rapid Acquisition, Experimentation, Legacy Systems and Systems that are not subject to DOD 5000 series acquisition requirements. J-6 will review rapid acquisition, experimentation, and other system's ISPs with DISA. JITC Joint Interoperability Test Certifications will be based upon Joint Staff I&S certifications of CDDs, CPDs, and ISPs, or any other J-6 certified interoperability requirements as applicable.

a. These programs may include:

(1) Advanced Concept Technology Demonstrations (ACTDs), Coalition Warfare Program (CW), Defense Acquisition Challenge Program (DACP), Technology Transition Initiative (TTI), Quick Reaction Special Projects (QRSP), Foreign Comparative Testing Program (FCT), Rapid Action Initiative – Net Centricity (RAI-NC), Coalition Warrior Interoperability Demonstration (CWID), Air Force Combat Capability Documents (CCDs), Army Operational Needs Statements (ONSS), Marine Corps Urgent Universal Need Statements (U-UNSS), and Navy Rapid Deployment Capability (RDC).

(2) Technology Insertion: Technology insertion within joint networks involves the introduction, integration, and fielding of emerging or interim technology either with entire systems or through the upgrading of existing systems or their elements within existing networks. It may be an approved commercial-off-the-shelf product or other non-developmental item.

b. Sponsors of any IT/NSS system that is developed and fielded from these programs will develop an ISP IAW references c and d (DOD 4630 series) and this instruction; and submit the ISP to the JCPAT-E. SCI ISPs will be posted on the JWICS. Sponsors may request consideration of use of the Tailored ISP in accordance with Appendix B of this enclosure. Other alternative approaches or processes may include (contact the J-6):

(1) C2IP. J-6 will assist, and specifically advise in the process when the C2IP is recommended as a resource option. In those situations, J-6 will staff, through the relevant C2IP process flow, the associated C2IP request. J-6 will also perform necessary reviews, within the established timelines herein; of information technology/national security systems to ensure that applicable interoperability, supportability, testing, information assurance, and information support plan requirements are implemented or adequately scheduled for implementation.

(2) Joint Urgent Operational Needs (JUONs). CJCSI 3470.01, "Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution," is an avenue for combatant commanders to resource needs in the year of execution. The J-6 coordinates with J-8 to incorporate interoperability and supportability certification, testing, and ISP requirements

CJCSI 6212.01D

8 March 2006

for all programs being developed to satisfy urgent operational needs. As per this instruction, J-6 will enforce the I&S requirements for all IT/NSS JUONs.

(3) Tailored ISP: OSD Memorandum, 26 August 2005, "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," (reference ss) provides a Tailored ISP option for select programs. A Tailored ISP may be produced provided the Component notifies the J-6 via JCPAT-E and receives J-6 concurrence with the program's tailored approach. J-6 coordinates with ASD(NII)/DOD CIO on this concurrence recommendation. Appendix B contains the detailed Tailored ISP request process.

(a) Those programs that have received approval to submit a Tailored ISP, per Appendix B, may tailor NR-KPP integrated architecture views to meet requirements analysis and design synthesis needs of the program.

(b) Architecture views will satisfy the minimum requirements established in paragraph 4c of Appendix B and per further written agreement with the Joint Staff/J-6.

APPENDIX A TO ENCLOSURE C

ISP(C4ISP) ASSESSMENT TOOL

1. General. The Office of the Assistant Secretary of Defense, Networks and Information Integration, ASD (NII)/DOD CIO, reviews all ISP documents for ACAT I and ACAT IA programs, and for other programs in which ASD (NII)/DOD CIO has indicated as special interest. This review is performed on the ISP (C4ISP) Assessment Tool in the JCPAT-E tool suite. The ISP (C4ISP) Assessment Tool supports document submission, assessor review and comment submission, collaborative workspace, and consolidated review comment rollup.

2. This enclosure provides guidance on the use of the ISP (C4ISP) Assessment Tool.

3. Access

a. The ISP (C4ISP) Assessment Tool can be accessed via the SIPRNET at <https://jcpat.disa.smil.mil> or on the NIPRNET at <https://jcpat.disa.mil>. Whenever possible, the SIPRNET should be used for program submissions.

b. A user ID and password are required to use the tool. Potential tool users who require accounts may go to the JCPAT-E home page on the SIPRNET and NIPRNET and follow the instructions for requesting an account.

4. Detailed ISP Review Procedures

a. System Registration within JCPAT-E. The JCPAT-E IT and NSS Registration Number is an important feature that establishes a system/program link to all related information in the Lifecycle Management Repository and Archive, i.e., profile documents, certification memorandums, etc. within the JCPAT-E database. System registration in JCPAT-E is required for all systems/capabilities. During the document submission process, the Program Manager may register a new system if the system does not already appear in the list of registered systems. To register a system, go to SIPRNET URL: <https://jcpat.disa.smil.mil> or NIPRNET URL: <https://jcpat.disa.mil> and click on Register System on the lower left hand side of the screen. Follow the on-line instructions to complete the system registration.

b. ISP Review Process. There are three ISP reviews (an initial, revised, and a final). There is a set of tasks associated with each of these reviews.

(1) The ISP reviews are tied to the acquisition milestones and the system engineering for the program and the decision reviews (preliminary design review (PDR), critical design review (CDR), and final plan submission prior to full-rate production decision review (FRP DR) for the program (See Figure C-1). At subsequent increments (upgrades) additional reviews are conducted. For PDR and CDR there is a similar ISP development cycle that should be scheduled for and completed. The following summarizes each set of tasks for each review.

(a) Initial ISP Review. At Milestone B and PDR: An Initial ISP shall be developed by the PM and submitted to ASD(NII)/DOD CIO via the JCPAT-E in sufficient time to permit completion of a 30-day review prior to the decision review. Upon completion of the Initial ISP review, ASD (NII)/DOD CIO will provide the comments to the PM for use in updating the document. The PM should coordinate responses to the comments with each reviewer during the comment adjudication process. Responses to critical IT support, interoperability or net-centric issues that have been raised during the review shall be briefed at the Milestone B IPT by the PM. Document structure issues shall not be briefed. A completed comment resolution matrix must be submitted to JCPAT-E prior to PDR

(b) Revised ISP Review. Prior to CDR: A Revised ISP shall be developed by the PM and submitted to ASD (NII)/DOD CIO via the JCPAT-E in sufficient time to permit completion of a 30-day review prior to the decision review. Upon completion of the Revised ISP review, ASD (NII)/DOD CIO will provide the comments to the PM for use in updating the document. The PM should coordinate responses to the comments with each reviewer during the comment adjudication process. A completed comment resolution matrix must be submitted to JCPAT-E prior to CDR.

(c) Final ISP Review. Prior to submission of the final ISP of Record, the PM shall submit a final draft of the program's ISP of Record to ASD (NII)/DOD CIO via JCPAT-E for a 10-day final acceptance review by J-2 and J-6, as part of their intelligence; and interoperability and supportability certification processes. Upon acceptance by J-2 and J-6 the PM will obtain a component approval (signed) and submit the ISP of Record to JCPAT-E for posting in the document repository. There is no DOD-level review of the ISP of Record.

(d) At further major system increments: The process is repeated for each major acquisition increment (upgrade).

CJCSI 6212.01D

8 March 2006

(2) Non-ACAT Program ISPs. Non-ACAT program ISPs will be posted to the JCPAT-E ISP assessment tool by the document sponsor and maintained in the JCPAT-E repository. Non-ACAT ISPs will not be staffed by ASD (NII)/DOD CIO) or J-6 to the CC/S/A for their review. The Joint Staff/J-6 will provide an I&S certification and post it on the JCPAT-E.

(3) Fielded System ISPs

(a) ISPs for fielded programs which are managed as an acquisition program per DOD 5000 series guidance will be staffed and certified for Interoperability and Supportability by ASD (NII)/DOD CIO and J-6 IAW the procedures for ACAT ISPs as described above. The only way to receive an I&S Certification is to submit a CPD or ISP.

(b) All other fielded program ISPs (i.e., for three-year Joint Interoperability Test Certification and recertification) will be posted to the ASD (NII)/DOD CIO ISP (C4ISP) JCPAT-E ISP Assessment Tool by the document sponsor and maintained in the JCPAT-E repository. SCI ISPs will be posted on the JWICS by the sponsoring entity. Fielded ISPs will not be staffed by ASD (NII)/DOD CIO or J-6 to CC/S/A for their review. The Joint Staff J-6 will provide the appropriate certification (IAW Table 1) and post it on the JCPAT-E.

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE C

TAILORED INFORMATION SUPPORT PLAN

1. Tailored Information Support Plan (TISP). The purpose of the Tailored ISP process is to provide a dynamic and efficient vehicle for certain programs to produce requirements necessary for Interoperability and Supportability Certification. Select program managers may request to tailor the content of their ISP (reference ss). For programs not designated OSD Special Interest by ASD(NII)/DOD CIO, the Component will make the final decision of the details of the tailored plan subject to the minimums in paragraph 4 (below) and any special needs identified by the J-6 for the Interoperability and Supportability Certification process. The final Component approved plan will be submitted to ISP(C4ISP) Assessment Tool on the JCPAT-E.

2. TISP Pilot Program Waiver Request Process. Waiver requests shall be sent via email to the Joint Staff J-6 through the applicable (Service/Agency/JFCOM) Interoperability Test Panel (ITP) Representative. The request will include: the program's name, the capability it provides, funding allocated to the program, and identification of key connectivity requirements (the NIPRNET website www.jitc.fhu.disa.mil/itp/isp_info.html contains the submission format). The J-6 will respond to the waiver request via e-mail with concur or non-concur. J-6 approval of a TISP Waiver will be contingent on the following:

a. If the mandatory sections of the form are not completed, the request will be returned for completion.

b. The Joint Staff (JS) J-6I Net Readiness Assessment, JCIDS, and Enforcement/Testing Branches shall review the submitted TISP application and make recommendations on including the submission for TISP processing. The J-6I Division Chief retains final approval authority for entry into the Tailored ISP process.

c. Applicants, and respective ISP representatives will be notified via email that they may proceed with completing the TISP.

3. TISP Waiver Request Approval.

a. Components/agencies responsible for ISP development IAW DODI 4630.8 shall comply with applicable portions of the instruction and the

CJCSI 6212.01D

8 March 2006

Tailored ISP Program. All TISP requests will be submitted through the appropriate CC/S/A ITP Representative to the J-6 using the form provided at www.jitc.fhu.disa.mil/itp/isp_info.html. The appropriate CC/S/A ITP Representative shall validate the TISP request.

b. Upon Component/Agency approval, the TISP will be submitted to J-6I for review and approval. J-6I will coordinate with ASD(NII)/DOD CIO on all submissions.

c. As required, J-6I will invite the requesting system's Program Management Office (PMO) or designated representative to the next scheduled ITP meeting to brief the members concerning the system and the justification for requesting TISP versus the DODI 4630.8 ISP procedures. The ITP will serve as an advisory panel to facilitate J-6I determination of system merits and means to mitigate Interoperability and Supportability Certification issues.

d. As the pilot program is intended to accelerate the Joint Interoperability and Supportability Certification and Validation process, programs should make early contact with the Joint Interoperability Test Command (JITC) to create a testing strategy and gain technical POCs for questions dealing with ISP testing.

4. Tailored ISP Content. The tailored plan will provide:

a. An explanation of the program's Concept of Operations (CONOPs).

b. IT supportability analysis of the CONOPS.

c. The following Integrated Architecture Products: AV-1, OV-1 (optional), OV-5, OV-6c (optional), SV-1 (optional), SV-5, SV-6, and TV-1. The J-6 determines if optional reviews are required.

d. Remaining Interoperability and Supportability requirements IAW Enclosure D and references c and d.

5. TISP I&S Certification. TISP I&S Certification and Validation is IAW Table 1, Table C-1, and Enclosure D.

ENCLOSURE D

DETERMINING INTEROPERABILITY, SUPPORTABILITY, AND NET-READINESS

1. This enclosure provides the J-6 Interoperability and Supportability Certification procedures. The recommended format for submission of NR-KPP documentation is provided in Appendix A, Appendix B includes procedures for developing the TV-1 and TV-2, and Appendix C includes the J-6I assessors checklist.

a. Inclusion of the NR-KPP is mandatory for all acquisition and post acquisition IT and NSS programs for systems used to enter, process, store, display, or transmit DOD information, regardless of classification or sensitivity, except those that do not communicate with external systems. Non-acquisition programs must also comply in accordance with DODD 4630.5 (reference c) and DODI 4630.8 (reference d).

b. Migration strategies to achieve the NR-KPP are no longer accepted.

c. Documentation of the four NR-KPP components is required for Interoperability and Supportability Certification. Additional criteria for determining interoperability and supportability are described below.

2. Interoperability and Supportability Certification

a. JCIDS and ISP Document Considerations

(1) Joint Capability Document (JCD) and Initial Capabilities Document (ICD). The NR-KPP is not required in and Interoperability and Supportability Certification is not provided for these capability documents.

(2) Capability Development Documents (CDDs). All CDDs for systems that exchange information with external systems will be evaluated and certified for Interoperability and Supportability based on the criteria listed in the following section. In this context external system means any system outside the scope of the program referenced in the CDD.

(3) Capability Production Documents (CPDs). All CPDs for systems that exchange information with external systems will be evaluated and certified for I&S based on the criteria listed in the following sections. In this context, 'external systems' means any system outside the scope of the program referenced in the CPD. The NR-KPP produced in the precursor CDD shall be refined with greater detail and form a completed integrated architecture to characterize the capabilities and performance of the proposed production

system. The architectural products must include any descriptions necessary to explain the system's operation and should be traceable between the views.

(4) Information Support Plans (ISPs). J-6 certifies the NR-KPP in all ISPs and provides the results to the sponsor and NII. Additionally, ISPs must address spectrum supportability IAW DODI 4630.8, Enclosure 4 (reference d).

(5) For each lifecycle development activity, IAW references f and r, there is a corresponding set of security activities that shall verify compliance with the security requirements and evaluate vulnerabilities (may consider those vulnerabilities identified in the System Threat Assessment Report (STAR)).

3. Components of the Interoperability and Supportability Certification Process

a. Net-Ready Key Performance Parameter. The NR-KPP is 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 consists of measurable, testable, or calculable characteristics and/or performance metrics required for the timely, accurate, and complete exchange and use of information.

b. The NR-KPP must be included in all CDDs, CPDs, and ISPs, describing systems that send and/or receive information with external systems. This documented NR-KPP shall be used in analyzing, identifying and describing IT and NSS interoperability, and test strategies in the Test and Evaluation Master Plan (TEMP) in accordance with sound systems engineering practices. Programs should synchronize documentation from the capabilities documents down through acquisition documentation including the TEMP, Systems Engineering Plan (SEP) and the Acquisition Program Baseline (APB).

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

(1) Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW RM)

(2) Integrated Architecture Products

(3) Compliance with Applicable Key Interface Profiles

(4) Compliance with DOD Information Assurance Requirements

d. The following table summarizes the four technical compliance elements of the NR-KPP and where they apply within JCIDS and Acquisition documentation:

| Document | NCOW RM Compliance | Integrated Architecture Products (IAW DODAF) | | | | | | | | | | | | | | | | KIP Compliance | IA Compliance |
|----------|--------------------|--|------|------|------|------|------|-------|------|------|------|------|------|------|-------|------|------|----------------|---------------|
| | | AV-1 | OV-1 | OV-2 | OV-3 | OV-4 | OV-5 | OV-6C | OV-7 | SV-1 | SV-2 | SV-4 | SV-5 | SV-6 | SV-11 | TV-1 | TV-2 | | |
| JCD | | | | | | | | | | | | | | | | | | | |
| ICD | | | X | | | | | | | | | | | | | | | | |
| CDD | X | X | X | X | 1 | X | X | X | 2 | | X | X | X | X | | X | 2 | X | X |
| CPD | X | X | X | X | 1 | X | X | X | 2 | | X | X | X | X | 2 | X | X | X | X |
| ISP | X | X | X | X | | X | X | X | X | | X | X | X | X | X | X | X | X | X |
| TISP | X | X | 3 | | | | X | 3 | | 3 | | | X | X | | X | | X | X |
| X | | Required | | | | | | | | | | | | | | | | | |
| Note 1 | | The OV-3 is not assessed as part of the NR-KPP review; however, normally the OV-3 is used to develop other architecture documents and can be included with the NR-KPP documentation to assist in development and conduct of the testing. | | | | | | | | | | | | | | | | | |
| Note 2 | | OV-7, SV-11, and TV-2 are required only when applicable. | | | | | | | | | | | | | | | | | |
| Note 3 | | TISP OV-1, OV-6c, and SV-1 may be waived by Joint Staff/J6-I | | | | | | | | | | | | | | | | | |

Table D-1. NR-KPP Products Matrix

e. The four NR-KPP elements along with other Interoperability and Supportability Certification requirements should be documented as an appendix to the CDD, CPD, and ISP. This CDD/CPD appendix can also be used for the analysis required in the ISP. See Appendix A for a recommended format.

(1) The NR-KPP Compliance Statement in Table D-2 provides the NR-KPP Threshold and Objective Values.

CJCSI 6212.01D
8 March 2006

| KPP | Threshold (T) | Objective (O) |
|---|---|---|
| Net-Ready: The system must support Net-Centric military operations. The system must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability. | The system must fully support execution of joint critical operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for transition to Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs identified in the KIP declaration table, 3) NCOW RM Enterprise Services 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Approval to Operate (IATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing specified in the applicable joint and system integrated architecture views. | The system must fully support execution of all operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs identified in the KIP declaration table, 3) NCOW RM Enterprise Services 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Approval to Operate (ATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing specified in the applicable joint and system integrated architecture views. |

Table D-2. NR-KPP Compliance Statement

(a) The threshold value is determined by analysis of the system's integrated architectural views as follows:

1. The joint critical mission threads for the system will be documented in OV-6Cs and should be identified as threshold or objective. The joint critical mission threads are determined by the sponsor's analysis of the system's required capabilities and other Key Performance Parameters. The associated joint critical operational activities required to perform these joint critical mission threads are documented in text with the OV-5.

2. The joint critical operational activities are traced through the integrated architectures from OV-6Cs to OV-5, SV-5, SV-4, SV-6, and finally TV-1. Since DODAF does not currently provide a method to identify joint critical operational activities, the text describing each view must identify these activities as they are traced.

3. The DOD IT standards are identified in the TV-1 by tracing from the SV-TV bridge and SV-6 products.

4. The NCOW RM activities are identified in the appropriate architecture views by tracing from the joint critical mission threads.

5. The GIG KIPs are identified using the SV-6 and SV-4 by tracing from the joint critical mission threads to determine the appropriate media and method of system data exchange. Analysis of the GIG KIPs and the external system data exchanges will identify the appropriate GIG KIPs.

6. The system data exchanges and mission critical performance attributes are identified in the SV-6 by tracing from the critical mission threads. The following are examples of these attributes: Periodicity, Criticality, Timeliness, and Size.

7. Include a discussion of the threshold information assurance requirements and information assurance attributes associated with the threshold system data exchanges shown in the SV-6 and derived from the joint critical mission threads. The following are examples of these attributes: IA – Access Control, IA – Availability, IA – Confidentiality, IA – Dissemination Control, IA – Integrity, IA – Non-Repudiation Consumer, and/or IA – Non-Repudiation Producer.

(2) Compliance with the NCOW RM (<https://disain.disa.mil/ncow.html>) and DOD Net-Centric Data Strategy (<http://www.defenselink.mil/nii/doc>).

(a) The NCOW RM (reference m), depicted in Figure D-1 (top-level activity model decomposition), describes the activities required to establish, use, operate, maintain and manage the net-centric enterprise information environment to include: the user-interface, the enterprise information environment services (core services, Community of Interest (COI) services, and environment control services), and the enterprise management components. It

also describes a selected target set of key standards that will be needed as the NCOW capabilities of the GIG are realized. Future versions of the NCOW RM will integrate elements of the IA Component of the GIG. The NCOW RM represents the objective end-state for the GIG. 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.

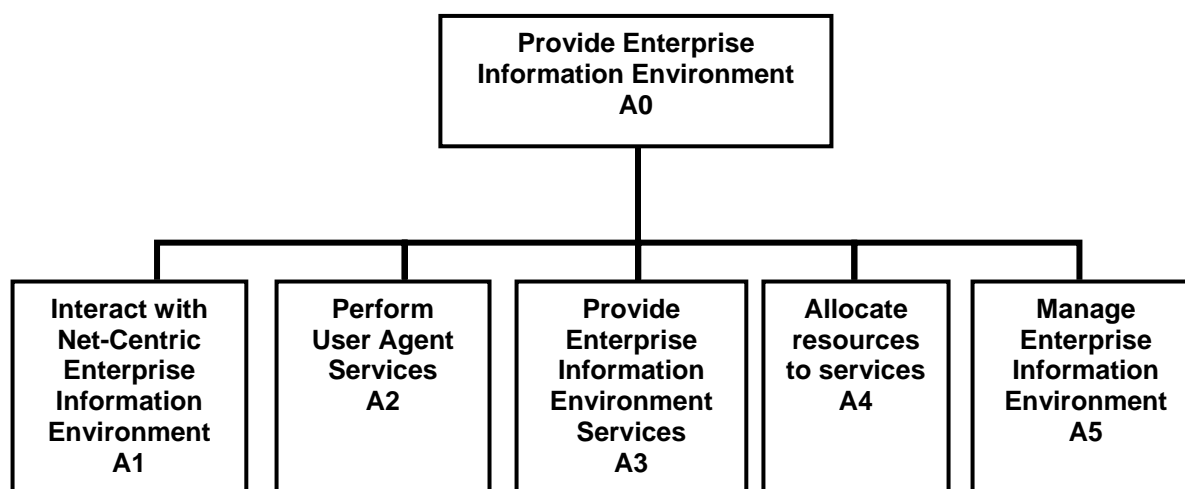


Figure D-1. NCOW RM Top Level Activity Model Decomposition

(b) 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.

(c) The program must comply with the NCOW RM in four ways:

1. Use the NCOW RM common language, lexicon (dictionary of terms), and taxonomy (structure of the information) in developing the architecture products.
2. Incorporate and/or account for the NCOW RM operational capabilities and services provided or demonstrate equivalence in its materiel solution.

3. Assess the value of the NCOW RM's emerging information technologies to the program's architecture relative to achieving DOD's net-centric, investment planning, and information superiority goals.

4. Comply with the DOD Net-Centric Data Strategy for all net-centric services and data shared at the enterprise level.

a. The DOD is moving to net-centric operations. The vision is that all elements of the DOD are networked and able to seamlessly share information, resulting in dramatic improvements in operational effectiveness. CDDs, CPDs, and ISPs will document compliance with the DOD Net-Centric Data Strategy as identified in references m, w, and x.

b. Verification of compliance with the DOD Net-Centric Data Strategy (reference x) will be accomplished through the analysis of the sponsor provided architecture products with accompanying text detailing the program's compliance strategy. Additional verification may include analysis against the DOD Metadata Registry (<http://metadata.dod.mil>); and the DOD COI Directory (<https://gesportal.dod.mil/sites/coidirectory/>). All enterprise level shared data should be tagged and associated metadata properly registered. Documentation (in integrated architecture products or other forms) must clearly identify all net-centric services and data delineated by COI(s), domain, and enterprise mission area.

c. DOD Net-Centric Data Strategy. DODD 8320.2 is the codification of the DOD Net-Centric Data Strategy.

(1) Compliance with the DODD 8320.2, "Data Sharing in a Net-Centric Department of Defense" December 2, 2004 (<http://www.dtic.mil/whs/directives/corres/dir2.html>) and the DOD Net-Centric Data Strategy (<http://www.defenselink.mil/nii/doc/>) is an essential prerequisite of net-centric operations.

(a) Data shall be made visible, accessible, and understandable to any potential user in the Department of Defense.

(b) Data assets shall be made visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset.

(c) Data assets shall be made accessible by making data available in shared spaces.

(d) Data assets shall be made understandable by publishing associated semantic and structural metadata in a federated DOD metadata registry.

(e) Data assets shall have associated information assurance and security metadata, and an authoritative source for the data shall be identified when appropriate.

(f) Data interoperability shall be supported by making data assets understandable and by enabling business and mission processes to be reused where possible.

(g) Semantic and structural agreements for data sharing shall be promoted through communities (e.g., communities of interest (COIs)), consisting of data users (producers and consumers) and system developers, in accordance with reference x.

(2) COIs will be registered in the ASD (NII)/DOD CIO COI Directory. The COI Directory provides visibility of COIs by enabling registration of pertinent COI information that is discoverable by other COIs and interested parties. The directory is at: <https://gesportal.dod.mil/sites/coidirectory>. Users will need a DOD issued PKI client certificate (for assistance see <http://gesnew.dod.mil/obtainPKI.html>).

(3) Data will be made visible by tagging it with DOD Discovery Metadata Specification (DDMS) compliant metadata and posting it to a catalog. Data tags will include metadata extensions to the DDMS defined by the appropriate COI. Semantic and structural metadata will be registered in the DOD Metadata Registry, located at: <http://diides.ncr.disa.mil/mdregHomePage/mdregHome.portal>. The DDMS is available at: <http://diides.ncr.disa.mil/mdreg/user/DDMS.cfm>.

(4) CDDs, CPDs, and ISPs will include the Logical Data Model (OV-7) and CPDs will include the Physical Schema (SV-11) if the system being described collects, processes, or uses any shared data not prescribed by NCES or KIP use (includes database systems). The SV-11 should include any metadata namespace (examples include XML or XHTML schemas) in the DOD Metadata Registry that documents data standards used by the proposed system. Verification of compliance with the DOD Net-Centric Data Strategy will be accomplished through the analysis of the integrated architecture products and accompanying textual description and testing. Additional analysis may include analysis against the DOD Metadata Registry (<http://metadata.dod.mil>); or the DOD COI Directory (<https://gesportal.dod.mil/sites/coidirectory/>).

(3) Integrated Architecture Products. A key component of NR-KPP documentation is the supporting integrated architecture description.

(a) An integrated architecture consists of three major perspectives or views (operational, systems, and technical standards) that logically combine to describe a program's architecture. The architecture is integrated when the data elements defined in one view are the same as architecture data elements

referenced in another view. Each of the three views depicts certain architecture attributes. Some attributes bridge two views and provide integrity, coherence, and consistency to architecture descriptions. They ensure the materiel solution set matches the proposed capabilities and that the relationships are understood.

(b) Architecture descriptions assist DOD in understanding the linkages between capabilities and systems and in making appropriate acquisition decisions.

(c) The DODAF (reference n) defines a common approach for DOD architecture description development, presentation, and integration for both warfighting operations and business operations and processes. It ensures that architecture descriptions can be compared and related across organizational boundaries, including Joint and multinational boundaries.

(d) Architecture development begins with a clear understanding of the capability or capabilities desired and the concept of operations, defined as a verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations.

1. The operational view describes the tasks and activities, operational elements, and information exchange required to conduct operational operations. Architecture view development begins with describing the tasks and activities, operational elements, and information exchanges required to accomplish the specified mission in the operational views.

2. The systems views, which flow from the operational views, describe the systems and their interconnections providing for, or supporting, DOD functions. The SV associates systems resources to the operational views, supports the operational activities, and facilitates the exchange of information among operational nodes.

3. The technical standards view (TV) provides the minimal set of rules, standards, and protocols governing the arrangement, interaction, and interdependence of system parts or elements. The TV includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture.

4. The overarching aspects of an architecture that relate to all three of the views are captured in the All-Views (AV) products. The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and timeframe for the architecture. The setting in which the architecture exists comprises the interrelated conditions that compose the context for the architecture. These

conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

5. An architecture description is integrated when products and their constituent architecture data elements are developed such that architecture data elements defined in one view are the same (i.e., same names, definitions, and values) as architecture data elements referenced in another view. There are common points of reference linking the OV and the SV and also linking the SV and the TV. For example, SV-5 relates operational activities from OV-5 to system functions from SV-4; the SV-4 system functions are related to systems in SV-1. In addition the operational needlines identified in the OV-2 are related to the interfaces and the performance attributes in the SV-6, and the performance attributes and specifications resident in the TV-1.

6. Integrated architecture products provide detailed descriptions of the system in the operational, system, and technical standards views. Included in the description should be discussion of the analysis used to create and integrate the various products. The architecture products should provide enough detail to describe the system and its interfaces with external systems to enable the assessment of end-to-end operational effectiveness. Systems not immediately interfacing with the subject system do not need to be shown in the architecture products and if they are shown, should be identified as outside the boundaries of the system. Additional information on completing the architecture products is located in Appendix A.

7. Information Technology Standards. IT and NSS must comply with applicable information technology standards mandated in the current DISR for all information exchanges internal to DOD. This includes conformance with standards and technical standards profiles identified in the NCOW RM, KIPs (known and sufficiently defined during the current acquisition phase of the program), etc. Late emerging KIPS and standards requiring substantive integration effort or capability redesign may be considered for waiver by the MDA, but should be incorporated into the next appropriate acquisition and PPBE cycle.

8. Completion of the IT Technical Standards Profile (TV-1). A system IT technical standards profile will be completed, published, and maintained in the SIPRNET JCPAT-E DISR Online module.

9. The TV-2 will be included to identify emerging standards that the program intends to use and to identify issues affecting program implementation (e.g. impacts of commercially available equipment or development of another program). The TV-2 is generated by DISRonline (see Appendix B of Enclosure D for details). The architecture views must include needlines, interfaces, exchanges, and attributes identified in the DODAF for the

views and must note whether items are critical or enterprise level, for determining the KPP threshold and objective values.

10. Architecture products will be Core Architecture Data Model (CADM) conformant and will be posted in an (a DOD) accessible online architecture repository. The exception to this requirement is the TV-1 and TV-2 developed and published on DISRonline. Architecture products should still be included as part of the document submission so that reviewers without DOD Architecture Repository System (DARS) access can review the products. Program Managers should consider adding a statement to their architecture development statement of work requiring the contractor to deliver CADM conformant architecture products (with the exception of the TV-1 and TV-2) in machine readable form.

11. Table D-3 describes the architecture products (IAW reference n) to document the required capability and assess information exchange and net-readiness. This table provides a general description of the purpose of each architecture product. Table D-1 and DODAF guidance identify the required products that shall be used in the NR-KPP.

| Framework Products | Framework Product Name | General Description |
|--------------------|--|---|
| AV-1 | Overview and Summary Information | Scope, purpose, intended users, environment depicted, analytical findings |
| OV-1 | High-Level Operational Concept Graphic | High-Level graphical/textual description of operational concept. |
| OV-2 | Operational Node Connectivity Description | Operational Nodes, operational activities performed at each node, connectivity and information exchange need lines between nodes |
| OV-3 | Operational Information Exchange Matrix | Information exchanged between nodes and the relevant attributes of that exchange. |
| 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. |
| OV-7 | Logical Data Model | System data requirements and structural business process rules of the Operational View |
| SV-1 | System Interface Description | Identification of systems nodes, systems, and system items and their interconnections, within and between nodes. |
| SV-2 | System Communications Description | Systems nodes and their related communications lay-downs |
| 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. |
| SV-11 | Physical Schema | Physical implementation of Logical Data Model entities, e.g. message format, file structures, physical schema |
| TV-1 | Technical Standards Profile | Extraction of standards that apply to the given architecture, including information assurance functions. Note: The TV-1 must be completed in DISRonline and included in the NR-KPP annex. |
| TV-2 | Technical Standards Forecast | Emerging standards, which are not currently approved. The TV-2 should also be used to document technical issues affecting program implementation (e.g. non-availability of JTRS radios). |

Table D-3. Architecture Products Descriptions

1. The following figure, Figure D-2, describes the required linkages between NR-KPP attributes, integrated architecture products, and performance metrics, which are necessary to assess the NR-KPP.

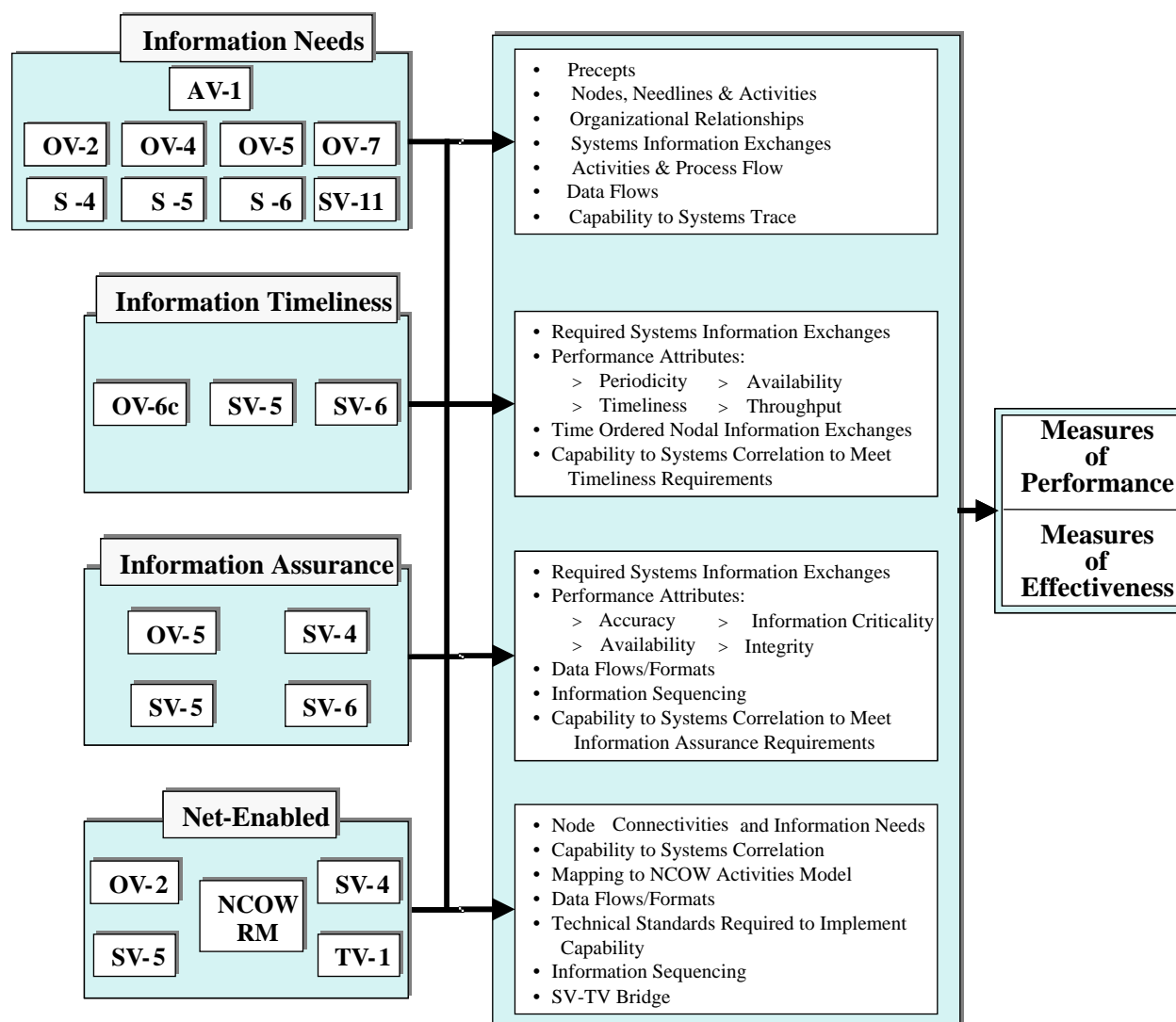


Figure D-2. Architecture Linkage to NR-KPP Attributes

(4) GIG Key Interface Profiles (KIPs). In light of the scope of the GIG environment, a form of enterprise-level integration management is needed to facilitate interoperability and testing at the seams of GIG components. Formally designated GIG KIPs offer organizations and system builders a set of managed technical interface specifications on which to converge. This brings visibility and stability to these critical interfaces, while freeing the GIG components to innovate on either side of the interface. GIG KIPs are applicable to all functional proponents, software developers, operators and users of IT and NSS systems, and encompass requirements pertaining to data, physical and logical interfaces, communications, service levels and security. GIG KIPs are

used to communicate the technical specifications and implementation of standards of the key interface.

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

1. Describes an interface with the GIG.
2. Details the key interface architectural, interoperability, test, and security attributes documenting KIP characteristics in conjunction with solution sets.

(b) A mandated GIG KIP consists of:

1. Refined operational and systems view products.
2. The technical specification of the applicable DISR standards implementation options and settings governing the key interface external presentation

1. Technical Standards Profile (TV-1) with specifications to bridge the Systems View to the Technical View

2. Technical standards forecast (TV-2).

3. Procedures for standards conformance testing

(c) A GIG KIP is associated with an interface to a network or between one or more systems. GIG KIPs are applicable to both the consumer and the provider of the service. Both the consumer and provider have responsibilities listed in Table D-4. GIG KIPs life cycle includes emerging and mandated phases.

| | Consumer Responsibilities | Provider Responsibilities |
|----------|---|--|
| Emerging | <ul style="list-style-type: none"> Identify possible use of key interfaces Plan for implementation of GIG KIPs Plan and program for testing of GIG KIPs | <ul style="list-style-type: none"> In coordination with DISA, support the GIG KIP detailed development in accordance with the KIP configuration management guide. Assist JITC in creating the test strategy for GIG KIPs |
| Mandated | <ul style="list-style-type: none"> Identify applicable GIG KIPs using the Table D-A-2 of Appendix 1, Enclosure D Implement the system IAW the applicable GIG KIPs Conduct KIP compliance testing | <ul style="list-style-type: none"> Adhere to enterprise configuration management of key interface In coordination with DISA, maintain the GIG KIPs in accordance with the KIP configuration management guide If requested by JITC, provide an instantiation of the key interface to JITC for testing. |

Table D-4. KIP Consumer and Provider Responsibilities

(d) A program complies with GIG KIPs by identifying relevant GIG KIPs in CDDs, CPDs, and ISPs, developing the program in accordance with the technical standards specifications in the KIP, and performing GIG KIP compliance testing. GIG KIPs shall be identified during the development of the CDD, CPD, and ISP. KIP compliance shall be verified during standards conformance and interoperability testing, which can be performed by JITC or performed by the program (in coordination with JITC). When a GIG KIP becomes mandated it will have an effective date. When completing CDDs, CPDs, and ISPs, programs will identify applicable, mandated GIG KIPs to establish a baseline for standards conformance testing and for meeting this portion of the KPP.

(e) The Chairman of the Joint Chiefs of Staff and DISA shall continue the development of the GIG KIPs according to the process outlined in Figure D-2. Key interfaces are defined as part of the capability development process. The appropriate FCB or Mission Area Lead (in the case of a COI enterprise service interface) will designate a capability as providing a key interface when it meets the following criteria:

- The interface spans organizational boundaries
- The interface is mission critical
- The interface is difficult or complex to manage

- There are capability, interoperability, or efficiency issues associated with the interface
- The interface impacts multiple acquisition programs
- The interface is vulnerable or important from a security perspective
- Very large set of point-to-point interfaces already exists or has the potential to emerge
- The number of current and potential providers and/or consumers of the services offered via the interface is large

(f) Key interfaces of the GIG are identified by the Joint Staff or appropriate Mission Area governance forum for COI enterprise services. Once the GIG KIP is identified, the Information Technology Standards Committee (ITSC) will designate an appropriate sponsor or program office for the key interface. DISA will develop the KIP in cooperation with the designated sponsor or program office. The KIP will be designated as emerging in DISR during development and will be coordinated with JITC for validation. Once completed, the Information Technology Standards Oversight Panel (ISOP) will approve the GIG KIP and it will become mandated in the DISR. Programs must identify, comply, and conduct compliance tests on applicable mandated GIG KIPs. The GIG KIPs will all include an effective date, after ISOP approval. The CDD, CPD, and ISP will include a list of mandated GIG KIPs, which each program will build to and conduct testing against. KIPs will continue to evolve and new KIPs will be identified, developed and approved over time. However, the CDD, CPD and ISP form KIP baselines, which do not change as additional GIG KIPs are mandated unless the ISOP approves an exception to policy requiring the newly mandated GIG KIP to be implemented immediately by all programs. Programs can choose to update their list of applicable GIG KIPs as necessary to include additional mandated GIG KIPs. These program-directed KIP baseline changes will be documented when the next CPD or ISP comes due, but KIP baseline changes alone do not require a separate I&S recertification. The GIG KIPs are maintained to accurately reflect evolving GIG interface standards and will be updated as the GIG and its enterprise services mature. DISA will maintain the list of emerging and mandated GIG KIPs as part of DISR and also on the web site: <http://kips.disa.mil>.

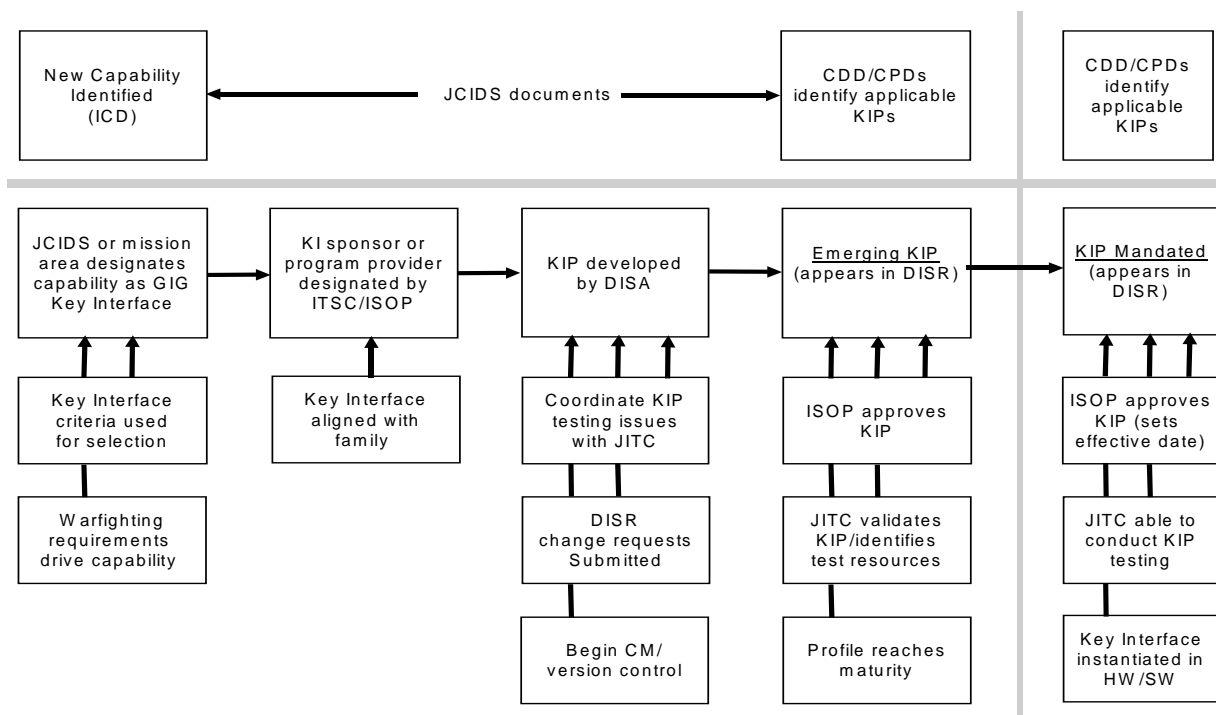


Figure D-3. KIP Development Process

(5) Information Assurance. Information assurance (IA) is a critical element in the GIG. The Department employs a defense-in-depth strategy to establish and maintain an acceptable IA posture across the GIG. Protection mechanisms shall be applied to minimize system and information vulnerabilities, such that information and information systems maintain the appropriate level of availability, integrity, authentication, non-repudiation based on mission assurance category, and confidentiality level, while maintaining the level of interoperability essential to the GIG. IT or NSS program managers/sponsors integrate information assurance into the acquisition life cycle as outlined in Defense Acquisition Guidebook (reference aa) paragraph 7.5.3.

(a) The CDD must:

1. Describe how the system will implement IA policies and procedures IAW the most current policies and procedures contained in references p through u and bb through dd; as well as references ee and ff for SCI and Special Access Programs. If encrypted key (including PKI) technology is required, include a statement that encrypted key technology will be acquired as part of this effort and will be installed and used, including initial fielding

efforts, to ensure information security over all voice, video, and data transmission.

2. Sponsors must certify compliance with IA requirements by including in the CDD an IA statement of compliance reading, "This program or system will be in full compliance with the IA requirements in DOD 8500 series and CJCS 6510 series directives, instructions and manuals." When published, the DIACAP DOD Instruction 8510, now in draft will supersede 5200.40. Include the point of contact information for accreditation decision documentation (e.g. Security System Authorization Agreement (DITSCAP) or implementation plan (DIACAP)² accreditation decision or other supporting documentation. For Intelligence Community (IC) and non-DOD products and systems interconnecting with DOD products systems, the applicable IA requirements of DCID 6/3 (reference ff) for IC, and NIST SP 800-53 (reference pp) (for non-DOD) must also be met.

(b) The CPD must:

1. Describe in greater detail how the production system implements the IA policies and procedures cited in the CDD IAW the most current policies and procedures contained in references p through u and bb through dd; as well as references ee and ff for SCI and Special Access Programs. If encrypted key technology is required, include a statement that encrypted key technology will be acquired as part of this effort and will be installed and used, including initial fielding efforts, to ensure information security over all voice, video, and data transmission.

2. Program managers must certify compliance with IA requirements by including an IA statement of compliance reading, "This program or system is in full compliance with the IA requirements in DOD 8500 series and CJCS 6510 series directives, instructions and manuals." Include the point of contact information for accreditation decision documentation (e.g. Security System Authorization Agreement (DITSCAP) or implementation plan (DIACAP)³ accreditation decision or other supporting documentation.

(c) Sponsors and program managers must demonstrate achievement of IA 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. IA requirements shall be identified and included in the architecture design, acquisition, installation, operation, upgrade, or replacement of all DOD IT and NSS in accordance with references p through u and bb through dd as well as references ee and ff for SCI and Special Access Programs. Interoperability and integration of IA solutions within or supporting the DOD shall be achieved

² Upon approval of DODI 8510.

³ Upon approval of DODI 8510.

through adherence to the DOD Architecture Framework (<http://www.defenselink.mil/nii/doc/>) including the IA Component of the GIG Architecture.

(d) IAW DODI 8580.1 (reference r), sponsors shall ensure that each assigned DOD information system has a designated Information Assurance Manager (IAM) with the support, authority and resources to satisfy the responsibilities established in DODI 8500.2 (reference q) and implement the DITSCAP for assigned DOD information systems. Ensure that information system security engineering (ISSE) is employed to develop the IA component of the system architecture in compliance with the IA component of the GIG Architecture and to make maximum use of enterprise IA capabilities and services including verifying compliance with the security requirements and evaluate vulnerabilities, for each lifecycle development activity where there is a corresponding set of security activities. Sponsors must provide J-6 documentation that each phase of the Defense Information Technology Security Certification and Accreditation Program (DITSCAP), has been completed throughout the phases of the JCIDS/acquisition process. The DITSCAP phases include Definition, Verification, Validation, and Post Accreditation.

(e) IT and NSS, including commercial and non-developmental items, must comply with applicable DOD Information Assurance and Critical Infrastructure policies and regulations/instructions and Director Central Intelligence Directives (DCIDs). This includes implementation of encrypted key when required to ensure information security over all voice, video, and data transmission. Interconnection of systems operating at different classification levels will be accomplished by processes approved by the DOD Chief Information Officer (CIO) in conjunction with DIA, DISA and NSA CIO's. IA will be an integral part of all net-readiness efforts thus allowing appropriate security measures to protect mission data and system resources from all known threats (references o, s, and bb). A thorough description must be included of how subject IT and NSS comply with each applicable policy and regulation/instruction to meet the requirements of this element of the NR-KPP.

(6) Additional Interoperability and Supportability Certification Requirements

(a) Sponsors are encouraged to use an integrated, automated suite of tools for developing and documenting system architecture and other NR-KPP related information. System NR-KPP information, and an appropriate tool suite, must be available for CDD, CPD, and ISP review and interoperability testing purposes. Note that this may require the sponsor to obtain additional user licenses and make tools available online in some situations. NR-KPPs shall also be submitted in machine-readable form, and the PM/sponsor will coordinate with reviewers (e.g., J-6) and testers (e.g., JITC) to ensure that

appropriate automated tools are available for processing and analyzing system NR-KPP information.

1. Submissions of documents (CDDs, CPDs, and ISPs) shall be accompanied by machine-readable copies of the NR-KPP package and identification of associated online files (e.g., DISRonline system profile, DARS files). Names and version identification and location (e.g., URL) shall be provided for machine-readable information as part of document submissions (e.g., a CPD submission should identify the associated DARS files, DISRonline entry, etc).

2. A consistent naming convention shall be used to the extent practicable for all machine readable information associated with a program/system. The naming convention (for databases and other files, including online entries) will identify the program/system/subsystem (system component), increment, configuration management information (e.g., date, version identification), and status (e.g., draft). Machine-readable information will be "locked" to the extent practicable upon submission of a documentation package, so that all sources of information (i.e., documents, database entries, computer files, etc.) will remain in sync for a given version. Any modifications to databases, online entries, etc. after submission of a documentation package shall be made to a new instance (i.e., a different copy), which shall be identified with an appropriate change in version identification of the item.

(b) IT and NSS must comply with Defense Critical Infrastructure guidance to ensure availability of DOD and non-DOD networked assets critical to project, support, and sustain military forces and operations worldwide (reference cc).

(c) Spectrum Supportability Policy (DODD 4650.1) and Electromagnetic Environmental Effects (E3) control (DODD 3222.3).

1. The spectrum supportability process includes national, international, and DOD policies and procedures for the management and use of the electromagnetic spectrum. This process ensures the following:

a. The spectrum-dependent system/equipment being acquired is designed to operate within the proper portion of the electromagnetic spectrum;

b. Permission has been (or can be) obtained from designated authorities of sovereign ("host") nations (including the United States) to use that equipment within their respective borders; and

c. The newly acquired equipment can operate compatibly with other spectrum-dependent equipment already in the intended operational environment (electromagnetic compatibility).

2. The objective of establishing E3 control requirements early in the acquisition process is to ensure that DOD equipment, subsystems, and systems are designed to be self-compatible and operate compatibly in the operational electromagnetic environment. E3 control applies to the electromagnetic interactions of both spectrum-dependent and non-spectrum-dependent objects within the operational environment. Examples of non-spectrum-dependent objects that could be affected by the electromagnetic environment are ordnance, personnel, and fuels. The increased dependency on and competition for portions of the electromagnetic spectrum have amplified the likelihood of adverse interactions among sensors, networks, communications, and weapons systems.

3. All IT and NSS systems must be mutually compatible with other systems in their electromagnetic environment and not be degraded below operational performance requirements due to electromagnetic environmental effects (reference i).

4. All IT and NSS must comply with reference DODD 4650.1, "Policy for Management and Use of the Electromagnetic Spectrum" (reference j). Spectrum supportability and E3 control requirements must be addressed IAW CJCSM 3170.01, as briefly outlined below.

a. At or During Concept Refinement – a Stage 1 (Conceptual) request for a spectrum supportability determination (i.e., a DD Form 1494) must be submitted prior to the Milestone (MS) A. If a determination has not been received by MS A, then a plan to obtain Spectrum supportability must be submitted concurrently with the initial MS B Information Support Plan (ISP).⁴

b. By Technology Development – a Stage 2 (Experimental) spectrum supportability determination must be obtained prior to the Technology Development Stage. If a spectrum supportability determination has not been obtained, DODD 4650.1 requires that specific authority be received from the Milestone Decision Authority (MDA) for the program to proceed into the System Development and Demonstration phase and to provide to the USD(AT&L), the ASD(NII), the DOT&E, and Chair, MCEB, a justification and plan to obtain spectrum supportability.

c. By System Development and Demonstration – a Stage 3 (Developmental) spectrum supportability determination must be obtained prior to Milestone B decision. If a spectrum supportability determination has not been obtained, DODD 4650.1 requires that specific authority be received from

⁴ The DD Form 1494 must be releasable to the Host Nation(s) (HN) to where the equipment will be deployed.

8 March 2006

the MDA for the program to proceed into the Production and Deployment phase and to provide to the USD(AT&L), the ASD(NII), the DOT&E, and Chair, MCEB, a justification and plan to obtain spectrum supportability.

d. By System Production and Deployment – a Stage 4 (Operational) spectrum supportability determination must be obtained prior to Milestone C decision. If a spectrum supportability determination has not been obtained, DODD 4650.1 requires that specific authority be received from the MDA for the program to proceed into the Production and Deployment phase and to provide to the USD(AT&L), the ASD(NII), the DOT&E, and Chair, MCEB, a justification and plan to obtain spectrum supportability.”

5. All IT and NSS must be compliant with other regulatory documents for spectrum supportability and certification such as the “Manual of Regulations and Procedures for Federal Radio Frequency Management” (a.k.a. “NTIA Redbook”), Office of Management and Budget (OMB) Circular A-11 (Part 2, section 33.4), and other documents listed in this instruction. While not required, it is highly recommended that Program Managers also reference section 7.6, “Electromagnetic Spectrum,” of the Defense Acquisition Guidebook (reference aa) where additional information including detailed Milestone requirements, additional mandatory policies, timelines, sample wordings for documents, and other specific requirements for gaining spectrum supportability are covered. Adherence to these guidelines will alleviate problems, expedite the process and is intended to help the Program Manager’s Office meet the intent of DODDs 3222.3 and 4650.1.

6. All proposed IT and NSS systems that include spectrum-dependent hardware must document spectrum certification of the hardware (reference j).

7. Commercial and non-developmental items must also comply with DOD policy on (E3) and Spectrum Supportability (references i and j).

8. Host-Nation Approval (HNA). To ensure compatibility as well as interoperability, all IT and NSS with equipment intended for operation in host nations will require HNA coordinated by the MCEB and the appropriate combatant commanders prior to use.

9. Hazards of Electromagnetic Radiation to Ordnance (HERO). All proposed IT and NSS should be assessed to determine their effects on all electro-explosive devices (ordnance) when the item is employed in IT and NSS radio frequency environments.

10. Ordnance containing electrically initiated devices (EIDs) will be compatible with the operational electromagnetic environment and will not be degraded by E3 (reference i).

11. Ordnance must be integrated into platforms, systems, and equipment to preclude safety problems and unintentional detonation when exposed to the operational electromagnetic environment (reference i).

12. IT and NSS documents (CDDs, CPDs and ISPs) must contain a spectrum compliance statement. An example spectrum compliance statement is provided below:

“Spectrum Supportability. Procurement or acquisition of this wireless, spectrum dependent device will be conducted IAW DOD guidance (e.g., DODD 3222.3, DODD 4650.1, DODI 4630.8, DODD 5000.1 and DODI 5000.2) as well as applicable MILDEP publications. A request for spectrum supportability assessment (i.e., DD Form 1494) was (will be) initiated on (date). The DD Form 1494 was (will be) releasable for coordination purposes to those foreign countries (host nations) in which permanent deployment or lengthy temporary use is contemplated. The program manager (PM) acknowledges that, before assuming contractual obligations for deployment, testing, production, or procurement of this spectrum dependent system, the required spectrum support is or will be available in those host nations determined by the PM or procurer for the equipment’s intended use. The PM has (will develop) a plan to obtain appropriate equipment allocation guidance/status prior to MS B or MS C as outlined in DODD 4650.1 in order to progress to the next phase.”

13. While not required in the ICD, spectrum supportability should be obtained as soon as possible and the ICD is one of the earliest opportunities to start that process. Program managers should consider including a statement similar to the following:

“This system will comply with DOD, national and international spectrum management policies.”

(d) Joint Tactical Radio System (JTRS). All future requirements for radio-based communications will be satisfied by the approved current JTRS requirements document unless ASD(NII)/DOD CIO grants authorization for a specific procurement. Authorization will be granted in accordance with reference qq. Under no circumstance will new research and development activities for any radio systems, to include software reprogrammable radio technologies, which may supplant the current JTRS program of record, be conducted.

(e) Selective Availability Anti-Spoofing Module (SAASM). All programs must comply with CJCSI 6140.01, which directs specific measures to protect GPS. Include a statement on how the program complies with CJCSI 6140.01.

(f) Tactical Data Link (TDL) Implementations. DOD has the joint family of TDL message standards, which includes Link 16, Link 22, Variable

CJCSI 6212.01D

8 March 2006

Message Format (VMF), etc. Interfaces employing TDL are joint interfaces. Joint Mission Area interoperability assessment of TDL participants requires identification of platform TDL implementation details at the bit level. For example, for Link 16 include the Data Field Identifier/Data Use Identifier and Data Item implementation. This detailed implementation information will be included in the I&S certified requirements document (usually the CPD).

CJCSI 6212.01D
8 March 2006

APPENDIX A TO ENCLOSURE D
RECOMMENDED NR-KPP DOCUMENTATION FORMAT

APPENDIX ____

CLASSIFICATION OR UNCLASSIFIED

NR-KPP

FOR

TITLE OF PROGRAM/SYSTEM

This appendix provides an example format for the NR-KPP documentation. The NR-KPP documentation should be developed as an appendix to the CDD or CPD. Each subparagraph should be numbered to facilitate correlation and traceability and for ease of identifying issues during staffing. The architecture products should be produced to be CADM conformant so they can be loaded into analysis tools.

1. NR-KPP Statement

| KPP | Threshold (T) | Objective (O) |
|---|---|---|
| Net-Ready: The system must support Net-Centric military operations. The system must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability. | The system must fully support execution of joint critical operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for transition to Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs identified in the KIP declaration table, 3) NCOW RM Enterprise Services 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Approval to Operate (IATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing specified in the applicable joint and system integrated architecture views. | The system must fully support execution of all operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs identified in the KIP declaration table, 3) NCOW RM Enterprise Services 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Approval to Operate (ATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing specified in the applicable joint and system integrated architecture views. |

Table D-A-1. NR-KPP Compliance Statement

2. Net-Centric Operations and Warfare Reference Model (NCOW RM)

Compliance Statement

a. Describe in the architecture products the NCOW RM activities, applicable to the system to establish, use, operate and manage the system capabilities within the net-centric enterprise information environment to include: the user interfaces, the intelligent-assistant capabilities, the net-centric service capabilities, and the enterprise management components.

b. The program's description and architecture products will comply with the taxonomy and lexicon of NCOW concepts and terms, and architectural descriptions of NCOW concepts. It must also comply with the NCOW RM activities, services and standards required to establish, use, operate, and manage the net-centric enterprise information environment (EIE) to include the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities, and the enterprise management components.

c. Clearly identify the following NCOW RM activities performed by the system/program:

(1) Activities conducted by system to access the Net-Centric Enterprise Services (NCES) and use the services/capabilities.

(2) Activities performed by the system or within the NCES to provide assistance to system and invoke services.

(3) Activities performed by the system or within NCES to provide services/capabilities.

(4) Activities that locate, activate, and connect the resources upon which the system and NCES operate.

(5) Activities performed by the system or within the NCES to architect, plan, engineer, provision and manage the environment.

d. Comply with the DOD Net-Centric Data Strategy and DODD 8320.2 Data Sharing in a Net-Centric Department of Defense requirements and intent. Make explicit the data that is produced and used by the program's implemented operations and that is to be shared with the user community. Provide the associated metadata, and define and document the program's data models. These requirements are met by performing the following actions. If not completed, indicate the extent to which progress has been made, or provide a plan to meet the requirement.

(1) At a minimum, the logical data models (LDMs) should include the logical entity types, the data attributes describing those entities, and the relationships between the entities.

(2) The Physical Data Models (PDMs) should contain the organization's database naming standards, data schema, data types, data tables, data columns of those tables, and the relationships between the tables. The detail varies depending on the complexity of the program's data requirements. PDMs must show greater detail, including associative tables required to implement the associations as well as the keys needed to maintain the relationships.

(3) List the Communities of Interest (COIs) and the COI POC (name, org, email, phone number) in which the program participates and which publish the metadata/taxonomies/vocabularies used by the program.

(4) Report the status of COI metadata tagging including DDMS compliant discovery metadata, associated information assurance and security metadata and authoritative sources for the data.

(5) Report the status of data asset tagging with DDMS and COI extensions and XML component tagging.

(6) Report the status of registering structural and semantic metadata in the DOD Metadata Registry, including COI extensions to DDMS. Provide representative samples of registry entries.

(7) Identify other shared spaces (registries, catalogs, repositories, etc.) where program data and semantic and structural metadata are posted. Provide names and URLs of the shared spaces.

(8) Identify web services that the program is developing and where the services and their associated metadata are registered.

3. Mandatory Integrated Architecture Products. Develop the mandatory integrated architecture products in accordance with the DOD Architecture Framework (DODAF). The mandatory integrated architecture products shall be consistent with existing joint integrated architectures developed for the missions/capabilities the system supports in a SoS or FoS context. When the joint integrated architecture has not been sufficiently developed, the system's integrated architecture products shall conform to the overarching Global Information Grid integrated architecture for interoperability assessment.

a. Ensure architecture data element tables are provided for each product, providing definitions of the metadata (i.e., the architecture data types that comprise the products).

b. Ensure architecture products are CADM conformant (each product is represented in a CADM XML document that can be loaded into DARS and other CADM conformant architecture tools and databases) as required by the DODAF. The exception to this requirement is the TV-1 and TV-2 developed and

published on DISRonline. DISRonline is moving towards CADM conformance and still contains the most up to date standards. The architecture views must still be included in the document.

c. Comply with the DODAF requirements in producing architectural products. This requirement is met by producing a complete integrated architecture using the specified products described in the DODAF and having it assessed for accuracy, consistency, and sufficiency with respect to its intended use (e.g., capability definition, process re-engineering, investment decisions, and integration engineering).

d. Ensure that all information exchanges specified in architecture products are measurable and testable. When needed to insure measurability and testability of information exchanges, include mandatory SV-6 performance attributes (such as periodicity, criticality, timeliness, and size).

e. Architecture products need to show information exchanges with both external systems and Net-Centric Core Enterprise Services (NCES).

4. Key Interface Profiles (KIPs) Declaration. Recognizing that the KIPs and IT standards will evolve over time, the list of applicable emerging and mandated KIPs will change. Use the most recent version of the table below, which can be found at <http://kips.disa.mil>. Uniquely identify the KIP, including the KIP version. Use the applicable column to identify if the KIP is applicable to the program. State whether the KIP is emerging or mandated as posted on the DISR. State whether this KIP will be implemented as part of the threshold or objective value of the NR-KPP. Also, identify the associated interfaces and include KIP implementation statement information. The statement, similar to the implementation statement for a standard, expands on the declaration to include an explanation of how well the design complies with an individual KIP. It identifies optional elements that are implemented, known deviations, and any necessary configuration details. The KIP statement alone does not ensure interoperability; a system must also be designed against the appropriate architectures and DOD DISR and IA standards. An example KIP declaration is provided in the following table:

| Key Interface Family/Name | Ver | Applicable (Yes or No) | DISR Status (Emerging or Mandated) | Implementation Phase (Objective or Threshold) | Consumer or Provider | Implementation Issues/KIP Options |
|---|-----|------------------------|------------------------------------|---|----------------------|-----------------------------------|
| Transport Family | | | | | | |
| UHF SATCOM | | | | | | |
| X-Band SATCOM | | | | | | |
| C-Band SATCOM | | | | | | |
| Ku-Band SATCOM | | | | | | |
| Ka-Band SATCOM | | | | | | |
| EHF SATC OM | | | | | | |
| AEHF SATCOM | | | | | | |
| MUOS | | | | | | |
| GPS | | | | | | |
| Unsecure voice | | | | | | |
| Secure voice | | | | | | |
| Video teleconferencing | | | | | | |
| Non Class IP Network | | | | | | |
| Secure IP Network | | | | | | |
| JIS | | | | | | |
| GBS | | | | | | |
| IBS | | | | | | |
| JTIDS | | | | | | |
| Tactical Wireless Multiband | | | | | | |
| CENTRIXS | | | | | | |
| Computing Infrastructure Family | | | | | | |
| NetOps | | | | | | |
| Applications Staging | | | | | | |
| Computing Infrastructure | | | | | | |
| Content Staging | | | | | | |
| Application Enterprise Services Family | | | | | | |
| Content Discovery | | | | | | |
| Service Discovery | | | | | | |
| Service Security | | | | | | |
| Service Messaging | | | | | | |

Table D-A-2. Example KIP Declaration Table

5. Information Assurance Compliance Statement. Provide the contact information for all the information assurance documentation described in Enclosure D along with an information assurance compliance statement. An example Information Assurance Compliance statement follows:

“This program or system will be in full compliance with the IA requirements in DOD 8500 series and CJCS 6510 series directives, instructions and manuals.” Change “will be” to “is” for CPD.

APPENDIX B TO ENCLOSURE D

TECHNICAL STANDARDS PROFILE AND FORECAST

1. General. The JCPAT-E DISRonline module enables Component Program Managers (PM) to develop Technical Standards Profiles (TV-1), Technical Standards Forecasts (TV-2), and OUS in compliance with the applicable standards contained in the DISRonline. The TV-1 is required as a supporting JCIDS predecessor document for all CDDs, CPDs and ISPs.

2. Access

a. The JCPAT-E DISRonline module for creating and publishing a TV-1, TV-2 and OUS profiles shall be accessed via the SIPRNET at <https://jcpat.disa.smil.mil>.

b. A user ID and password are required to use the tool. Potential tool users who require accounts may go to the JCPAT-E home page on the SIPRNET (Request Account) and follow instructions for requesting JCPAT-E access, which shall also allow access to the DISRonline module.

3. Background. DISRonline provides users with an easy method to identify the applicable DOD Mandated, Emerging, Retired, and Organization Unique standards, and helps them build a TV-1, TV-2, and OUS profiles through analysis of their IT and NSS Capability/System requirements.

4. Requirements

a. DISRonline shall be used to develop and publish all TV-1s, TV-2s, and OUSs referenced in JCIDS documents and ISPs.

b. All CDDs, CPDs, and ISPs will have a current TV-1 and TV-2, which is published in the JCPAT-E DISRonline module on the SIPRNET (Check for new versions published between reviews; the DISR is refreshed every four months).

c. The PMs or sponsor may cite additional standards within a capabilities document that are not mandated in the DISR, however the following conditions must be met.

(1) Prior to Milestone B, the PM or sponsor shall, for each non-cited

standard, either include a waiver or submit change request(s) (CR) into DISRonline NIPRNET (<https://disronline.disa.mil>). In addition the PM or sponsor will identify, in Appendix A of the CDD or Chapter II of the ISP, the date that the CR was submitted. An Interim Standards Acknowledgement (ISA) of non-cited standards and their corresponding CR will be addressed during the routine assessment of the TV-1 with its CDD or (Stage I or Initial) ISP documents. The ISA will be provided in the assessor comments.

(2) Prior to Milestone C decision, CPD and (Stage II or Revised) ISP documents that identify standards not contained in the DISR will require a waiver.

d. Waivers for non-cited standards must be obtained in accordance with DOD Instruction 4630.8 from the Component Acquisition Executive, Component CIO or cognizant official.

e. PMs will provide notification in JCIDS and ISP documents that they have obtained waivers or an ISA for all standards not mandated in DISR that are used in their TV-1.

f. For Milestones B and C. PMs will develop a technology insertion risk assessment for all waived standards included in their TV-1. Standards that have received an ISA will not require a Technology Insertion Risk Assessment. This Technology Insertion Risk Assessment will be included as an individual attachment to JCIDS and/or ISP documents.

(1) Risk Assessment for Using Retired Standards. The risk assessment for selecting "Retired" standards for the TV-1 shall identify all approved waivers, describe the cost, schedule or performance risk associated with implementing the retired standard in place of a mandated standard and, within their mitigation plan, include a migration strategy for transitioning from the retired standards included in the TV-1 to applicable mandated standards.

(2) The risk assessment for using emerging standards in favor of, or in the absence of, a mandated standard shall describe the cost, schedule or performance risk impacting the program in the event that the selected emerging standards implemented do not transition in the future to a mandated status in the DISR.

5. Technical Standards Profile/Forecast (TV-1 and TV-2) Development.

a. CDD and (Stage I or Initial) ISP Preparation of TVs for Milestone B. The document sponsor, with appropriate system and IT Standards subject matter experts (SME), using the DISRonline tool and profile building privileges will begin the development of a TV-1 and TV-2 for review and subsequent J-6 interoperability assessment. Mandated standards should be used in the TV-1.

Retired standards identified in the TV-1 shall be accompanied by a waiver. It is preferred that Emerging standards be placed in the TV-2. The PM or sponsor can add an Emerging standard to their TV-1, however this will require that they enter a Change Request into DISRonline NIPRNET for each applicable standard. The PM or sponsor will then make a statement in the CDD or ISP document that all applicable Change Requests have been entered into DISRonline NIPRNET. The PM or sponsor may then be granted an ISA. This ISA will not be valid for future associated CPD or (Stage II or Revised) ISP. If Emerging standards are placed in the TV-1 without an associated Change Request, then a waiver is required. Standards not cited in the DISRonline but contained in the CDD or (Stage I or Initial) ISP will be treated like Emerging standards and will require either a waiver or that a Change Request be submitted into the DISRonline on the NIPRNET. In addition an appropriate statement in the JCIDS or ISP document will be required.

(1) Producing the TV-1 and TV-2. A TV-1 and TV-2 residing in the DISRonline application on the SIPRNET shall be referenced in CDDs being submitted via JROC KM/DS and ISPs submitted via JCPAT-E.

(a) The TV-1 and TV-2 must be built using one or more of DISRonline's profile building methods. During the building process the TVs can be saved as system profiles. Prior to publishing, these system profiles can only be seen by the PM or sponsor, and their designated profile builders (emerging standards will be placed automatically in the TV-2 upon publication).

(b) If KIPs are being used by the PM or sponsor, then applicable Mandated KIP standards must be included in the system profiles. Upon completion of the system profile, the PM or sponsor shall publish the system profile as a TV-1 and TV-2. During the publishing process:

1. Mandated and retired standards will be placed into the TV-1, the PM or sponsor can choose to add Emerging or Retired standards to the TV-1 but these standards will require a Change Request or waiver as indicated in paragraph 5.a. above. All remaining Emerging standards that have not been placed in the TV-1 will be put in the TV-2.

2. The PM or sponsor will be required to publish them as a TV-1 and TV-2. This will require the PM or sponsor to assign a JCPAT-E system registration number and a system classification to the TVs. Once the TVs are published, all DISRonline users can publicly view the most recent versions.

3. The PM or sponsor will be required to assign a JCPAT-E system registration number and a system classification to the TV-1 and TV-2. Once the TVs are published, all DISRonline users can publicly view the most recently published version.

(2) Change Requests for Non-Mandated Standards. PMs or sponsor shall submit a Change Request in DISRonline (NIPRNET) and acknowledge in the CDD or (Stage I or Initial) ISP that they have submitted a Change Request for any Emerging or other standard not mandated in the DISR that is contained in their CDD or (Stage I or Initial) ISP by entering the Change Request number and the date that the Change Request was submitted.

(3) DISR-Retired Standards Waivers. In lieu of submitting a change request, the PM or sponsor will acknowledge in DISRonline SIPRNET and in the CDD or (Stage I or Initial) ISP that they have obtained a waiver for any Retired standard that is contained in their TV-1 by entering the approval authority and the date that the waiver was granted.

(4) Technology Insertion Risk Assessment. The use of a retired or other standard not mandated in DISR will require completion of a technology insertion risk assessment. This document must be submitted with its corresponding CDD into the KM/DS tool during the JCIDS process. Risk attributes that should be discussed in the risk assessment include: value/benefits gained, evaluation (high, moderate, low), mitigation, and impact.

b. CPD and (Stage II or Revised) ISP Preparation of TVs for Milestone C. IT Standards contained in the DISR are initially confirmed for a system when the TV-1 developed for a CPD or ISP is subsequently assessed for I&S. Once the TV-1 developed in DISRonline is completed, the PM or sponsor will publish it in DISRonline.

(1) TV-1 and TV-2 Refinement. The PM or sponsor, with appropriate system and IT Standards subject matter experts (SME), using the DISRonline tool and profile building privileges and previously developed CDD and ISP TVs, will generate refined TV-1 and TV-2 in the DISRonline application on the SIPRNET that shall be referenced in the CPDs (and ISPs) being submitted via JCIDS KM/DS (or JCPAT-E).

(2) Producing a TV-1 and TV-2 for a CPD or ISP. A TV-1 residing in the DISRonline application in the SIPRNET is required. In addition a TV-2 is required for a CPD and is optional for an ISP. The TV-1 and TV-2 shall be referenced in the applicable CPDs and ISPs submitted via the JROC KM/DS tool or JCPAT-E.

(a) TV-1s for CPDs shall be developed using the TV-1 published previously with the CDD as a starting point. The PM or sponsor will then update the previously developed TV-1 using one or more of DISRonline's profile building methods.

(b) For ISPs where no prior TV-1 has been developed, a system profile shall be developed in a manner similar to TV-1 development for a CDD.

PMs or sponsors should pay special attention to other published TV-1s created for systems that they are required to interoperate with.

(c) If KIPs are being used by the PM or sponsor, then applicable standards referenced in the KIP must be included in the system profile. Upon publishing the system profile, mandated and retired standards will be placed into the TV-1 and emerging standards will be placed into the TV-2.

(d) Once the new system profile is completed, the PM will be required to publish it as a TV-1 and TV-2. This will require the PM to assign a JCPAT-E system registration number and a system classification to the TVs. Once the TV-1 is published, all SIPRNET DISRonline users can publicly view the most recent TV-1. The PM will store the published TV-1 and TV-2 in DISRonline according to its corresponding JCPAT-E system registration number.

(3) DISR Standards Waivers. PMs or sponsors will acknowledge in DISRonline on the SIPRNET and in the CPD or Stage II ISP that they have obtained a waiver for any Emerging, Retired or other standard not mandated in DISR by entering the approval authority and the date that the waiver was granted.

(4) Technology Insertion Risk Assessment. The use of any Retired or other standard not mandated in the DISR in a TV-1 will require a risk assessment to address the status of prior waivers and any new waivers approved since J-6 certification of the CDD. This document must be submitted with its corresponding CPD into the KM/DS tool during the JCIDS process. For ISPs where no prior TV-1 has been developed, the use of any retired standards in a TV-1 also will require completion of a risk assessment. This document must be submitted as an individual attachment to the ISP. Risk attributes that should be discussed in the risk assessment include: value/benefits gained, evaluation (high, moderate, low), mitigation, and impact. Refer to the TISP for information on risk assessments associated with Technology Insertions.

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

APPENDIX C TO ENCLOSURE D

INTEROPERABILITY AND SUPPORTABILITY ASSESSOR'S CHECKLIST

General. The intent of Table D-C-1, the Interoperability and Supportability Assessor's Checklist, is to provide guidelines for J-6 assessors in certifying the NR-KPP in acquisition documents and ISPs. It does not supersede or negate requirements listed in this instruction and in the references. Programs are not required to submit or use this checklist.

| Item # | References | Criteria | TISP ⁶ | ISP ⁶ | JCD | ICD | CDD | CPD | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------|--|-------------------|------------------|-----|-----|-----|-----|--|---|
| 1 | Encls D | Net-Ready Key Performance Parameter (NR-KPP) Statement. (Assessor: J-6I) | X | X | | | X | X | | |
| 2 | m | Net-Centric Operations and Warfare Reference Model (NCOW RM) Compliance (Assessor J-6I) | | | | | | | | |
| 2.1 | m, u | a. DOD Architecture Framework (DODAF). All DOD architectures are expected to comply and conform to the NCOW RM by: | | | | | | | | |
| 2.11 | | (1) Common NCOW RM definitions and vocabulary used. | X | X | | X | X | X | | |
| 2.12 | | (2) The capabilities and services described in the NCOW RM have been incorporated. | X | X | | | X | X | | |
| 2.13 | | (3) The IT/NSS standards identified in the NCOW RM have been incorporated. | X | X | | | X | X | | |

Table D-C-1. Interoperability and Supportability Assessor's Checklist

⁵ Reference = Location in this Instruction or Reference identified in Enclosure F

⁶ The TISP column is provided as information only for the assessors in the J6 to review, certify and validate the NR-KPP. The governing documents for the ISP and TISP are DODI 4630.8 and DOD Memorandum "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," dated 26 August 2005.

CJCSI 6212.01D

8 March 2006

| Item # | Reference # | Criteria | T I S P 6 | I S P 6 | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|-------------|---|-----------------------|------------------|-------------|-------------|-------------|-------------|--|---|
| 2.2 | | b. Net-Centric Operations and Warfare Reference Model (NCOW RM). Architectures must fully integrate the following key aspects of the NCOW RM: | | | | | | | | |
| 2.21 | | (1) Interaction with the Net-Centric Information Environment: Organizations in the Enterprise interact using the GIG and the services provided by net-centric services. | X | X | | | X | X | | |
| 2.211 | | (a) Services provided and performed by the information environment: The reference model describes the services that are provided to users or performed by the information environment. These services, found under the A2-Perform Net-Centric User/Entity Services and A3-Provide Net-Centric Services, consist of three categories: Core Services, COI Services, and Environment Control Services. Knowing what these services are and what they bring to the table, is essential for architects to incorporate them into architecture development and optimize use of the services. | X | X | | | X | X | | |
| 2.212 | | (b) The TPPU vision: TPPU (task, post, process, and use). Architects should incorporate and reflect this concept throughout their architectures. Posting information before processing supports discovery and storage services, and then publish and subscribe concept. | X | X | | | X | X | | |
| 2.213 | | (c) Target Technical | X | X | | | X | X | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference ⁵ | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------------------|---|-------------------------------|--------------------------|-------------|-------------|-------------|-------------|--|---|
| | | View: The Target Technical View is an integral part of the NCOV RM as an addendum to the DISR. It identifies key standards (protocols) and frameworks that play an important role in enabling net-centricity and that are common throughout the GIG. These standards and frameworks focus on interoperability for information sharing and network operations. The systems associated with any architecture should reflect these standards to ensure interoperability. | | | | | | | | |
| 2.214 | | (d) Data management strategy: Net-centricity is dependent upon the ability to locate and retrieve information and services regardless of where they are stored. Common strategy for data management that is incorporated into the architectures of all COIs and shared space providers. (See DOD Net-Centric Data Strategy, 9 May 2003). | X | X | | | X | X | | |
| 2.3 | m, w, x | <u>DOD Data Strategy Implementation.</u> | | | | | | | | |
| 2.311 | x | a. Is the program a member of any Communities of Interest (COIs)? | | | | | X | X | | |
| 2.312 | | b. Does the program provide adequate evidence that it is tagging data with DDMS compliant metadata (including associated information assurance and security metadata and authoritative sources), and posting it on the DOD Metadata Registry? | | | | | X | X | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference ⁵ | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------------------|---|-------------------------------|--------------------------|-------------|-------------|-------------|-------------|--|---|
| 2.313 | | c. Was a representative sample of the tagged data assets with discovery metadata and COI extensions provided? | | | | | X | X | | |
| 2.314 | | d. Does the program show that it is has registered structural and semantic metadata with the DOD Metadata Registry? | | | | | X | X | | |
| 2.315 | | e. Is the registered metadata published by a COI? | | | | | X | X | | |
| 2.316 | | f. Does the program address the requirement to post data and metadata to shared spaces for users to access? | | | | | X | X | | |
| 2.317 | | g. If the program is developing/maintaining services, is the appropriate metadata stored in registries or catalogs? | | | | | X | X | | |
| 2.318 | | h. Are these COIs registered in the DOD COI Directory? | | | | | X | X | | |
| 3 | | Mandatory Integrated Architecture Products: (Assessor: J-6I) | | | | | | | | |
| 3.1 | n | a. Architecture Products | | | | | | | | |
| 3.11 | | (1) AV-1 | X | X | | | X | X | | |
| 3.121 | | (2) OV-1 | X | X | | | X | X | | |
| 3.122 | | (3) OV-2 | | X | | | X | X | | |
| 3.123 | | (4) OV-3 ⁷ | | | | | X | X | | |
| 3.124 | | (5) OV-4 | | X | | | X | X | | |
| 3.131 | | (6) OV-5 | X | X | | | X | X | | |
| 3.132 | | (7) OV-6C | X | X | | | X | X | | |
| 3.133 | | (8) OV-7 | | | | | X | X | | |
| 3.141 | | (9) SV-1 | X | | | | | | | |
| 3.142 | | (10) SV-2 | | X | | | X | X | | |
| 3.143 | | (11) SV-4 | | X | | | X | X | | |

⁷ The OV-3 is not assessed as part of the NR-KPP review; however, normally the OV-3 is used to develop other architecture documents and can be included with the NR-KPP documentation to assist in development and conduct of the testing.

CJCSI 6212.01D

8 March 2006

| Item # | Reference # | Criteria | T I S P 6 | I S P 6 | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|-------------|---|-----------------------|------------------|-------------|-------------|-------------|-------------|--|---|
| 3.144 | | (12) SV-5 | X | X | | | X | X | | |
| 3.145 | | (13) SV-6 | X | X | | | X | X | | |
| 3.146 | | (14) SV-11 | | | | | | X | | |
| 3.151 | g | (15) TV-1 generated from DISR Online | X | X | | | X | X | | |
| 3.152 | g | (16) TV-2 | | X | | | X | X | | |
| 3.2 | | b. Architecture Analysis. (Assessor: FCB) | | | | | | | | |
| 3.21 | | (1) First order analysis – Performed by the respective FCB identifying capability gaps, shortfalls and duplications. Once a first order of analysis identifies capability gaps and deficiencies, a decision process follows to evaluate what to do about it. Measures of effectiveness (MOEs) are developed to guide the DOTMLPF process. | | | | X | X | X | | |
| 3.211 | | (a) Where capability gaps exist, a new system needs to be developed to meet the requirement? | | | | X | X | X | | |
| 3.212 | | (b) Where capability deficiencies exist, existing systems need to be improved or modified to meet the requirement? | | | | X | X | X | | |
| 3.213 | | (c) ©If the analysis identifies systems that have no required capability based on the first order analysis, they should be eliminated. | | | | X | X | X | | |
| 3.214 | | (d) If there are capability duplications, a follow-on question needs to be addressed to determine if the redundancy is necessary. There may be circumstances where it is strongly desired to maintain secondary and even tertiary capability. In these cases, maintain the | | | | X | X | X | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference # | Criteria | T I S P 6 | I S P 6 | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|-------------|--|-----------------------|------------------|-------------|-------------|-------------|-------------|--|---|
| | | redundant systems. However, when system redundancy is identified that is not necessary, the less capable systems should be deleted. | | | | | | | | |
| 3.215 | | (e) How will the system operate in a net-centric environment? | X | X | | X | X | X | | |
| 3.216 | | (f) How will the system operate in a degraded environment (limited bandwidth, changes in the information condition level (INFOCON))? For example, what is lost, what is the alternative method and impact on operations? | X | X | | X | X | X | | |
| 3.22 | | (2) Second order analysis. Identifies interoperability requirements? Tasks and capabilities are grouped into operational nodes. System interfaces required within nodes and between nodes are mapped out. (Assessor: J-6I) | | | | | X | X | | |
| 3.221 | | (a) If there is no system that performs a required function (capability gap), then the interoperability requirements become key design criteria in the proposed solution, | | | | | X | X | | |
| 3.222 | | (b) For legacy systems, the first question that should be resolved through the first order analysis is whether the system is even needed. If a system does not support a capability need in the architecture, there is no need to proceed with interoperability analysis, it should simply be cut. | | | | | | | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference # | Criteria | T I S P 6 | I S P 6 | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|-------------|---|-----------------------|------------------|-------------|-------------|-------------|-------------|--|---|
| 3.23 | | c. Detailed Architecture Analysis | | | | | | | | |
| 3.231 | | (1) Do the architecture products (as applicable AV-1, OV-2, OV-4, OV-5, OV-6c, OV-7, SV-1, SV-2, SV-4, SV-5, SV-6, SV-11, TV-1, TV-2) include a short complete description that describes the architecture, its intended use, and discusses the highlights of each product? | X | X | | | X | X | | |
| 3.232 | | (2) Do the architecture products demonstrate integration by showing that the architecture graphics are traceable between each of the other architecture views? | X | X | | | X | X | | |
| 3.233 | | (3) Does the OV-1 architecture product present a top-level view of the system's interoperability requirements with other current and known future systems? | | | | X | | | | |
| 3.234 | | (4) Do the mandatory architecture views provide all the essential data elements specified by the DODAF for an integrated architecture product set? | X | X | | X | X | X | | |
| 3.235 | | (5) Does the document identify the information exchange for the system for each mission area that the system is proposed to support (e.g., CAS, AAW, surveillance, and reconnaissance)? | X | X | | | X | X | | |
| 3.236 | | (6) Do the document architecture views (as applicable AV-1, OV-2, OV-4, OV-5, OV-6c, | X | X | | | X | X | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference # | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|-------------|---|----------------------|--------------------|-------|-------|-------|-------|--|---|
| | | OV-7, SV-4, SV-5, SV-6, SV-11, TV-1, TV-2) identify specific current and known IT and NSS sub-systems and interfaces that need to exchange information? | | | | | | | | |
| 3.237 | | (7) Does the document describe considerations for joint, combined, and coalition use? | X | X | | X | X | X | | |
| 3.238 | | (8) Does the document identify procedural and technical interfaces, communications, protocols, and standards required to be incorporated to ensure compatibility and interoperability with other Service, joint Service, NATO, and other allied and friendly nation systems? | X | X | | | X | X | | |
| 3.239 | | (9) Does the document require the system to comply with applicable information technology standards contained in the DISR? NIPRNET: http://disronline.disa.mil/SIPRNET : http://disronline.disa.smil.mil/a/DISR | X | X | | | X | X | | |
| 3.240 | | (10) Does the document identify multinational interoperability considerations, where applicable? | X | X | | X | X | X | | |
| 3.241 | | (11) Core Architecture Data Model (CADM). Are architecture products/views CADM Conformant? (CJCSI 3170.01 and the DODAF require architecture products | X | X | | | X | X | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference ⁵ | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------------------|---|-------------------------------|--------------------------|-------------|-------------|-------------|-------------|--|---|
| | | are CADM conformant for analysis - met by products provided as CADM XML documents). | | | | | | | | |
| 4 | ENCL D | Key Interface Profile Declaration. (Assessor: J-6I) | | | | | | | | |
| 4.1 | | a. Does the program/system capability document include the KIP declaration table? | X | X | | | X | X | | |
| 4.2 | | b. Does the architecture agree with the declared KIPs? | X | X | | | X | X | | |
| 4.3 | | c. Does the KIP declaration table contain all appropriate information? | X | X | | | X | X | | |
| 5 | p-u | Information Assurance. (Assessor: J-6X) | | | | | | | | |
| 5.11 | | a. Is compliance with DOD 8500 series documents required? (If yes, continue) | X | X | | | X | X | | |
| 5.12 | | b. Does program address system accreditation as defined in DITSCAP (DODI 5200.40) ⁸ ? | X | X | | | X | X | | |
| 5.13 | p-q | c. Is the Mission Assurance Category (I, II or III) and Confidentiality Level (Classified, Sensitive or Public) identified? | X | X | | | X | X | | |
| 5.14 | II | d. Has the requirement(s) for cross-domain interconnection(s) or information sharing (e.g., different classification levels or outside DOD) identified? | X | X | | | X | X | | |
| 5.15 | p, ff | e. Is the program in the Certification and Accreditation Process (e.g., DITSCAP ⁸)? | X | X | | | | X | | |
| 5.16 | r | f. Has the program's Acquisition Information Assurance Strategy been approved by the Component CIO and for ACAT 1AM, ACAT | X | X | | | X | X | | |

⁸ DIACAP replaces DITSCAP upon approval of DODI 8510.

CJCSI 6212.01D

8 March 2006

| Item # | Reference ⁵ | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------------------|---|-------------------------------|--------------------------|-------------|-------------|-------------|-------------|--|---|
| | | 1C, and ACAT 1D programs reviewed by the DOD CIO? | | | | | | | | |
| 5.17 | p, ll | g. Has a Designated Accrediting Authority been identified and appointed in writing? | X | X | | | | X | | |
| 5.18 | p | h. Has a Certifying Authority and/or Certifying Agent been identified and appointed in writing? | X | X | | | | X | | |
| 5.19 | p | i. Has a User Representative been identified and appointed in writing? | X | X | | | | X | | |
| 5.20 | p, ll | j. Has an IA Manager (IA) been identified and appointed in writing? | X | X | | | | X | | |
| 5.21 | | k. Does the CDD include an Information Assurance Compliance Statement with words similar to: "This program or system will be in full compliance with the IA requirements in DOD 8500 series CJCS 6510 series directives, instructions and manuals?" | | | | | X | | | |
| 5.22 | | l. Does the CPD include the Information Assurance Compliance Statement with words similar to: "This program or system is in full compliance with the IA requirements in the DOD 8500 series and CJCS 6510 series directives, instructions and manuals?" | | | | | | X | | |
| 5.23 | q | m. Have required baseline DOD IA controls been identified and implemented? | X | X | | | | X | | |
| 5.25 | s | n. Has the point of contact and contact information been identified for accreditation decision documentation (e.g., Security System Authorization | X | X | | | | X | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference ⁵ | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------------------|--|-------------------------------|--------------------------|-------------|-------------|-------------|-------------|--|---|
| | | Agreement (DITSCAP) or implementation plan (DIACAP) ⁹ accreditation decision or other supporting documentation)? | | | | | | | | |
| 5.26 | rr | o. Has the program been registered with the Ports, Protocols and Services Management (PPSM) database? | X | X | | | | X | | |
| 6 | i, j | <u>Spectrum Supportability, E3, and Frequency Management. (Assessor: J-6B)</u> | | | | | | | | |
| 6.1 | | a. If applicable, does the document identify a requirement for spectrum supportability? | X | X | | X | X | X | | |
| 6.2 | | b. If applicable, does the document address electromagnetic environmental effects (E3)? | X | X | | X | X | X | | |
| 6.3 | | c. If applicable, does the document address host nation approval? | X | X | | X | X | X | | |
| 6.4 | | d. If applicable, has a DD Form 1494 been submitted to the Service Frequency Manager Office? | X | X | | X | X | X | | |
| 6.5 | | e. Does the document include a spectrum supportability compliance statement or outline a plan to obtain spectrum supportability? | X | X | | X | X | X | | |
| 6.6 | | f. Does the document address spectrum supportability as a separate requirement in a paragraph? | X | X | | | X | X | | |
| 7 | gg, qq | <u>Joint Tactical Radio System</u> | X | X | | X | X | X | | |

⁹ Upon approval of DODI 8510.

CJCSI 6212.01D

8 March 2006

| Item # | Reference ⁵ | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------------------|--|-------------------------------|--------------------------|-------------|-------------|-------------|-------------|--|---|
| | | (JTRS). If applicable, does the document identify requirements for radio-based communications that will be satisfied by the JTRS CDD/CPD? (Assessor: J-6C) | | | | | | | | |
| 8 | 1 | Space and SAASM. If applicable, does the document include a requirement for NAVSTAR global positioning system (GPS) and precise positioning service (PPS)? If yes, does the document clearly state that the system will develop and procure only selective availability anti-spoofing module (SAASM) based equipment? (Assessor: J-6C) | X | X | | X | X | X | | |
| 9 | ENCL E | JITC Testing. Does the document adequately address the requirement for interoperability system testing and certification? (Assessor: J-6I) | X | X | | | X | X | | |
| 10 | | Miscellaneous. (Assessor: J-6I) | | | | | | | | |
| 10.1 | OSD Memo | a. Is the program registered in the DOD IT Portfolio Registry? | X | X | | | X | X | | |
| 10.2 | | b. Is the program/system registered in JCPAT-E? | X | X | | | | | | |
| 10.3 | | c. NR-KPP Configuration Management. Are the NR-KPP package and associated files and online entries (e.g., DISR, DARS) uniquely identified with an appropriate naming convention and changes strictly controlled. (Associated | X | X | | | X | X | | |

CJCSI 6212.01D

8 March 2006

| Item # | Reference ⁵ | Criteria | T I S P ⁶ | I S P ⁶ | J C D | I C D | C D D | C P D | Status C = Complete I = In process F = Failure to Complete NA = Not Applicable | Comments Include Risk Assessment: H = High Risk M = Moderate Risk L = Low Risk N = No Risk |
|--------|------------------------|--|-------------------------------|--------------------------|-------------|-------------|-------------|-------------|--|---|
| | | computer files and database entries should be “locked” upon submission of the document package (i.e., any changes made to a new version)). | | | | | | | | |
| 10.31 | | d. Are DARS files uniquely identified with name/version ID? | X | X | | | X | X | | |
| 10.32 | | e. Is the DISRonline entry (TVs) uniquely identified with name/version ID? | X | X | | | X | X | | |
| 10.33 | | f. Documents marked with version/date? | X | X | | | X | X | | |
| 10.34 | | g. Are references to outside material provided: standards, standards profiles, KIPs, interface control documents, etc. all identify a specific version? (At least major version ID with an unambiguous method for determining the specific version to be implemented.) | X | X | | | X | X | | |
| 11 | | Acquisition History. (Assessor: J-6I) | | | | | | | | |
| 11.1 | | a. Does the document identify applicable predecessor documents? | X | X | | X | X | X | | |
| 11.2 | | b. Is the associated ISP submitted to JCPAT-E database? | | | | | X | X | | |

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

ENCLOSURE E

JOINT INTEROPERABILITY TESTING AND CERTIFICATION PROCESS

1. General. All Information Technology (IT) and National Security Systems (NSS) must be evaluated and certified by the Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC). All systems – Acquisition Category (ACAT), non-ACAT, and fielded systems – must be evaluated and certified prior to (initial or updated) fielding, and periodically during their entire life – as a minimum, every 3 years. JITC Joint Interoperability Test Certification is based on Joint Staff J-6 certified Net-Ready Key Performance Parameters (NR-KPPs) and other approved requirements. Testing associated with evaluations may be performed in conjunction with other testing (e.g., Developmental Test & Evaluation (DT&E), Operational T&E (OT&E)) to conserve resources. JITC as the Joint interoperability test certifier may use test results from another testing organization (i.e., an EA-TJTN JUICE assessment/test, USJFCOM JSIC) as the basis for a Joint Interoperability Test Certification if the testing results are sufficient. Joint interoperability testing and certification is a continuous process that must be managed and resourced throughout the system lifecycle.

2. Applicability – Systems Requiring Certification. All systems affecting joint/enterprise information exchange will be certified for net-readiness before being placed into operation (see DOD 4630 series). This includes, but is not limited to:

a. All IT and NSS (systems or services) acquired, procured or operated by any component of the Department of Defense, to include:

(1) Joint network infrastructure system components (e.g., voice switches for Defense Switched Network (DSN), encryption devices, network routers, network firewalls).

(2) Each increment of an evolutionary acquisition strategy, including each increment of a spiral development.

(3) Systems with changes (e.g., Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facility (DOTMLPF), DOTLPF, hardware or software modifications, including firmware) affecting net-readiness, similar changes to interfacing systems, or systems with revoked certifications or J-6 validation, or systems with expired certifications.

3. Joint Interoperability Test Certification. JITC will evaluate the four NR-KPP elements: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM) (reference m), supporting integrated architecture products (references n and o) required to assess information exchange and operationally effective use for a given capability, compliance with applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) (<http://kips.disa.mil>), and verification of compliance with DOD information assurance requirements (references p through u). In addition, Service and Agency operational test agencies may provide assessments of the operational effectiveness of information exchanges based on operational test events or exercises.

a. Systems without an NR-KPP will be evaluated based on alternate J-6 approved requirements. For all systems, interoperability evaluation will assess the degree to which the interoperability requirements are met and the expected operational impact of any discrepancies.

b. Joint Interoperability Test Certification is the part of the overall certification process that characterizes interoperability capabilities in an operational environment and assesses the operational impact of any discrepancies. Related processes are the J-6 Interoperability and Supportability Certifications and the J-6 System Validation. J-6 certified interoperability requirements and capabilities feed the JITC interoperability test and evaluation process, and, in turn, JITC Interoperability Test Certifications provide input to the J-6 System Validation process and the Milestone Decision Authority (MDA) (or equivalent) fielding decision.

c. JITC issues full joint interoperability test certifications when all critical interoperability requirements are met and there are no discrepancies with a critical operational impact. When appropriate, JITC issues limited certifications to provide the interoperability status when only a subset of critical requirements have been adequately demonstrated. "Limited" certifications provide an indication of the interoperability status in cases where useful capabilities are provided, despite not meeting threshold requirements, and there are no expected critical operational impacts or adverse effects on the interoperability environment.

d. JITC updates Joint Interoperability Test Certifications throughout the lifecycle of a system to reflect changes in the status and environment.

4. Clarification of Scope. Joint Interoperability Test Certification is not a substitute for J-6 System Validation – programs in the JCIDS process must have both a Joint Interoperability Test Certification from JITC and J-6 System Validation before fielding. The only exception is systems that have been issued an Interim Certificate To Operate (ICTO) by the Military Communications-Electronics Board/Interoperability Test Panel (MCEB/ITP) (or appropriate authority). There may also be other certifications or validations required in

addition to Joint Interoperability Test Certification, J-6 Interoperability and Supportability Certification, and J-6 System Validation. Spectrum certifications, IA certifications or accreditations, network manager approval, and other validations/approvals may be required and are not necessarily satisfied by JITC Joint Interoperability Test Certification.

5. Program Manager (PM)/Sponsor Guidelines. The system sponsor shall ensure that the following items are adequately addressed at least 120 days prior to any interoperability testing.

a. J-6 certified requirements, or alternate J-6 approved requirements.

(1) Certified Capabilities Production Document (CPD), Information Support Plan (ISP), or NR-KPP/Interoperability KPP (I-KPP).

(2) J-6 confirmation that previously approved/certified Requirements Generation System (RGS – predecessor to JCIDS) documents are valid (e.g., older Operational Requirements Documents (ORDs), C4I Support Plans (C4ISPs) when used as the source of requirements).

(3) J-6 confirmation that any changes to the certified NR-KPP/I-KPP are also valid (i.e., are also J-6 certified).

b. Validity of any non-JCIDS requirements is confirmed by J-6. This includes requirements derived from JCIDS certified documents, such as a system that implements a subset of CPD requirements.

c. System component requirements are coordinated with JITC to ensure that requirements are defined, testable and measurable (e.g., requirements for non-DOD systems/components, commercial off-the-shelf (COTS) components).

d. Planning has been coordinated and testing scheduled with JITC including:

(1) If applicable, approved Test and Evaluation Master Plan (TEMP), or equivalent, is available. As a minimum, all CPD/ISP enterprise-level and critical information exchanges will be used to develop the TEMP measures of effectiveness.

(2) Coordination with JITC to develop an interoperability test and evaluation strategy, which is documented in an Interoperability Certification Evaluation Plan (ICEP), interoperability test plan (ITP), or equivalent documentation, as appropriate.

(3) Funding and resources are provided to JITC for test planning, conduct, and reporting. Standards Conformance testing programs serve as a foundation for overall joint interoperability testing. Service Participating Test Unit Coordinators (PTUCs) will be the point of contact for conducting or

coordinating standards conformance testing activities for Service programs. Program Sponsors will coordinate with Service PTUCs for funding and scheduling of standards conformance and testing resources. Service PTUCs can also serve to coordinate participation of Service resources in joint distributed federations that enable JITC joint interoperability testing. The PTUC will be the Program Sponsor's POC for coordinating funding of standards conformance testing and participation in Joint distributed federations supporting interoperability testing to ensure efficient and effective testing and certification of the program.

(4) Standards profiles have been validated in DISRonline, as applicable.

e. Net-Centric Operations and Warfare Reference Model (NCOW RM) compliance has been verified.

f. IA compliance has been verified, as applicable.

g. Results from standards conformance, KIPs compliance tests, Service testing, any assessments, etc. are available.

h. Coordination with JITC during the planning and execution of standards conformance and system interoperability testing for each acquisition milestone and subsequent fielding decisions and for recertification to ensure that the required data elements for system interoperability evaluation are collected and validated.

i. Coordination, funding, and scheduling considerations negotiated with proponents of interfacing systems (e.g., interfacing systems must be available during interoperability testing).

j. Issues are resolved or presented to the appropriate authority for resolution – J-6 for interoperability requirements, MCEB/ITP for ICTOs, etc.

6. Joint Interoperability Test Certification Process. The JITC Interoperability Test Certification process comprises four basic steps. Joint interoperability testing and evaluation is an iterative process – some or all of the steps may need to be repeated as conditions change. The four basic steps are (see figure E-1):

- (1) Identify (Interoperability) Requirements
- (2) Develop Certification Approach (Planning)
- (3) Perform Evaluation
- (4) Report Certifications and Statuses

a. Identify Interoperability Requirements. Establishing requirements/capabilities is a critical step, and system sponsors must resolve any requirements/capabilities issues with the Joint Staff J-6. If a J-6 System Validation is needed (e.g., for JCIDS systems), requirements/capabilities must be J-6 certified. The JITC provides input to the J-6 requirements/capabilities certification process and uses the results as the foundation for the remaining three steps of the Joint Interoperability Test Certification process. Thus, system sponsors must coordinate with the JITC beginning with the initial capabilities documentation processing to ensure requirements/capabilities are defined in measurable and testable form.

b. Develop Certification Approach (Planning). The sponsor and JITC will work closely to establish a strategy for evaluating interoperability requirements in the most efficient and effective manner, in an operationally realistic environment (the environment must be as operationally realistic as practicable – this includes employing production representative systems, members of the user community as operators, realistic messages and network loads, configurations in compliance with IA requirements, etc.). This evaluation strategy identifies data necessary to support JITC Joint Interoperability Test Certification as well as the test events/environments planned to produce that data. Sponsors will coordinate with JITC to integrate interoperability and standards conformance test needs into the system's T&E documents (e.g., TEMP, test plans), identify and use any applicable existing plans, and ensure test data is available to JITC for evaluation. Sponsors are encouraged to coordinate with other interoperability testing organizations and JITC to try to identify interoperability demonstration venues acceptable for JITC interoperability assessment testing or interoperability certification testing activities.

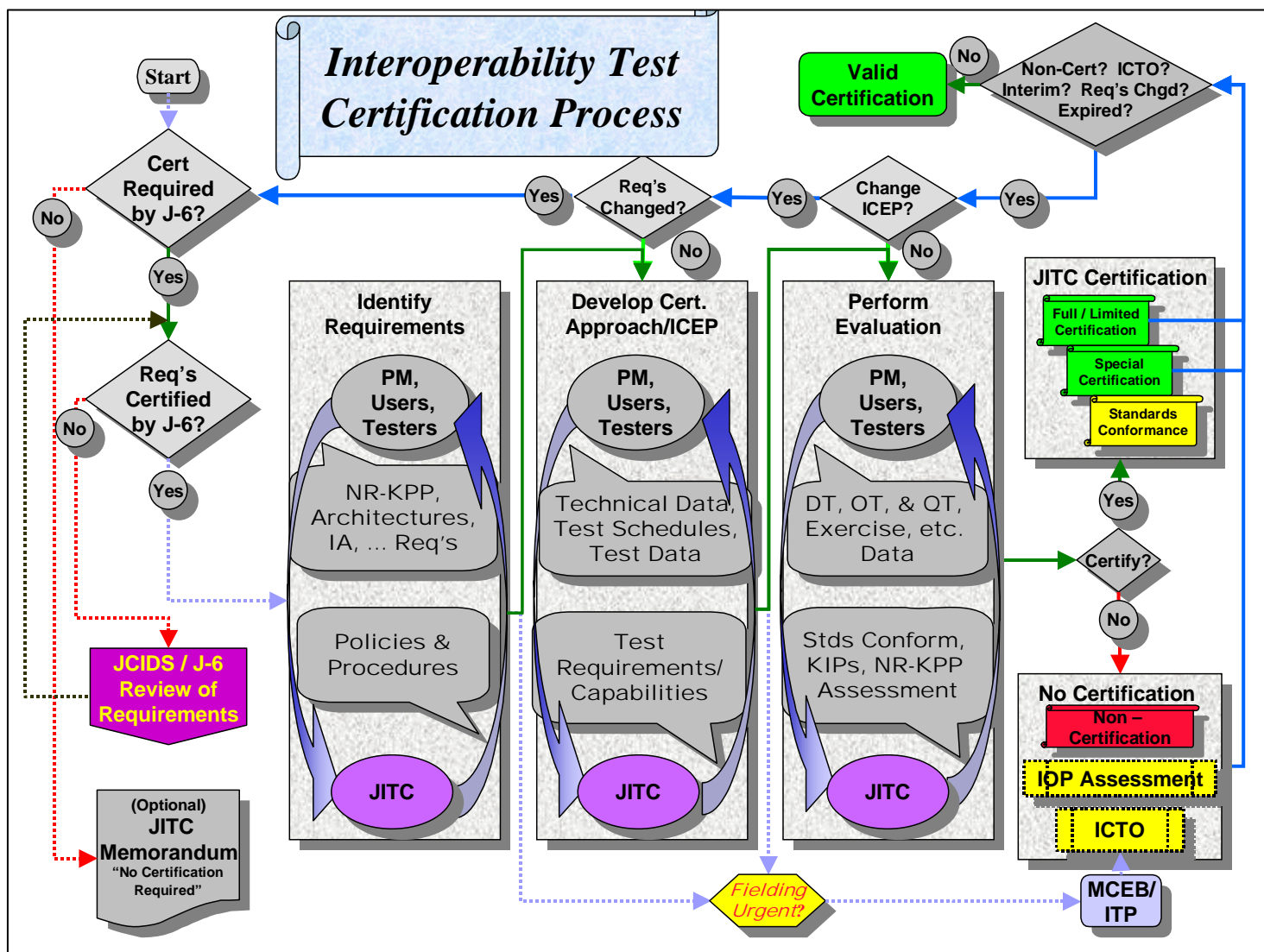


Figure E-1. Interoperability Test Certification Process

| | | | |
|---------|---|----------|--|
| Legend: | | | |
| Cert | Certification | KIP | Key Interface Profile |
| DT | Developmental Test | MCEB/ITP | Military Communications-Electronics Board/Interoperability and Policy Test Panel |
| IA | Information Assurance | NR | Net-Ready |
| ICEP | IOP Certification Evaluation Plan | NR-KPP | Net-Ready Key Performance Parameter |
| IOP | Interoperability | OT | Operational Test |
| ICTO | Interim Certificate to Operate | PM | Program Manager (Sponsor) |
| JCIDS | Joint Capabilities Integration and Development System | QT | Qualification Test |
| JITC | Joint Interoperability Test Command | Req's | Requirements |
| J-6 | Joint Staff J-6 | Std's | Standards Conformance |

(1) Additionally, complex systems that depend on multiple evaluation events will require JITC to develop an Interoperability Certification Evaluation Plan (ICEP).

(2) Some systems and programs will have a TEMP (see DoDI 5000.2) to guide interoperability planning. These systems/programs may have a JITC ICEP. ICEPs will lay out how the systems will be tested and evaluated. Generic test plans will accommodate testing of frequently tested system components (e.g., telecommunications switches, individual KIPs). The sponsor and JITC will work closely to establish a viable testing program that satisfies testing requirements in the most efficient and effective manner.

(3) JITC works with the system sponsor to develop an ICEP. The ICEP outlines how the system will be tested against the J-6 certified requirements in the CPD/ISP. The testing is conducted during DT&E, OT&E, and various joint exercises and deployments.

(4) In support of test planning and JITC development of a certification approach and ICEP, system sponsor and developers will provide necessary system technical data and interface specifications, and coordinate with JITC to identify test data collection requirements.

c. Perform Evaluation. Interoperability evaluation often spans DT and OT and relies on multiple test events conducted by various organizations. The amount and type of testing will vary based on characteristics of the system being evaluated. This is further reason to coordinate early with the testing organizations.

(1) When JITC is not the responsible testing organization, the system sponsor (for DT) or appropriate Operational Test Agency (OTA) (for OT) will coordinate test plans, analysis, and reports with JITC to ensure sufficient information is available to support a certification determination. Sponsors must coordinate testing changes (e.g., schedule, locations, scope, methodology, etc.) with JITC, since such changes may impact JITC's ability to evaluate and certify.

(2) When JITC is the responsible test organization, JITC will develop the necessary plans and reports and coordinate them with the sponsor. Regardless of the responsible test organization, tests must employ production representative systems in as realistic an operational environment as practicable, including use of authorized IA configurations.

(3) Interoperability evaluation requires results from standards conformance testing/certification. Standards conformance testing should be coordinated early with JITC to ensure that the testing is adequate to support interoperability evaluation. Standards conformance testing may be performed by other organizations with prior coordination with JITC. JITC conducts some

standards conformance testing for standards that have a direct impact on interoperability and where there is not an existing standards testing and certification program.

(4) Interoperability assessments are a special case of interoperability evaluation where the objective is to determine the interoperability of a system or system component prior to formal evaluation. Assessments may be based on preliminary requirements (e.g., from a Capabilities Development Document (CDD)), or may be designed to assess only part of the overall requirements. Assessments can provide valuable insight to the sponsor on the state of interoperability, and may also be used to provide input to the OT Readiness Review (OTRR).

d. Report Certifications and Statuses. JITC uses data from the various types of testing to produce interoperability reports and certifications, as appropriate. Standards conformance testing may result in a Standards Conformance Certification. Interoperability testing results may be documented in a number of ways, depending on the test purpose, status of requirements, and nature of the system. Only Joint Interoperability Test Certifications are examined by the J-6 for consideration of issuing a J-6 System Validation.

(1) The JITC Interoperability evaluation will be an independent analysis of the data to determine the interoperability status of the system.

(2) Joint Interoperability Test Certifications report on the status of the four NR-KPP elements, including net-readiness, information exchange (individual interfaces and the status of top-level exchange requirements), KIPs compliance, IA, and any other specified system interoperability performance parameters. The certification will also specify if it applies only to special operational environments, and will also indicate the expiration period.

(3) JITC distributes Interoperability Test Certifications to the MCEB/ITP members, J-6, the program manager (sponsor), and other interested, authorized parties. In addition to distribution, JITC maintains a database of all JITC certification related products, the System Tracking Program (STP).

7. Joint Interoperability Test Certification Process –Typical Events. The following is an example of the major interoperability test related events that may occur during a "typical" (medium to large JCIDS) system development. For non-JCIDS systems, the events would be similar, however, the details may differ (e.g., RGS ORD may be used in place of CPD).

a. Initiation of development/acquisition/procurement.

(1) Sponsor contacts JITC; POCs established, JITC STP entry made.

- b. Interoperability requirements established, test plans developed.
 - (1) Initial Capabilities Document (ICD)/CDD used to create initial test plans (ICEP, ITP, etc.).
 - (2) If non-JCIDS, alternate ISP or NR-KPP/I-KPP requirements coordinated with J-6.
 - (3) Any interoperability requirements issues resolved by J-6 and MCEB/ITP, with those related to intelligence resolved by the Military Intelligence Board (MIB).
- c. Standards conformance and interoperability assessments may be performed (if system components are available).
 - (1) Standards Conformance Certifications issued.
 - (2) Interoperability Assessments produced, if needed.
- d. Interoperability requirements refined, certified, derived, as appropriate.
 - (1) CPD used to refine interoperability test plans (ICEP, ITP...).
 - (2) TEMP developed or refined, and approved, as needed.
- e. Standards profiles validated, other validations and certifications occur (e.g., N-COW RM compliance).
- f. Standards conformance and interoperability assessments continue throughout the development phase.
- g. JITC provides input to OTRR process, as requested.
- h. JITC provides testing status to J-6, MCEB/ITP, etc., as requested.
- i. Interoperability testing conducted, usually in conjunction with OT.
- j. JITC interoperability evaluation performed.
 - (1) Joint Interoperability Test Certification issued. Full, limited, or non-certification. Alternatively, an interoperability assessment letter/report may be produced.
 - (2) Interoperability status posted to JITC STP, and distributed to appropriate parties (J-6, MCEB/ITP, sponsor).
- k. J-6 issues J-6 System Validation (if J-6 certified requirements exist and other conditions met).

1. Life-cycle support. Changes affecting interoperability, including new releases or planned increments, or expiration/revocation of certifications, require additional testing and evaluation starting at the appropriate step.

8. JITC Interoperability Products. JITC interoperability products include the following, though not all products may apply to all systems:

a. ICEP/Test Plans (planning documents) and various types of reports and online (NIPRNET/SIPRNET) product registers.

b. Standards Conformance Certification. Issued after technical testing against published standards/standards profiles documented in the TV-1 and TV-2 created in the DISRonline tool to describe the degree of conformance to that standard/profile (e.g., conformance to MIL-STD-188-181 (DAMA SATCOM)). A standards conformance certification is not sufficient to allow fielding. Additional testing beyond that needed for a standard may be required to determine compliance with standards profiles.

c. Interoperability Assessment. Issued following testing (Operational Assessments (OAs), JITC compatibility and interoperability assessments) to provide feedback concerning interoperability strengths and weaknesses when a certification is not appropriate. An interoperability assessment is not sufficient to allow fielding.

d. OT Readiness Review (OTRR) Interoperability Statement. JITC recommendation, to the OTRR assessing whether a system is ready for OT from an interoperability perspective. DODI 4630.8 describes the contents of the JITC OTRR input.

e. Interoperability Test Certifications: All JITC interoperability test certifications expire upon changes that may affect interoperability. Additionally, all certifications expire three (3) years from original date of issue.

(1) Special Interoperability Test Certification. Issued for systems or system components (e.g., network infrastructure components) that require interoperability test certification but are not subject to the JCIDS process, and generally do not individually need requirements certified by J-6 (e.g., commercial switches being procured to operate in the DSN, in-line encryption devices). JITC will work with J-6 to verify that the item is not subject to J-6 certification.

(2) Limited Joint Interoperability Test Certification. Issued when a system has adequately demonstrated interoperability for a subset of interoperability requirements (has not met all threshold requirements). A “limited” certification may not be sufficient to allow fielding. If military necessity warrants fielding of the system for the demonstrated capabilities, the system sponsor should contact the J-6 to request a formal modification of the

NR-KPP (or legacy I-KPP) or the MCEB/ITP for an Interim Certificate to Operate (ICTO).

(3) Joint Interoperability Test Certification. Issued when a system has adequately demonstrated interoperability for at least all critical threshold requirements pertaining to a specific increment. This system certification attests that the system's interoperability is sufficient to support a fielding decision. Evaluation should continue until the status of all objective interoperability requirements can be determined and reported.

9. Interoperability Evaluation and Certification. Interoperability evaluation will evolve along with evolution of the established NR-KPP elements. During the transition to the NR-KPP, I-KPP evaluations (from valid J-6 certified ORDs/I-KPPs) may still be conducted until 24 May 2007. After this date, interoperability evaluations based on I-KPP requirements shall not be performed without consent of the J-6 and J-8 (Certification letters, including extension of certification, associated with I-KPP evaluations will be issued NLT 90 days after this cutoff date).

a. Policy applicable to all types of interoperability test certifications includes:

(1) The Interoperability and Supportability Certification process determines interoperability requirements.

(2) All interoperability requirements shall be used for evaluation and the status reported for all interoperability requirements, not merely the capabilities that have been implemented. This includes critical (threshold) and all (critical plus non-critical -- objective) requirements. If requirements for increments were not clearly delineated by increment (phase, spiral, block, etc.) in the J-6 certified requirements, as mandated by DOD policy, all interoperability requirements shall be assumed to apply to the current increment and be evaluated as such. Changing the increment or criticality of a requirement is a modification to the requirements that requires J-6 (re-) certification.

(3) As a minimum, all enterprise level and external (top-level) information exchanges shall be evaluated. Any other system interoperability requirements shall also be factored into the overall interoperability evaluation (e.g., some interoperability requirements do not appear in the integrated architecture products, such as a capability to communicate on two channels simultaneously. Other interoperability-related requirements may appear as KPPs separate from the NR-KPP, such as the tagging of data, reliability of certain types of communications, etc.).

(4) Standards conformance requirements, as documented in TV-1 products, or derived from other requirements and specifications, shall be

evaluated and reported as appropriate for the complexity and maturity of the protocols.

(5) Interoperability evaluation will be based on testing of production representative systems in as realistic an operational environment as practicable. This includes use of test scenarios with a typical message mix, loading that reflects normal and wartime modes, and benign and hostile environments. System test configurations will represent realistic IA aspects of the operational environment.

(6) Interoperability evaluation must assess the end-to-end exchange and use of information. For the exchange to be assessed as meeting all requirements, the technical exchange and use in an operational environment must be confirmed, including associated attributes for accuracy, completeness, and timing (i.e., QoS attributes); security, etc. Meeting the requirements means that not only the system functions correctly, but that the interfacing systems also perform as required, and that the network infrastructure provides the necessary reliability, bandwidth, response times, security, etc. JITC interoperability evaluation is not an assessment of operational effectiveness, but does include the expected operational impact of any discrepancies.

(7) Version identification information shall be provided for the system, interfacing systems, and net-centric components (both services and data).

(8) Status reporting on items shall include the criticality associated with the item, the status (e.g., certified, not tested), the degree of compliance (e.g., all critical requirements met, all requirements met), and the expected operational impact of any discrepancies. Expected operational impact includes the effects on the system, interfacing systems, and interoperability environment (e.g., net-centric services and data).

(9) The interoperability test certification memorandum shall include a statement on any conformance certification requirements, whether conformance has been conducted as a separate test or included in the interoperability testing.

(10) Testing limitations shall be reported, including the impact they may have on interpretation of the results and conclusions. Any untested requirements shall be included in the testing limitations.

(11) Life cycle interoperability evaluation will continue until objective requirements have been satisfied and certified, and then will continue as needed to satisfy re-certification needs.

(12) Certification status will be verified during exercises and deployments throughout the life cycle. If indications warrant (e.g., serious problems are observed or reported, requirements or operational environment

appear to have changed, configuration has changed significantly) assessments or complete evaluations will be performed to confirm and update the status, as necessary. Existing certifications may be confirmed (no action required), extended to minor system releases (updates), or revoked, and certification, non-certification, and interoperability status memoranda issued as appropriate.

b. Net-Ready Key Performance Parameter (NR-KPP) Based Interoperability Test Certifications. For programs subject to NR-KPP processes, the evaluation will determine the operational status of the NR-KPP requirements (including interfaces, enterprise-level exchange requirements and other interoperability requirements). Guidance specific to the NR-KPP process includes:

(1) Requirements shall be obtained from a J-6 interoperability and supportability certified NR-KPP contained in a CPD – alternatively, an ISP if a CPD is not required. If there is both a CPD and ISP with different requirements (or different J-6 certification status), J-6 must be consulted to resolve the issue. When J-6 has granted a waiver for the NR-KPP requirement, an alternate J-6 approved source of requirements information will be specified by J-6. This alternate source shall then be used for JITC interoperability evaluation.

(2) The certification must address the NR-KPP statement, with the four primary elements of the NR-KPP and associated performance attributes, and provide the status of standards conformance. (Note that the elements are not mutually exclusive – there is considerable overlap and interplay of the requirements of the NR-KPP elements.)

c. As noted, in addition to reporting on the NR-KPP elements, standards conformance shall be reported separately where appropriate. A summary of the status reporting for these items follows.

(1) NCOW (GIG Enterprise Services (GIG ES (GES)) compliance (i.e., net-readiness). Evaluation of the NCOW element to determine if a system is net-enabled involves dynamic testing in addition to the static NCOW RM compliance checklist. For example, standards conformance testing is the dynamic analog of the static DISR compliance assessment. JITC's evaluation of this element comprises compliance with GES that comprises compatibility with Core Enterprise Services (CES) and COI services and data. A given system may be a provider or consumer of services/data, or both, and for the entire enterprise or a subset.

(2) Integrated Architectures. This element of the NR-KPP includes both the technical exchange of information and the end-to-end use of that exchange. Exchange status is reported by physical/logical interface (as defined in architecture products), and critical, enterprise-level exchange requirements. Interface status will include an identification of any KIPs associated with the interface and its compliance status.

(3) Key Interface Profiles (KIPs) are operational, systems, and technical specifications of key GIG interfaces. The categories of KIPs comprise a wide range of interface specifications, from complete interface requirements to merely protocol specifications for part of an interface. The KIP Declaration Table (Table D-A-2) includes additional information on the system compliancy requirements to the KIPs (i.e., not all systems may need to implement 100% of a KIP specification). KIPs compliance will be reported separately to clarify the overall compliance with this NR-KPP element, and will also be included in the reporting of other elements where appropriate (e.g., in the interface requirements matrix, where one or more KIPs may apply to an interface). KIPs compliance must be reported in sufficient detail to indicate the degree of compliance (for those cases where 100% compliance is not required), and the method of determining the compliance status (e.g., standards conformance testing, derived (from other formal testing), demonstrated). Any discrepancies must be assessed for expected operational impact.

(4) Information Assurance (IA) is an integral part of all aspects of net-centric systems – it should not be viewed as an independent element of the NR-KPP, except for reporting purposes. JITC will evaluate IA (or portions of IA requirements) when requested, and will report any known IA status as part of reporting the NR-KPP status. However, some portions of IA requirements (e.g., DITSCAP) may not be assessed until after JITC interoperability certification, and cannot be reported in the certification. As noted above, testing environments will employ realistic IA configurations.

(5) Standards conformance requirements also appear throughout the NR-KPP, however, like KIPs, the status will be reported separately or included in the reporting of other elements where appropriate (e.g., in the interface requirements matrix). A thorough, consistent methodology must be applied when testing and certifying standards conformance. The system standards profile is documented in the TV-1, created with the help of the DISR online tool. Other standards requirements may be defined in KIPs declared in requirements documents (and KIPs used by other KIPs), the NCOW RM, etc.

d. Interoperability Key Performance Parameter (I-KPP) Based Interoperability Test Certifications. Interoperability evaluation and status reporting for systems documented under the RGS system shall use the following guidance.

(1) Requirements shall be obtained from a J-6 Interoperability Certified ORD or certified I-KPP package. Some ORDs approved by the Joint Requirements Oversight Council (JROC) before JCIDS may still be valid. However, JROC approved ORDs, ORDs approved before 2001 (prior to CJCSI 6212.01B), and ORDs without an I-KPP statement require coordination with, and approval by, J-6 before use. The I&S certification must address whether the I-KPP and individual top-level IERs and overall system interoperability

performance have been met. The status of physical/logical interfaces is also reported.

e. JITC Certification Determination – Joint Interoperability Test Certification. Interoperability test and evaluation quantifies to the Warfighter the degree to which a system will operate in relation to its overall interoperability requirements. The status also conveys the level of risk associated with the system meeting requirements by identifying the expected operational impact of any discrepancies. Status reporting is dependent on the form of requirements (e.g., I-KPP statements qualitatively differ from NR-KPP statements).

f. Foreign Systems. JITC cannot issue a Joint Interoperability Test Certification for foreign systems because requirements are not defined by JCIDS processes. Using an Interoperability Assessment, JITC can report interoperability testing results for foreign systems whose requirements are defined. JITC can also report on the test status of U.S. and foreign programs in combined and coalition environments, when the requirements in these environments are defined. There is also an exception in cases where a foreign program is U.S. sponsored and has defined interfaces with U.S. programs. Additionally, JITC can perform standards conformance certification for foreign systems for any standard affecting interoperability.

g. Homeland Security-Related Systems. JITC test methodologies will treat information exchanges with Homeland Defense (non-Department of Defense (DOD)) systems as any other external interface for the purposes of evaluating DOD system interoperability. Special policy for evaluating interoperability of Homeland Security-related systems themselves has not been established. As with other systems without J-6 certified requirements, JITC cannot issue an interoperability test certification. However, JITC may produce assessments or standards conformance certifications, as appropriate.

h. Stimulators/Simulators and Training Systems. Stimulators/simulators and training systems, separate from operational systems, may be used in the development and testing of IT and NSS and to support exercises. These devices may interface with other systems in the testing environment. Using these systems in a testing environment does not necessarily mean the test is not adequately operationally realistic. Potential differences between the test environment and the operational environment, as well as associated risks, must be considered in accordance with applicable policy before issuing any certification.

(1) JITC may certify stimulator/simulator and training systems in the same manner as operational systems. These systems must have J-6 certified requirements (I-KPP/NR-KPP) for certification. JITC does not certify that these systems provide an accurate model of any particular environment.

i. Validation of Test Tools and Standards. Test tools (and any associated components such as test suites) and standards/standards profiles should be validated before T&E use. JITC does not have the unique mission to validate test tools or standards. However, JITC may contribute to the validation as requested by a standards body or perform validation under the authority used to establish a JITC testing program.

j. Testing Resources include:

(a) Services and Defense Agencies, such as DISA (JITC), the DOD Intelligence Information System (DODIIS) Independent Test Authority (ITA), and USJFCOM JSIC.

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

k. Information Assurance (IA). JITC shall verify that system and network configurations used in testing are representative of a realistic operational environment, to include IA characteristics of the environment. For cryptographic devices, JITC shall confer with the National Security Agency (NSA) and user community, to confirm that IA characteristics of the environment are operationally realistic.

l. Minor System Version Updates - No Test Required. J-6 certified requirements shall be used to determine the appropriate type and amount of testing required, including the situation where no interoperability testing is required. A new system version having only minor changes not affecting interoperability of the system or interfacing systems, nor otherwise impacting the operational interoperability environment may not require interoperability testing, if previously certified. JITC will use information provided by the sponsor and from other sources to decide if the previous certification still applies to the updated version (i.e., that the interoperability status remains unchanged). Since any system modification has the potential of adversely impacting interoperability, a risk assessment will be performed by JITC to determine the probability and consequences of impacts to interoperability. This situation will be documented in an extension of certification letter (see paragraph l.(2) below).

m. Recertification and Extension of Certification. Joint interoperability recertification is required upon any of the following events.

When materiel changes (e.g., hardware or software modifications, including firmware) and similar changes to interfacing systems affect interoperability

Upon revocation of joint interoperability test certifications or JS/J-6 System Validation

Upon automatic expiration 3 years after the date of the certification

When non-materiel changes (i.e., DOTLPF) occur that may affect interoperability

n. Other than the case of an expired certification, any of these events will require additional interoperability evaluation and certification in order to update the interoperability status.

(1) Expired Certifications. If a review of the circumstances for a particular system indicates no change in interoperability characteristics or requirements or J-6 System Validation since the last certification, a new certification may be issued upon expiration. Contact the JITC at least six months prior to expiration to coordinate the recertification effort. A new certification is required to reset the 3-year validity period. This "re-issued" certification may not require additional interoperability testing. However, requirements certification and J-6 validation status shall be reconfirmed. Contact Joint Staff J-6I for to determine specific certification status and clarification of requirements. The status of all interfacing systems must be examined to ensure that their status or requirements with respect to the system under test have not changed. The interoperability environment must not have changed, and the previously certified status should have been verified during exercises or deployments. Only if all of these conditions have been met will a new certification be granted without additional testing. A limited certification where only partial requirements were certified because some requirements (critical or not) were not tested or implemented shall not be reissued. The goal is a certification of all objective requirements.

(2) Certification Extensions ("derived" certification). If a certified system has been modified, but JITC determines that the modifications do not affect interoperability and the interoperability environment and interfacing systems have not changed significantly; the certification may be extended to cover the modified version. Contact the JITC to request/coordinate extensions. The system sponsor should provide a written statement that the modifications do not affect interoperability, along with sufficient information for JITC to independently make a determination of the impact of changes. The extended certification will expire 3 years from the date of the certification being extended (i.e., the extension applies only to the specific system versions being covered, not to the expiration date).

o. Revocation and Re-issuance of JITC Joint Interoperability Test Certifications. There are situations that may warrant the rescinding, revocation, or re-issuance of a Joint Interoperability Test Certification. These situations range from the need to correct simple administrative errors (e.g.,

wrong configuration identified) to serious cases where the J-6 fails to validate the testing and requests the status be reexamined. It is impossible to anticipate all of these situations and the appropriate actions. Everyone that received the original certification notice will be properly notified of any changes.

p. Standards and Standards Profiles Conformance Test Methodology. Standards conformance certification results from testing a system/component for conformity with standards/standards profiles (for information processing, content, format, or transfer). Conformity is characterized with a matrix showing whether an implementation (the hardware/software under test) meets the individual mandatory and optional requirements specified in the standard/standards profile. Certification is confirmation that the system/component meets - as a minimum - all of the mandatory and implemented optional requirements and that there are no critical discrepancies. Other types of products may be extremely useful to the sponsor; however, they do not satisfy requirements for including standards conformance certifications.

(1) Standards conformance certification is based on detailed assessment of protocol elements and other specified requirements. Standards conformance certification means that all mandatory items, and all implemented optional items, are correctly supported. If an optional item fails, it must be removed or disabled. Standards conformance certifications should be based on a test plan that has procedures to test all requirements. A table that shows all requirements (at a level sufficient to show at least the major capabilities supported), what is implemented, and the status. Status must be "rolled up" -- a higher-level item passes only if all subordinate elements pass or are not applicable.

(2) Most standards identify mandatory and optional items and don't necessarily identify the criticality. With complex standards there is almost never 100 percent conformance, so a status of "limited conformance" or "not met, but minor impact or workaround exists" may be appropriate (in effect factoring in criticality).

10. Funding and Other Certifications. The following must also be considered during the interoperability testing process.

a. Funding for interoperability certification, including planning, testing, analysis, and reporting is the responsibility of the program sponsor. Contact JITC for guidance on testing fund planning.

b. There may also be other certifications, validations, or accreditations required prior to fielding a system (e.g., DODI 5200.40 (DITSCAP), IA, and security, electromagnetic spectrum, and authorization to connect to specific networks).

11. Exceptions and Other Considerations. Programs that do not follow the JCIDS process should coordinate with the J-6 to confirm interoperability requirements. Other programs where system components are certified (e.g., network infrastructure components), may have requirements derived from Chairman of the Joint Chiefs of Staff Manuals (CJCSMs), program specifications, or other sources. These will need to be handled on a case-by-case basis, with the sponsor coordinating with JITC and J-6.

a. Some examples of these exceptions are:

(1) Missile Defense Agency – exempt from DOD 5000 requirements until systems are transitioned to the Services.

(2) DSN switches/network components – requirements defined in Joint Staff approved Generic Switching Center Requirements (GSCR), DSN ATM specification, CPDs for network, etc.

(3) In-line encryption devices (security capabilities independently tested and certified by National Security Agency (NSA)).

(4) COTS VTC, network infrastructure components – derived from network or commercial standards.

(5) SATCOM terminals, radios – CPDs for program or FoS; requirements may be derived from multiple documents (e.g., commercial and military SATCOM covered in different requirements documents) or be selected from overall requirements (e.g., JTRS defines requirements for entire program, individual radios would have a subset of requirements).

b. Other categories of systems with special sources of requirements may include foreign and non-DOD systems (without an interface to DOD systems – systems that do interface to DOD systems should have the DOD interfaces documented and the requirements confirmed by J-6).

c. Other considerations include:

(1) For COTS systems and software not requiring formal JCIDS, ISP, or NR-KPP documentation, proponent-sponsored interoperability testing and JITC evaluation/certification shall be conducted prior to IOC.

(2) The MCEB/ITP will resolve issues concerning joint interoperability testing and Joint Interoperability Test Certification. Interoperability issues related to intelligence will be referred to the MIB.

(3) The MCEB/ITP may grant a temporary waiver from interoperability test certification requirements – an ICTO – in special situations, based on justifiable circumstances, impacts, or urgent operational requirements. Note

that there may be exceptions for specific programs (e.g., DSN waivers must be issued from ASD(NII)/DOD CIO).

(4) Additional approval may be required before a system is connected to some networks. The system sponsor is responsible for coordinating these requirements with the appropriate authority. Examples include:

(a) DITSCAP/IA accreditation/certification requirements.

(b) DRSN PMO approval for connection to the DRSN.

(c) TJTN approval for certain tactical networks.

(d) NSA/CSS is the certifier for approved security for protecting classified or national security information (see NSD42).

(5) Life-cycle support.

(a) JITC assesses systems during exercises and operational use to determine if changes to joint architectures, standards, operational concepts, procedures, or interfacing systems have affected interoperability.

(b) JITC also documents the employment of systems that deviate from certified capabilities documents (CPD and ISP, or equivalent). Identified deviations, deficiencies, and uncertified (never certified or expired certification) systems are tracked and reported to J-6 for appropriate action.

12. Related Information

a. The JITC public Web site provides information and access requirements, and points of contact (POCs). JITC maintains a variety of information online, including basic policy and procedures, descriptions of testing programs, program/product registers, and interoperability databases. Refer to: <http://jitc.fhu.disa.mil/>.

b. System Tracking Program (STP). JITC uses the STP to track interoperability information for programs and systems. The STP includes (unclassified) information on requirements documentation, ICTOs, and certification status. Authorized users (.mil/.gov) may refer to: <https://stp.fhu.disa.mil> for instructions on requesting access.

13. Conclusion. The interoperability certification process must begin during interoperability capabilities development and continue throughout the system lifecycle, including testing and fielding. The intent is to detect interoperability deficiencies sufficiently early to ensure that no system is fielded without achieving critical interoperability capabilities. Thorough and continuous coordination among the Joint Staff, JITC, and sponsors is required to ensure

CJCSI 6212.01D

8 March 2006

that systems provided to the warfighter have met the requisite interoperability requirements to support joint operations.

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

ENCLOSURE F

REFERENCES

- a. CJCSI 3170.01E, 11 May 2005, "Joint Capabilities Integration and Development System"
- b. CJCSM 3170.01B, 11 May 2005, "Operation of the Joint Capabilities Integration and Development System"
- c. DODD 4630.5, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- d. DODI 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- 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. Department of Defense Information Technology Standards Registry current Baseline Release located on the NIPRNET at <http://disronline.disa.mil> and on the SIPRNET at <http://disronline.disa.smil.mil/a/DISR>
- h. DODD 8100.1, 19 September 2002, "Global Information Grid (GIG) Overarching Policy"
- i. DODD 3222.3, 8 September 2004, "DOD Electromagnetic Environmental Effects (E3) Program"
- j. DODD 4650.1, 8 June 2004, "Policy for Management and Use of the Electromagnetic Spectrum"
- k. US Department of Commerce, National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management," May 2003 Edition (May 2005 Revision)
- l. CJCSI 6140.01A, 31 March 2004, "NAVSTAR Global Positioning System Selective Availability Anti-Spoofing Module Requirements"
- m. Net-Centric Operations and Warfare (NCOW) Reference Model (RM) (<https://disain.disa.mil/ncow.html>)

- n. DOD Architecture Framework (DODAF)
- o. Global Information Grid (GIG) Architecture, Version 2.0, 9 December 2003, located at <https://disain.disa.mil/ncow.html>
- p. DODD 8500.1, 24 October 2002, "Information Assurance (IA)"
- q. DODI 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"
- r. DODI 8580.1, 9 July 2004, "Information Assurance (IA) in the Defense Acquisition System"
- s. DODI 5200.40, 30 December 1997, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)"¹⁰
- t. End-to-End IA Component of the GIG Integrated Architecture, 26 October 2004, located at <https://gesportal.dod.mil>
- u. Net-Centric IA Strategy, 30 June 2004, located at <https://gesportal.dod.mil>
- v. National Security Space Acquisition Policy 03-01, 27 December 2004
- w. DODD 8320.2, 2 December 2004, "Data Sharing in a Net-Centric Department of Defense"
- x. DOD Chief Information Officer memorandum, 9 May 2003, "DOD Net-Centric Data Strategy"
- y. Subtitle III of title 40, United States Code, Information Technology Management Reform Act of 1996 (Clinger-Cohen Act) as amended by Public Law 105-261 and Public Law 107-217
- z. Federal Information Security Act of 2002, E-Government Act (Public Law 107-347), title III
- aa. Defense Acquisition Guidebook located at <http://akss.dau.mil/dag>
- bb. AsstSecDef memorandum, 21 May 2002, "Department of Defense (DOD) Public Key Infrastructure (PKI)"
- cc. DODD 3020.40, 19 August 2005, "Defense Critical Infrastructure Program (DCIP)"

¹⁰ DODI 8510.1, DOD Information Assurance Certification and Accreditation Process (DIACAP) supersedes DODI 5200.40 and DOD 8510.1-M, DOD Information Technology Security Certification and Accreditation Process (DITSCAP) when approved.

CJCSI 6212.01D

8 March 2006

dd. DODD 8581.1E, 21 June 2005, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense"

ee. DCID 6/1, 1 March 1995 (Administratively updated 4 November 2003), Security Policy for Sensitive Compartmented Information and Security Policy

ff. DCID 6/3, 5 June 1999, Protecting Sensitive Compartmented Information Within Information Systems (administratively updated 3 May 2002, Directive classified)

gg. ASD(C3I) memorandum, 28 August 1998, "Radio Acquisitions"

hh. DODD 5100.35, 10 March 1998, "Military Communications-Electronics Board (MCEB)"

ii. MCEB Pub 1, 1 March 2002, "MCEB Organization, Mission and Functional Manual"

jj. CJCSI 3312.01, 10 November 2004, "Joint Military Intelligence Requirements Certification"

kk. Horizontal Integration JROCM 124-04

ll. CJCSI 6510.01D, 15 June 2004, "Information Assurance (IA) and Computer Network Defense (CND)"

mm. DODD 5101.7, 21 May 2004, "DOD Executive Agent for Information Technology Standards"

nn. CJCSI 5122.01B, 25 March 2003, "Theater Joint Tactical Networks Configuration Control Board Charter"

oo. CJCSI 3470.01, 15 July 2005, "Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) In The Year of Execution"

pp. NIST SP 800-53, Recommended Security Controls for Federal Information Systems, February 2005

qq. ASD(NII)/DOD CIO memorandum, 23 May 2005, "Temporary Suspension of the Joint Tactical Radio Systems (JTRS) Waive Process"

rr. DODI 8551.1, 13 August 2004, "Port, Protocols, and Services Management (PPSM)"

ss. ASD (NII)/DOD CIO memorandum, 26 August 2005, "Information Support Plan (ISP) Acquisition Streamlining Pilot Program"

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

A

| | |
|------------------|---|
| ACAT | Acquisition Category |
| ASD(NII)/DOD CIO | Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer |
| AT&L | Acquisition Technology and Logistics |
| ATD | Advanced Technology Demonstration |
| ATM | Asynchronous Transfer Mode |
| ATO | Authority to Operate |
| AV | All Views |

C

| | |
|--------|---|
| C&A | Certification and Accreditation |
| C2 | Command and Control |
| C2IP | Command and Control Initiative Program |
| C3I | Command, Control, Communications, and Intelligence |
| C4I | Command, Control, Communications, Computers, and Intelligence |
| C4ISP | Command, Control, Communications, Computers, and Intelligence Support Plan |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| CC/S/A | Combatant Commands, Services, Agencies |
| CCB | Configuration Control Board |
| CDD | Capability Development Document |
| CDR | Critical Design Review |
| CES | Core Enterprise Services |
| CFLC | Community Functional Lead for Cryptology |
| CIO | Chief Information Officer |
| CIP | Critical Infrastructure Protection |
| 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 |
| CND | Computer Network Defense |

| | |
|------|----------------------------------|
| COI | Communities of Interest |
| COTS | Commercial off the Shelf |
| CPD | Capabilities Production Document |
| CRM | Comments Resolution Matrix |
| CR | Change Request |
| CSS | Central Security Service |

D

| | |
|---------|---|
| DAA | Designated Approving Authority |
| DAU | Defense Acquisition University |
| DCID | Director of Central Intelligence Directive |
| DCIP | Defense Critical Infrastructure Program |
| DCR | DOTMLPF Change Recommendations |
| DIA | Defense Intelligence Agency |
| DIACAP | Defense Information Assurance Certification and Accreditation Process |
| DICE | DOD Interoperability Communications Exercise |
| DISA | Defense Information Systems Agency |
| DISR | DOD Information Technology Standards Registry |
| DITPR | DOD Information Technology Portfolio Repository |
| DITSCAP | DOD Information Technology Security Certification and Accreditation Process |
| DNI | Director of National Intelligence |
| DOD | Department of Defense |
| DODAF | DOD Architecture Framework |
| DODD | Department of Defense Directive |
| DODI | DOD Instruction |
| DODIIS | DOD Intelligence Information System |
| DOT&E | Director, Operational Test and Evaluation |
| DOTMLPF | Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities |
| DRSN | Defense Red Switch Network |
| DSN | Defense Switch Network |
| DT | Developmental Testing |
| DT&E | Developmental Test and Evaluation |

E

| | |
|-----|---------------------------------------|
| E3 | Electromagnetic Environmental Effects |
| EA | Executive Agent |
| EID | Electrically Initiated Devices |
| EIE | Enterprise Information Environment |
| EMC | Electromagnetic Compatibility |

F

| | |
|--------|--------------------------------------|
| FCB | Functional Capabilities Board |
| FRP DR | Full-Rate Production Decision Review |
| FSA | Functional Solution Analysis |
| FY | Fiscal Year |

G

| | |
|--------|---------------------------------------|
| GEOINT | Geospatial Intelligence |
| GIG | Global Information Grid |
| GIG-ES | GIG Enterprise Services |
| GPS | Global Positioning System |
| GSCR | Generic Switching Center Requirements |

H

| | |
|------|--|
| HERO | Hazards of Electromagnetic Radiation to Ordnance |
| HNA | Host-Nation Approval |

I

| | |
|-------|--|
| I&S | Interoperability and Supportability |
| IA | Information Assurance |
| IAM | Information Assurance Manager |
| IATO | Interim Approval to Operate |
| IAW | In Accordance With |
| IC | Intelligence Community |
| ICD | Initial Capabilities Document |
| ICEP | Interoperability Certification Evaluation Plan |
| ICTO | Interim Certificate To Operate |
| I-KPP | Interoperability KPP |
| IOC | Initial Operational Capability |
| IP | Internet Protocol |
| ISA | Interim Standards Acknowledgement |
| ISP | Information Support Plan |
| ISRP | Interoperability Senior Review Panel |
| ITSC | Information Technology Standards Committee |
| ISSE | Information System Security Engineering |
| ISOP | IT Standards Oversight Panel |
| IT | Information Technology |
| ITP | Interoperability Test Panel |
| ITP | Interoperability Test Plan |
| IWL | Interoperability Watch List |

J

| | |
|---------|---|
| JCD | Joint Capabilities Document |
| JCIDS | Joint Capabilities Integration and Development System |
| JCPAT | Joint C4I Program Assessment Tool |
| JCPAT-E | Joint C4I Program Assessment Tool - Empowered |
| JITC | Joint Interoperability Test Command |
| JPD | Joint Potential Designator |
| JROC | Joint Requirements Oversight Council |
| JSIC | Joint Systems Integration Command |
| JTF-GNO | Joint Task Force for Global Network Operations |
| JTRS | Joint Tactical Radio System |
| JUICE | Joint Users' Interoperability Communications Exercise |
| JWICS | Joint World Wide Intelligence Communications System |

K

| | |
|-------|---------------------------------------|
| KIP | Key Interface Profile |
| KM/DS | Knowledge Management/Decision Support |
| KDP | Key Decision Point |
| KDP-A | Key Decision Point Milestone A |
| KDP-B | Key Decision Point Milestone B |
| KDP-C | Key Decision Point Milestone C |
| KPP | Key Performance Parameter |

L

| | |
|-----|--------------------|
| LDM | Logical Data Model |
|-----|--------------------|

M

| | |
|--------|---|
| MAC | Mission Assurance Category |
| MASINT | Measurement and Signature Intelligence |
| MCEB | Military Communications-Electronics Board |
| MDA | Milestone Decision Authority |
| MIB | Military Intelligence Board |
| MS | Milestone |

N

| | |
|---------|--|
| NATO | North Atlantic Treaty Organization |
| NCES | Net-Centric Enterprise Services |
| NCOW | Net-Centric Operations and Warfare |
| NCOW RM | Net-Centric Operations and Warfare Reference Model |
| NGA | National Geospatial-Intelligence Agency |

| | |
|---------|--|
| NII | Networks and Information Integration |
| NIPRNET | Non-secure Internet Protocol Router Network |
| NR-KPP | Net-Ready Key Performance Parameter |
| NSA | National Security Agency |
| NSS | National Security Systems |
| NSTISSP | National Security Telecommunications Systems and Information Systems Security Policy |

O

| | |
|------|--|
| O | Objective |
| OA | Operational Assessment |
| OASD | Office of the Assistant Secretary of Defense |
| ORD | Operational Requirements Document |
| OSD | Office of the Secretary of Defense |
| OT | Operational Testing |
| OT&E | Operational Test and Evaluation |
| OTRR | Operational Test Readiness Review |
| OUS | Organization Unique Standards |
| OV | Operational View |

P

| | |
|------|---|
| PDM | Physical Data Model |
| PDR | Preliminary Design Review |
| PKI | Public Key Infrastructure |
| PM | Program Manager |
| POC | Point Of Contact |
| POM | Program Objective Memorandum |
| PPS | Precise Positioning Service |
| PPSM | Ports, Protocols, and Services Management |
| PTUC | Participating Test Unit Coordinator |

Q

| | |
|-----|--------------------|
| QoS | Quality of Service |
|-----|--------------------|

R

| | |
|-----|--------------------------------|
| RGS | Requirements Generation System |
|-----|--------------------------------|

S

| | |
|-------|---|
| SAASM | Selective Availability Anti-Spoofing Module |
| SAP | Special Access Program |

CJCSI 6212.01D
8 March 2006

| | |
|---------|---|
| SATCOM | Satellite Communications |
| SCI | Sensitive Compartmented Information |
| SDD | System Development and Demonstration |
| SIGINT | Signals Intelligence |
| SIPRNET | SECRET Internet Protocol Router Network |
| SME | Subject Matter Expert |
| SSAA | System Security Authorization Agreement |
| STP | System Tracking Program |
| SV | Systems View |

T

| | |
|------|---|
| T&E | Test and Evaluation |
| T | Threshold |
| TEMP | Test and Evaluation Master Plan |
| TISP | Tailored Information Support Plan (ISP) |
| TJTN | Theater Joint Tactical Networks |
| TV | Technical Standards View |

U

| | |
|------------|---|
| USA | United States Army |
| USAF | United States Air Force |
| USCENTCOM | United States Central Command |
| USD(AT&L) | Under Secretary of Defense (Acquisition, Technology, and Logistics) |
| USD(C) | Under Secretary of Defense (Comptroller) |
| USD(P) | Under Secretary of Defense (Policy) |
| USEUCOM | United States European Command |
| USJFCOM | United States Joint Forces Command |
| USMC | United States Marine Corps |
| USMS | United States MASINT System |
| USN | United States Navy |
| USNORTHCOM | United States Northern Command |
| USPACOM | United States Pacific Command |
| USSID | US Signals Intelligence Directives |
| USSOCOM | United States Special Operations Command |
| USSOUTHCOM | United States Southern Command |
| USSTRATCOM | United States Strategic Command |
| USTRANSCOM | United States Transportation Command |

X

| | |
|-----|----------------------------|
| XML | Extensible Markup Language |
|-----|----------------------------|

PART II – DEFINITIONS

Acquisition Category (ACAT). Categories established to facilitate decentralized decision making as well as execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. Reference e provides the specific definition for each acquisition category.

Administrative comments. Administrative comments to correct what appear to be typographical or grammatical errors.

Advanced Concept Technology Demonstration (ACTD). A demonstration of the military utility of a significant new technology and an assessment to clearly establish operational utility and system integrity.

Advanced Technology Demonstration (ATD). A demonstration of the maturity and potential of advanced technologies for enhanced military operational capability or cost-effectiveness. ATDs are identified, sponsored and funded by the Services and Agencies.

Architecture. The organizational structure and associated behavior of a system. An architecture can be recursively decomposed into parts that interact through interfaces, relationships that connect parts, and constraints for assembling parts. Parts that interact through interfaces include classes, components, and subsystems.

Capability Development Document (CDD). A document that captures the information necessary to develop a proposed program(s), 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.

Coalition interface. Any interface that passes information between one or more US IT and NSS and one or more coalition partner IT and NSS.

Combined interface. Any interface that passes information between one or more US IT and NSS and one or more allied IT and NSS.

Communities of Interest (COI). Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared vocabulary for the information they exchange (source: reference x)

Critical Comments. Critical comments will cause non-concurrence in a document if comments are not satisfactorily resolved. During a flag-level review, persons commenting are required to contact and coordinate critical comments with document submitters prior to submission of the comments.

Critical Infrastructure Protection. Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.

Defense Agencies. All agencies and offices of the Department of Defense, including the Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency/Central Security Service.

Defense Critical Infrastructure Program. A DOD risk management program that seeks to assure the availability of networked assets critical to DOD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.

Defense-in-Depth. The DOD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness.

DOD Information Assurance Certification and Accreditation Process (DIACAP). Establishes the standard DOD process for identifying, implementing, and validating IA controls, for authorizing the operation of DOD information systems, and for managing IA posture across DOD information systems consistent with the Federal Information Security Management Act (FISMA).

DOD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DOD process for identifying information security requirements, providing security solutions, and managing information system security activities.

DOD Information Technology Standards Registry (DISR). The DISR provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It defines the

service areas, interfaces, standards (DISR elements), and standards profiles applicable to all DOD systems. Use of standards mandated in the DISR is required for the development and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense. The DISR replaced the Joint Technical Architecture.

DOD Interoperability Communications Exercise (DICE). An annual exercise that is sponsored by the Joint Forces Command and conducted by the Joint Interoperability Test Command. DICE is the only exercise dedicated to testing interoperability between systems from each Service, DOD agencies, coalition members, and commercial vendors.

Electromagnetic environmental effects (E3). E3 is the impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including compatibility, interference; vulnerability, pulse; electrostatic discharge; hazards of radiation to personnel, ordnance, and volatile materials; and natural phenomena effects, of lightning and precipitation static.

Emerging KIP. A maturing profile developed by the KIP PM using the SIPRNET DISRonline tool allowing visibility of the state of the system interface design implementing standards projected for inclusion in the KIP. This KIP lifecycle phase provides all PMs the opportunity to plan for incorporating the KIP technical specifications.

Equipment Spectrum Certification. The statement(s) of adequacy received from authorities of sovereign nations after their review of the technical characteristics of a spectrum-dependent equipment or system regarding compliance with their national spectrum management policy, allocations, regulations/instructions, and technical standards. Equipment Spectrum Certification is alternately called "spectrum certification".

Enterprise. A unit of economic organization or activity, i.e., business organization.

Fielded System. Post acquisition IT and NSS operational systems.

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 JROC.

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

GIG Key Interface. GIG key interface is an external presentation through which a GIG enterprise service can be accessed. They are designated as a Key Interface when one or more of the following criteria are met:

- a. The interface spans organizational boundaries. Different entities (service, agency, organization) have ownership and authority over the hardware and software capabilities on either side of the boundary,
- b. The interface is mission critical. Data from joint organizations, multiple services, and/or multiple agencies/organizations must move across the interface to satisfy joint information flow requirements. If systems are not interoperable at that interface, the ability to accomplish the mission is endangered.
- c. The interface is difficult or complex to manage.
- d. There are capability, interoperability, or efficiency issues associated with the interface.
- e. The interface impacts multiple acquisition programs, usually more than two (e.g. network points of presence, many-to-many or one-to-many connections).
- f. The interface is vulnerable or important from a security perspective.

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security Systems, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

IA Component of the GIG Architecture. The set of guiding documents and DODAF products which provides an IA strategy for achieving the assured, integrated, and survivable information enterprise necessary to attain the strategic objectives of the DOD and IC.

Information assurance (IA). 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. (Joint Publication 3-13).

Information Needs. A condition or situation requiring knowledge or intelligence derived from received, stored, or processed facts and data.

Information Support Plan (ISP). The identification and documentation of information needs, infrastructure support, IT and NSS interface requirements and dependencies focusing on net-centric, interoperability, supportability and sufficiency concerns (DODI 4630.8).

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. Information technology 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.

Information Timeliness. Occurring at a suitable or appropriate time for a particular condition.

Initial Capabilities Document (ICD). Documents the need for a materiel solution to a specific capability gap derived from an initial analysis of alternatives executed by the operational user and, as required, an independent analysis of alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects, and time.

Integrated Architecture. An architecture consisting of multiple views or perspectives (Operational View, Systems View, and Technical Standards View) that facilitates integration and promotes interoperability across family of systems and system of systems and compatibility among related architectures. An architecture description that has integrated Operational, Systems, and Technical Standards Views with common points of reference linking the Operational View and the Systems View and also linking the Systems View and the Technical Standards View. An architecture description is defined to be an *integrated architecture* when products and their constituent architecture data elements are developed such that architecture data elements defined in one view are the same (i.e., same names, definitions, and values) as architecture data elements referenced in another view.

Interim Certificate to Operate (ICTO). Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.

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. IT and NSS 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 is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the lifecycle and must be balanced with information assurance.

Interoperability Certification Evaluation Plan (ICEP). A JITC plan, developed in conjunction with the PM/proponent, that establishes a strategy for evaluating interoperability requirements in the most efficient and effective manner, in an operationally realistic environment. This evaluation strategy identifies data necessary to support an interoperability evaluation as well as the test events/environments planned to produce that data. The PM/proponent should coordinate with JITC to integrate interoperability into the system's T&E documents (e.g., Test and Evaluation Master Plan (TEMP), test plans). Complex systems that depend on multiple evaluation events will require JITC to develop an ICEP, in addition to interoperability test plans (ITPs). Separate from any ICEP, ITPs are written for individual test or data collection events. These plans detail the testing and data collection and analysis procedures that apply to that event. Generalized test plans may be applicable to some testing programs where the only variable is the specific system under test (i.e., test configuration, procedures, etc., remain the same).

Interoperability Watch List (IWL). IAW reference g (DODI 4630.8) IT and NSS with significant interoperability deficiencies (as determined by the offices of the USD(AT&L), the ASD(NII)/DOD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, U.S. Joint Forces Command), shall be placed on the IWL to ensure that sufficient attention is given to achieving and maintaining interoperability objectives; and to provide DOD oversight for those IT and NSS activities for which interoperability is deemed critical to mission effectiveness, but interoperability issues are not being adequately addressed. IT and NSS considered for the IWL may be pre-acquisition systems, acquisition programs (any ACAT), already fielded systems, or combatant commander-unique procurements.

J-6 System Validation. Occurs upon completion of both the I&S Certification and the Joint System Interoperability Test Certification provided by JITC. The Validation is valid for three-years from the date of the Test Certification.

Joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (Joint Publication 1-02)

Joint Capabilities Board (JCB). The JCB functions to assist the JROC in carrying out its duties and responsibilities. The JCB reviews and, if appropriate, endorses all JCIDS and DOTMLPF proposals prior to their submission to the JROC. The JCB is chaired by the Joint Staff/J-8, Director of Force Structure, Resources, and Assessment. It is comprised of Flag Officer/General Officer representatives of the Services.

Joint Capabilities Document (JCD). The JCD identifies a set of capabilities that support a defined mission area utilizing associated Family of Joint Future Concepts, 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 functional solution analyses leading to the appropriate Initial Capabilities Document or joint doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) change recommendations, 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 supported Family of Joint Future Concepts, CONOPS or assigned missions.

Joint Capabilities Integration and Development System (JCIDS). A Chairman of the Joint Chiefs of Staff process to identify, assess, and prioritize joint military capability needs. The JCIDS process is a collaborative effort that uses joint concepts and integrated architectures to identify prioritized capability gaps and integrated DOTMLPF solutions (materiel and non-materiel) to resolve those gaps.

Joint Information. Joint Potential Designator used to keep the Services and combatant commands informed of ongoing efforts for programs that do not reach the threshold for JROC Interest or Joint Integration.

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.

Joint Interoperability Test Certification. Provided by JITC upon completion of testing, valid for three years from the date of the certification or when subsequent program modifications change components of the NR-KPP or

supportability aspects of the system (when materiel changes (e.g., hardware or software modifications, including firmware) and similar changes to interfacing systems affect interoperability; upon revocation of joint interoperability test certifications or JS J-6 System Validation; non-materiel changes (i.e., DOTLPF) occur that may affect interoperability).

Joint Interface. An IT and NSS interface that passes or is used to pass information between systems and equipment operated by two or more combatant commanders, Services, or agencies.

JROC Interest. Programs identified by the JROC Secretary as being of interest to the JROC for oversight even though they do not meet the ACAT I cost thresholds or have been designated as ACAT ID.

Key Interface. Interfaces in functional and physical characteristics that exist at a common boundary with co-functioning items, systems, equipment, software and data.

Key Interface Profile (KIP). An operational functionality, systems functionality and technical specifications description of the Key Interface. The profile consists of refined Operational and Systems Views, interface control specifications, Technical View with SV-TV Bridge, and referenced procedures for KIP compliance. The key interface profile is the technical specification that governs access to the GIG.

Key Interface Profile PM (KIP Owner). The Joint Staff/ASD(NII)/DOD CIO designated Program Manager assigned the responsibility for developing a specified external interface governing access to an enterprise service contained within the three GIG ES Key Interface Profile families.

Key Interface Profile Family. Individual KIPs are organized into three families: Transport (define the interface profiles for communications and network components), Computing Infrastructure (define the external interfaces providing access to the computing environment hosting GIG Application Enterprise Services), and Application Enterprise Services (define the interface profiles for software services).

Key Performance Parameters (KPPs). Those capabilities or characteristics considered essential for successful mission accomplishment. Failure to meet a system or program's KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a system or program's KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the JROC. KPPs are included in the acquisition program baseline.

KIPs Declaration. A list identifying applicable KIPs. Key information to be provided includes: KIP family/KIP identification, version identification, applicability and status, threshold/objective indicator, associated interface(s), and implementation statement, as appropriate. The implementation statement expands on the basic declaration to include information on optional elements that are implemented, known deviations, and any necessary configuration details. The categories of KIPs comprise a wide range of interface specifications, from complete interface requirements to protocol specifications for part of an interface. The implementation statement includes additional information on system compliancy to the KIPs (i.e., not all systems may be required to implement 100% of a KIP specification). Implementation and assessment of KIPs compliance will require knowing which key interfaces are implemented and any constraints/parameters associated with the implemented interface(s).

Mandated KIP. A fully mature profile, that can be tested for compliance by the JITC, certified by the J-6, published in DISRonline with an assigned compliance date designated by the ISOP, and available with standards implementations with options and settings for DOD PM use.

Metadata. Information describing the characteristics of data; data or information about data; or descriptive information about an entity's data, data activities, systems and holdings. For example, discovery metadata is a type of metadata that allows data assets to be found using enterprise search capabilities.

Milestone Decision Authority (MDA). The individual designated in accordance with criteria established by the USD(AT&L), or by the ASD(NII)/DOD CIO for acquisition programs, to approve entry of an acquisition program into the next phase.

Milestones. Major decision points that separate the phases of an acquisition program.

Mission Assurance. A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DOD to carry out the National Military Strategy. It links numerous risk management program activities and security related functions -- such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness -- to create the synergistic affect required for DOD to mobilize, deploy, support and sustain military operations throughout the continuum of operations.

Mission Need. A deficiency in current capabilities or an opportunity to provide new capabilities (or enhance existing capabilities) through the use of new technologies. They are expressed in broad operational terms by the DOD components.

National Security Systems (NSS). 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. Information-based operations that use service-oriented information processing, networks, and data from the following perspectives: user functionality (capability to adaptively perform assigned operational roles with increasing use of system-provided intelligence/cognitive processes), interoperability (shared information and loosely coupled services), and enterprise management (net operations).

Net-Centric Operations and Warfare (NCOW). Describes how DOD will conduct business operations, warfare, and enterprise management. It is based on the concept of an assured, dynamic, and shared information environment that provides access to trusted information for all users, based on need, independent of time and place. It is characterized by assured services, infrastructure transparency (to the user), independence of data consumers and producers, and metadata supported by information discovery, protection and mediation. This fundamental shift from platform-centric warfare to net-centric warfare provides for an Information Superiority-enabled concept of operations. The NCOW RM provides a common taxonomy and lexicon of NCOW concepts and terms, and architectural descriptions of NCOW concepts. It represents an important mechanism in DOD transformation efforts, establishing a common framework for net-centricity. It will enable capability developers, program managers, and program oversight groups to move forward on a path toward a transformed, net-centric enterprise.

Net-Centric Operations and Warfare Reference Model (NCOW RM). 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 Global Information Grid (GIG) are realized. The NCOW RM represents the objective end-state for the GIG. 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. The NCOW RM is a key compliance mechanism for evaluating DOD information technology capabilities and the Net-Ready Key Performance Parameter.

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. Net-readiness requires that IT/NSS operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure seamless communications within and across diverse media; information is in a common format with a common meaning; there exist common human-computer interfaces for users; and there exists effective means to protect the information. Net-Readiness is critical to achieving the envisioned objective of a cost-effective, seamlessly integrated environment. Achieving and maintaining this vision requires interoperability:

- a. Within a Joint Task Force/combatant command area of responsibility (AOR).
- b. Across combatant command AOR boundaries.
- c. Between strategic and tactical systems.
- d. Within and across Services and agencies.
- e. From the battlefield to the sustaining base.
- f. Among US, Allied, and Coalition forces.
- g. Across current and future systems.

Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP is a key, measurable, performance parameter stating a system's information needs, information timeliness, information assurance, and net-ready attributes

required for both the technical exchange of information needs, information timeliness, information assurance, 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 consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM) (reference m), supporting integrated architecture products (references n and o) required to assess information exchange and operationally effective use for a given capability, compliance with applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) (<http://kips.disa.mil>), and verification of compliance with DOD information assurance requirements (references p through u).

NR-KPP Certification. Required by ASD (NII)/DOD CIO for ISPs, J-6 provides this certification in the form of an I&S certification

Open Standard. Widely accepted and supported standards set by recognized standards organizations or marketplace. These standards support interoperability, portability, and scalability and are equally available to the general public at no cost or with a moderate license fee.

Operational View (OV). An architecture view that describes the joint capabilities that the user seeks and how to employ them. The OVs also identify the operational nodes, the critical information needed to support the piece of the process associated with the nodes, and the organizational relationships.

Spectrum Supportability. The determination as to whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or system during its expected lifecycle is, or will be, available (that is, from system development, through developmental and operational testing, to actual operation in the electromagnetic environment.) The assessment of equipment or system as having “spectrum supportability is based upon, as a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of electromagnetic compatibility (EMC).

Substantive Comment. Substantive comments are provided because sections in the document appear to be or are potentially unnecessary, incorrect, incomplete, misleading, confusing, or inconsistent with other sections.

Systems View (SV). 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.

CJCSI 6212.01D

8 March 2006

Technical Standards View. The Technical Standards View (TV) provides the technical systems-implementation standards upon which engineering specifications are based, common building blocks are established, and product lines are developed.

Top-Level Exchanges. Top-level refers to exchanges between systems of Combatant Command/Service/agency, Allied, and Coalition partners.

CJCSI 6212.01D
8 March 2006

(INTENTIONALLY BLANK)