CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6212.01E
DISTRIBUTION: A, B, C 15 December 2008

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure G.

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 of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems (references a and b).

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

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

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

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

g. Adds the requirement from Joint Requirements Oversight Council Memorandum (JROCM) 010-08, 14 January 2008, "Approval to Incorporate Data and Service Exposure Criteria into the Interoperability and Supportability Certification Process" for reporting of data and service exposure information as part of I&S submissions.

2. Cancellation. CJCSI 6212.01D, 8 March 2006, "Interoperability and Supportability of Information Technology and National Security Systems" is canceled.

3. Applicability. This instruction applies to:

a. Joint Staff, Services, combatant commands, defense agencies and joint and combined activities. This instruction also applies to other agencies preparing and submitting JCIDS documents IAW references a and b.

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

(1) All programs of record, regardless of ACAT, require I&S certification. I&S certification authority is delegated to C/S/As for ACAT II and below programs of record without joint interface requirements. ACAT programs include all DOD 5000-Series (references e and f) and post-acquisition/ procurement (fielded) IT and NSS acquisition systems.

(2) Non-ACAT activities and procurements, and fielded systems. Non-ACAT activities and procurements include all defense IT and NSS projects, IT and NSS pre-acquisition demonstrations such as Advanced Concept Technology Demonstrations (ACTD), Advanced Technology Demonstrations (ATD), 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 including 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; government off the shelf (GOTS) software, and post-acquisition (fielded) IT and NSS.

(3) 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.

(4) 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 sensitive information. Accordingly, implementation of this instruction must be tailored to comply with Director of National Intelligence (DNI) directives and intelligence community policies.

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

(6) All component IT and NSS supporting business areas and domains within DOD.

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

4. Organization of Enclosures

a. Enclosure A. Policy Overview.

b. Enclosure B. Life Cycle Process Overview.

c. Enclosure C. Responsibilities. Outlines the stakeholder responsibilities in the I&S policies and processes described in this instruction.

d. Enclosure D. Staffing Process and Certification Procedures. Provides additional detail on the processes for submission of documentation for I&S review and certification for all IT and NSS.

e. Enclosure E. Determining Interoperability, Supportability and Net Readiness. This enclosure describes the technical aspect of determining I&S, including the NR-KPP and compliance with DOD IT and NSS specific policies.

f. Enclosure F. Joint Interoperability Testing and Certification Process. This enclosure details the policy and processes for joint interoperability test certification of IT and NSS over their lifecycle.

g. Enclosure G. References.

h. Enclosure GL. Glossary of Definitions, Acronyms and Abbreviations

5. Definitions. See Enclosure GL, Part II.

6. Responsibilities. See Enclosure C.

7. Summary of Changes. This revision:

a. Prescribes the use of the Joint Common System Function List (JCSFL) as the methodology to describe IT and NSS functionality in a common lexicon.

b. Adds the "Net-Centric Data/Services" element to the NR-KPP.

c. Adds the "Supportability" element to the NR-KPP.

d. Adds requirement to include Data and Services Exposure verification.

e. Deletes the “Key Interface Profile” element of the NR-KPP and replaces it with the "Technical Standards/Interfaces" element.

f. Deletes the "Network-Centric Operations and Warfare-Reference Model" element of the NR-KPP and adds compliance items from this element into the "Net-Centric Data/Services", “solution architectures”, and “Information Assurance” elements.

g. Establishes the Information Support Plan (ISP), Tailored ISP or ISP Annex as the preferred reference for all technical artifacts mandated for I&S certification compliance. Introduces the Enhanced ISP (EISP) Tool as a preferred tool to be used to create ISP documents to facilitate the development of a standard ISP format and assist programs in risk mitigation.

h. Changes the Joint Interoperability Test Certification periodicity from three years to four years.

i. Adds Test Exemptions and Legacy Waiver Process.

j. Adds I&S Certification and Testing criteria for incremental fielding of Services and Applications.

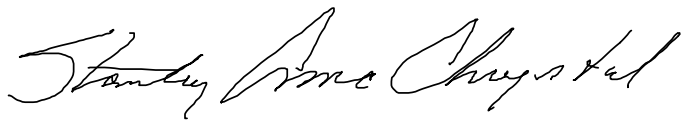
k. Introduces GIG Technical Guidance (GTG) as an emerging source for technology guidance and standards implementation information used in describing GIG Enterprise Service Profiles (GESPs) to meet the net-centric operational requirements specified in the CDD/CPD and ISP as identified in the TV review.

l. Authorizes the use of C/S/A Test Agencies and Operational Assessment and Evaluation Reports (OAR/OER) to evaluate the operational effectiveness of the interoperability and information exchanges outlined in the NR-KPP integrated architecture products and information assurance posture. Proposes Operational Testing address interoperability through the use of common outcome-based assessment methodologies as part of the evaluation of system effectiveness. The OARs and OERs will support the certification that information exchanges are operationally effective and enhance mission accomplishment.

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, CJCS Directives Home Page, http://www.dtic.mil/cjcs_directives.

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

For the Chairman of the Joint Chiefs of Staff:



STANLEY A. MCCHRYSTAL
Lieutenant General, USA
Director, Joint Staff

Enclosures:

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

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

FIGURE Page

TABLE Page

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY OVERVIEW

1. Policy. It is Joint Staff policy to assure that DOD components develop, acquire, deploy, and maintain IT and NSS that (1) meet the essential operational needs of U.S. forces; (2) are interoperable with existing and proposed IT and NSS through standards, defined interfaces, modular design, and reuse of existing IT and NSS solutions; (3) are supportable over the existing and planned Global Information Grid (GIG); (4) are interoperable with allies, coalition partners and other U.S. and local agencies as appropriate; (5) allow U.S. forces to protect mission essential data and to detect and respond to network intrusion/system compromise; and restore mission essential data; (6) leverage emerging capability-based references and methods, including the Joint Capability Areas (reference a), as a common language to discuss and describe capabilities across many related Department activities and processes; and (7) incorporate records management requirements into automated information systems development and redesign.

a. DOD combatant commands/Services/Agencies (C/S/A) play a key role in assuring consistent interoperability is appropriately inculcated into the capability's life cycle. The C/S/A will institute appropriate controls to assure C/S/A capability interoperability and verify compliance and alignment of all capability and materiel development activities in support of this policy.

b. All IT and NSS and modifications to existing IT and NSS that impact the interoperability capabilities of the program shall be compliant with DOD regulations and policies (references c through j and u through w). The NR-KPP is a mandatory element of Capability Development Documents (CDDs), Capability Production Documents (CPDs), Information Support Plans (ISPs) and Tailored Information Support Plans (TISP) for IT and NSS that communicate with external systems. Establishing and maintaining Interoperability and Supportability (I&S) in a DOD system is a continuous process that must be managed throughout the lifecycle of the system.

c. I&S Certification verifies adherence to the NR-KPP throughout the life-cycle by analyzing requirements documents, ISPs, and testing plans for appropriate requirements characterization and execution of the five elements of the NR-KPP.

d. A NR-KPP, consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, information assurance (IA), and net-ready attributes required for both the technical

exchange of information and the end-to-end operational effectiveness of that exchange.

e. The five NR-KPP elements are (1) compliant solution architecture; (2) compliance with net-centric data and services strategies; (3) compliance with applicable GIG Technical Guidance (GTG); (4) compliance with DOD Information Assurance (IA) requirements; and, (5) compliance with supportability requirements to include spectrum utilization and information bandwidth requirements, Selective Availability Anti-Spoofing Module (SAASM) and the Joint Tactical Radio System (JTRS), as applicable.

f. The Joint Staff (JS) I&S Certification process is an integral part of the JCIDS process. I&S Certifications granted under the former CJCSI 6212.01D remain valid (including for use in JITC Test Certification); however, all capabilities documents supporting a Milestone B or Milestone C decision will include applicable NR-KPP elements from the effective version of this document. Capability documents entering the review cycle within six months of the release date of this version (CJCSI 6212.01E) may seek compliance with either the current version or the previous version (CJCSI 6212.01D). See National Security Space Acquisition Policy 03-01 (reference t), for space program key decision points.

g. I&S Certification of IT and NSS.

(1) The requirement for I&S Certification of IT and NSS capabilities for ACAT programs will be determined during the JCIDS process and will be updated prior to each milestone and reviewed prior to recertification every four years, or when significant changes occur throughout the operational life of a system.

(2) Table A-1 summarizes the JS I&S Certification requirements of IT and NSS. The entries in the table reference the document(s) containing the detailed procedures.

(3) I&S of IT and NSS capabilities for non-ACAT and fielded systems will be determined by the approving authority and will be updated as necessary throughout the acquisition period, deployment, and operational life of a system. J-6 will provide Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DOD Chief Information Officer (CIO) an I&S certification on ISPs submitted by C/S/A; however, ASD(NII) makes the final determination of acceptance on all ACAT I, IA and special interest ISPs.

IT&NSS Program		ICD	CDD	CPD	TISP	ISP*
JCIDS JPD	**JROC Interest**		1	1		2
	JCB Interest		3	3		2
	Joint Integration		1	1	2	2
	Joint Information **				2	2
	Independent				2	2
OSD Special Interest ***						4
Non-ACAT					2	2
Fielded Systems					2	2
Incrementally Delivered Services / Applications						2
I&S Certification Governing Directives 1: CJCSI 3170.01 and CJCSI 6212.01 2: CJCSI 6212.01 3: JRCOM 130-08 and CJCSI 3170.01G (pending) 4: DODI 4630.8		Certification requirements for ISP annexes and ISPs developed using the EISP tool are the same as those for ISPs ** Joint Information Joint Potential Designator (JPD) per CJCSI 3170.01 may be elevated to JROC Interest or Joint Integration *** All programs of record, regardless of ACAT, require I&S certification. I&S certification authority is delegated to C/S/As for ACAT II and below programs of record without joint interface requirements.					

Table A-1. I&S Certification Summary

h. All IT and NSS with Joint interfaces must obtain an Interim Certificate to Operate (ICTO) from the Military Communications-Electronics Board's (MCEB) Interoperability Test Panel (ITP) if a requirement exists to operate within the GIG prior to achieving JITC Joint Interoperability Certification. A status report of IA activities shall be obtained prior to JITC interoperability testing and certification. The JITC Joint Interoperability Test Certification is valid for four years from the date of the certification or until changes occur that may affect the interoperability of the certified capability. Some IT & NSS that meet the eligibility criteria outlined in Enclosure C and Enclosure E may request waivers or test exemptions.

(INTENTIONALLY BLANK)

ENCLOSURE B

LIFE CYCLE PROCESS OVERVIEW

1. This enclosure provides an overview of the I&S Certification process within the overall DOD IT and NSS Acquisition Life Cycle. To accomplish this, the following activities are built into each phase of the life cycle to focus the net-centric or interoperability considerations and measure effectiveness. Interoperability assessments are conducted throughout the life cycle to identify and resolve potential interoperability and/or emerging net-centricity challenges, mitigating the risk of delivering non-interoperable capabilities to the warfighter.

a. The general steps are:

(1) Establish overarching interoperability & net-centric requirements as defined in the Net-Ready Key Performance Parameters (NR-KPP).

(2) Execute document reviews, architecture development, and analyses to identify potential interoperability issues early in the life cycle.

(3) Evaluate the ISPs against related architecture artifacts to identify potential interoperability disconnects between interdependent systems or services. ISPs document the detailed information exchange or technical information sharing strategies.

(4) Establish and certify Joint Threads (JTs) to document and characterize capability information and data exchanges. The information and data exchanges identified in the ISP are evaluated against the established JTs to analyze whether the system effectively supports the capability information sharing requirements without breaching net-centricity or interoperability of the capability and the supporting network.

(5) Complete the Defense Information Systems Agency (DISA)/JITC Joint Interoperability Test Certification based on supported information flow and information exchange requirements documented or specified in the J-6 I&S certified capabilities documents.

b. Interoperability is further ensured through stringent configuration management of approved interfaces or standards prior to employment in the joint operation environment. Stringent configuration management of these interfaces or standards will mitigate the potential for unauthorized modification to fielded systems that may negatively impact interoperability.

c. Early identification and resolution of interoperability issues minimize negative impact to the joint, multi-national, interagency, and warfighter community. Architectures are foundational to effectively evaluating the probability of interoperability and net-centricity. Interoperability testing verifies the actual capability net-centric/interoperability characteristics.

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 (i.e., DOD and its components) to 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 (NSSAP) 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. The Defense Acquisition Guidebook (reference aa) and the Defense Acquisition University (DAU) are primary sources of acquisition guidance. CJCSI 6212.01 supports these acquisition policy and instruction documents by providing I&S Certification at key milestones.

d. DOD 4630 Series. The DOD 4630 Series publications prescribe policy for establishing and maintaining I&S for all IT and NSS throughout their lifecycle. DODI 4630.8, “Procedures for I&S of Information Technology (IT) and National Security Systems (NSS)” introduces and establishes the requirement for an 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 supports the DOD 4630 policy to help ensure all non-ACAT, ACAT, and fielded systems are interoperable and supportable throughout their lifecycle.

e. CJCS 3170 Series Documents. CJCSI 3170.01 prescribes 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 with advice and an assessment on acquisition programs in support of the Defense Acquisition Process. CJCSI 6212 provides in detail how the J-6 performs I&S certification of JCIDS documents required by acquisition programs for milestone decisions.

f. DODD 8320.02. DODD 8320.02, "Data Sharing in a Net-Centric Department of Defense". Implements the DOD Net-Centric Data Strategy and 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. The DOD Net-Centric Services Strategy defines similar characteristics for services on the GIG. This instruction outlines the policy for net-centric data and services as part of I&S Certification.

g. DOD and Joint Staff IA Policies. IA is one of the five 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 or critical infrastructure protection (CIP) policies and processes, such as DODI 8510.01, "DOD Information Assurance Certification and Accreditation Process (DIACAP), rather this instruction synchronizes these policies and processes with those established for interoperability and supportability in CJCSI 6212.01.

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 (EMC) aspects.

i. DODD 3222.3, "DOD Electromagnetic Environmental Effects (E3) Program" (reference i). This directive provides policies and responsibilities to ensure mutual Electromagnetic Compatibility 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 refinement and technology development

phases and included in the pertinent acquisition and verified throughout the acquisition process.

j. Figure B-1 illustrates the general relationship between the DOD acquisition, JCIDS, I&S Certification processes and Interoperability Testing and Certification documentation.

k. URLs for (I&S) Internet resources are located on the CJCSI 6212 Resource Page https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page - This page will be kept up-to-date as websites change. If unable to access the Resource Page for any reason, contact the J-6 for further guidance.

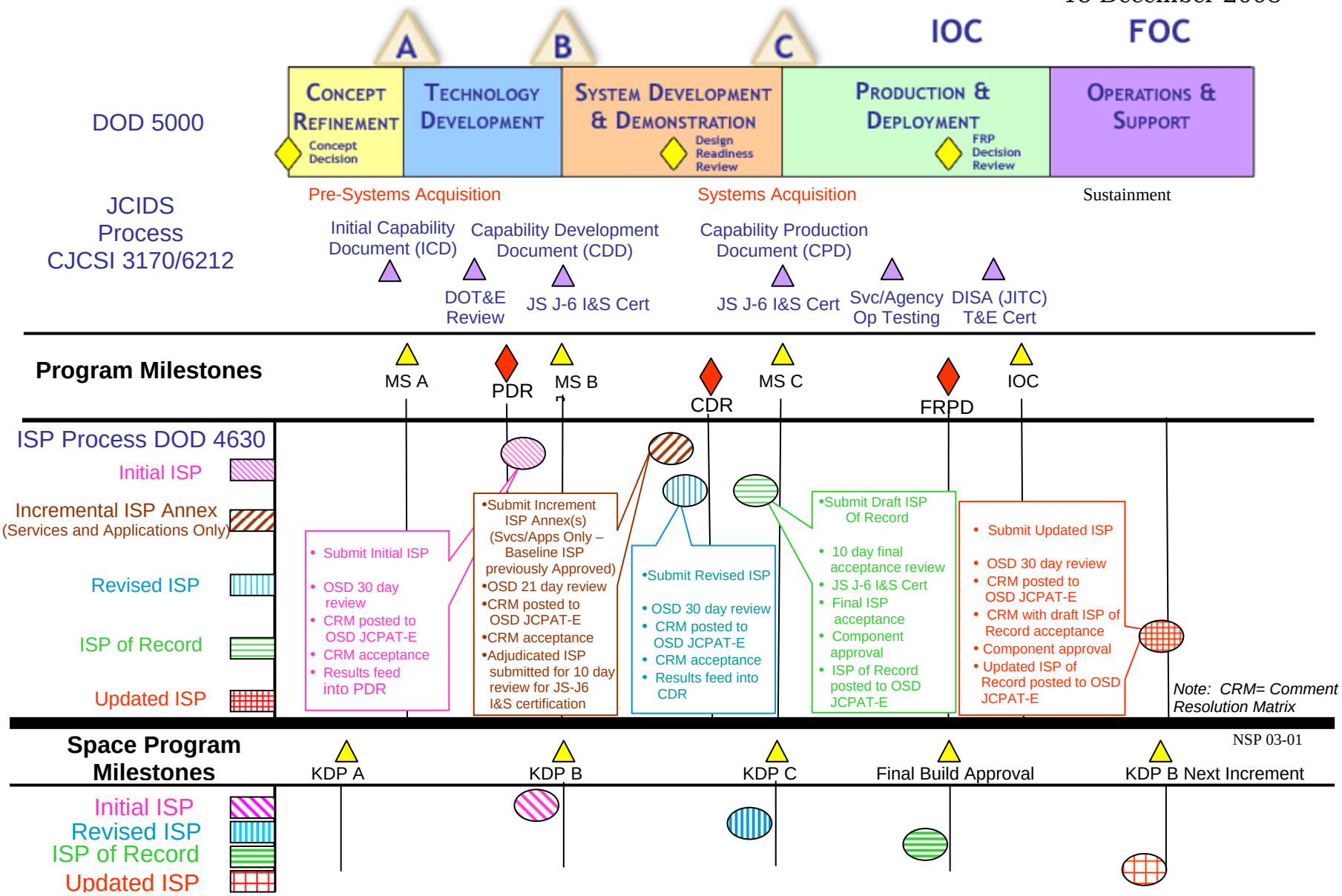


Figure B-1. Relationship between the DOD acquisition, JCIDS, and I&S Certification processes

(INTENTIONALLY BLANK)

ENCLOSURE C

RESPONSIBILITIES

1. The Joint Staff, J-6 will:

a. Perform IT and NSS I&S Certifications IAW Table A-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 I&S Certification to ASD(NII)/DOD CIO for ACAT I programs and programs designated as OSD Special Interest (IAW reference f) or for programs which the ASD(NII)/DOD CIO has indicated a special interest (IAW reference d); however, ASD(NII) makes the final determination of acceptance on all ISPs.

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

(4) Promote, evaluate, and validate interoperability test processes designed and implemented under authority of service/agency OTAs. Evaluation will be conducted by an outcomes-based assessment methodology; while the interoperability test processes may vary among the OTAs, the metrics and measures applied to determine effectiveness of each interoperability process will be based on common standard and will include evaluation of each test activity/organization's application of the NR-KPP.

b. Attend all Joint Capability Boards and Joint Requirement Oversight Council meetings to provide I&S Certification results. Conduct a J-6 Net-Centric FCB Working Group assessment of all Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) Change Recommendations (DCR) through related FCBs.

c. Review ISP submissions and facilitate participation in the collaborative department-wide configuration management process to develop and validate GTG-based guidance and products.

d. Coordinate IT and NSS I&S policies, procedures and programs with combatant commands/Services/Agencies (C/S/A).

e. Conduct Military Communications-Electronics Board (MCEB) Pub 1 responsibilities (references hh and ii), which includes chairing the MCEB Interoperability Test Panel (ITP) and the MCEB Interoperability Panel (IP).

f. Designate a Point of Contact (POC) to act as Executive Agent (EA) of the Joint C4I Program Assessment Tool-Empowered (JCPAT-E).

g. Ensure that Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)), Assistant Secretary of Defense (Networks and Information Integration) / Department of Defense Chief Information Officer (ASD (NII)/DOD CIO), Director Operational Test and & Evaluation (DOT&E),and other DOD components have the earliest opportunity to participate in or review JCIDS documents and ISPs for I&S of IT and NSS.

h. Review legacy systems for applicability of the NR-KPP.

i. Review architecture products, Data and Service Exposure Verification Tracking Sheets and other submissions to determine compliance with the Net-Centric Data Strategy and Net-Centric Services Strategy.

j. Participate in Capability Portfolio Management (CPM) focus areas and on capability analysis and assessment teams, as appropriate.

k. Maintain the CJCSI 6212 Resources Page at https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page

2. The combatant commands will:

a. Review and comment on interoperability and supportability aspects of programs during the J-6 I&S certification process. Provide feedback to the appropriate Title 10 supporting entity on the results of combatant command conducted interoperability testing

b. Participate in or support, as appropriate, IT and NSS joint interoperability testing programs (for programs under the combatant commander's title 10 Authority) by planning, programming, budgeting, executing and providing resources IAW agreed-to schedules and test plans. Fund required interoperability testing and certifications.

c. Prioritize interoperability requirements in support of capability-focused joint assessment, design, development, and testing.

d. In coordination with the DISA (JITC), develop joint interoperability Test and Evaluation (T&E) criteria and/or requirements for inclusion in system acquisition documents, Test and Evaluation Strategy (TES), Test and Evaluation Master Plans (TEMP), and other test plan submissions.

e. Provide input for the Interoperability Watch List (reference d) based on the observations of the Executive Agent 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 in Capability Portfolio Management (CPM) focus areas and on capability analysis and assessment teams, as appropriate.

g. Provide input to the J-6 and/or DOT&E regarding significant changes in systems and/or architectures that will be employed during combatant command exercises and/or prior to deployment in an operational environment. Significant changes can include the implementation of new IT and NSS equipment or software, as well as upgraded versions of currently used IT and NSS equipment or software that affect systems' interoperability.

h. Establish access to the JCPAT-E.

3. U.S. Joint Forces Command (USJFCOM) as the DOD Command and Control (C2) CPM, joint capability developer and chief advocate for interoperability will:

a. Under their responsibilities in DODD 5100.30 as the lead integrator for C2 capabilities and as the C2 CPM, provide JCIDS and other review comments in order to advise the Joint Staff on the C2 interoperability and sustainability of IT and NSS capabilities.

b. Serve as the joint force integrator of DOD. USJFCOM, as the Chairman's Advocate for interoperability, may require selected programs' and systems' interoperability assessments using the Joint Systems Integration Command (JSIC). These assessments are based on the warfighter's perspective using joint mission threads linked to the universal joint task list (UJTL). These assessments do not replace the JITC interoperability test certification. However, JITC as the Joint interoperability test certifier may elect to use assessment results to issue the Joint Interoperability Test Certification.

c. Use other exercise venues as available (e.g., Joint Users' Interoperability Communications Exercise (JUICE), Coalition Warrior Interoperability Demonstration (CWID), and DOD Interoperability Communications Exercise (DICE), or combatant command exercises) for system, program or mission thread based interoperability assessments. Another available venue is JSIC's Joint Systems Baseline Assessment (JSBA). JFCOM is the supporting combatant commands for JUICE, DICE, and JSBA.

d. Maintain the Joint Common System Function List (JCSFL) in coordination with the Services. The JCSFL provides, as applicable, a common lexicon for warfighter system functionality that includes (1) C4ISR, (2) weapon system; and, (3) those system functions that support Joint Force mission sustainment capabilities, such as: Logistics, Medical Support, Personnel Support, System Maintenance, System Test, System Protection, and Training. The JCSFL also provides the traceability of Military Services' Common System

Function Lists (CSFLs) functions to their joint equivalent, for interoperability and comparative analyses. This information can be accessed at the JCSFL Portal Page on DKO at: https://www.us.army.mil/suite/page/419489.

e. Sponsor JUICE and DICE. Ensure Services and Agencies support these interoperability certification exercises and efforts. Assist JITC with planning, coordination, and conduct of the exercises. Coordinate with TJTN and JITC on the development of event announcement messages.

f. Review programs for applicability of the NR KPP and potential interoperability issues.

g. Participate in Capability Portfolio Management (CPM) focus areas and on capability analysis and assessment teams, as appropriate.

h. Establish access to the JCPAT-E.

4. U.S. Strategic Command (USSTRATCOM) will:

a. Review any programs planned to support global strike, missile defense, intelligence, surveillance and reconnaissance, information operations, and space operations.

b. As the Joint Task Force for Global Network Operations (JTF-GNO), assist the DISA and the National Security Agency (NSA) in reviewing and defining IA standards.

c. Participate in Capability Portfolio Management (CPM) focus areas and on capability analysis and assessment teams, as appropriate.

d. Establish access to the JCPAT-E.

5. Military Services, Defense Agencies and U.S. Special Operations Command (USSOCOM) will:

a. Ensure all IT and NSS requirements and capabilities are documented and certified (IAW references a through d and ss) for Service or Agency systems with external joint and combined interfaces with other Service or agency programs and systems.

b. Ensure interoperability activities required by this policy are compliant with C/S/A and Joint/DOD interoperability strategies.

c. C/S/A assure that required documentation/activities are appropriately prepared/conducted prior to submission to the Joint and/or DOD staff for review and approvals.

d. 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. Fund required interoperability testing and certifications.

e. In coordination with the DISA (JITC), develop interoperability test and evaluation criteria, measures, and requirements for inclusion in acquisition documents, TES, 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 or net-centric capabilities undergo and successfully complete joint interoperability test and evaluation IAW these criteria. This includes any limited or prototype Initial Operational Capability (IOC) fielding.

f. Ensure that an All View-1 (AV-1) is registered in the DOD Architecture Registry System (DARS). Ensure all other DODAF architecture artifacts developed are registered and maintained in DARS once approved.

g. Comply with applicable standards mandated in the DISR and use DISRonline as the system of record for development of TVs.

h. Consider the applicable GIG Technical Guidance (GTG) to include DOD Information Technology Standards and Profile Registry (DISR) mandated IT Standards reflected in the Technical View-1 (TV-1). Consideration will be given to implementation guidance of those standards used in applicable GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Information Enterprise Architecture and solution architecture system/service views. GTG content will be evolutionary in nature and, as developed and validated, will be released for use through a JROCM.

i. Ensure all IT or NSS systems or net-centric capabilities are compliant with current DOD IA directives and policies.

j. Ensure IA requirements are identified and included at the earliest stage of acquisition.

k. Ensure the CDD and CPD NR-KPPs along with other KPPs are used as the authoritative source for interoperability requirements baseline to develop the ISP and the Test and Evaluation Master Plan (TEMP). Ensure that the solution architectures documented in the ISP align with those presented in the capabilities documents. Further, ensure critical technical and operational issues identified during the CDD/CPD development shall be included in the follow-on technical analysis.

l. For the DISA (JITC) standards conformance and Joint Interoperability Test Certification:

(1) Coordinate funding for all IT and NSS with the DISA (JITC) prior to a test event (initiation of the 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.

(2) Consider funding for the Service/Agency Participating Test Unit Coordinator (PTUC).

m. For systems or net-centric capabilities being acquired (under reference f), ensure a TEMP is approved prior to Milestone B. This ensures the system will complete interoperability testing certification prior to fielding decision (i.e., Full Rate Production Design Review) IAW criteria. Actual interoperability certification testing will occur after Milestone B and be integrated throughout Operational Testing. For space systems being acquired (under reference t), ensure a TEMP is approved prior to Key Decision Point B (KDP-B) that ensures the system will complete interoperability testing certification prior to IOC declaration IAW criteria. Actual interoperability testing certification may occur after KDP-B and will be integrated throughout Operational Testing. Ensure TES and TEMP include strategies and the identification of resources to test in the expected joint operational environment and opportunities to assess with dependent and related programs/systems providing similar key capabilities to meet the warfighter's need.

n. Provide direction to acquisition managers and program managers to ensure that all IT and NSS are certified and tested for interoperability IAW Table A-1. All program managers must include assessments and testing in the joint operational environment to ensure integrated, interoperable capability (DOD Strategic Planning Guidance (SPG) and Capability Portfolio Management alignment)

o. Provide guidance to all program managers and Operational Test Agencies (OTAs) to ensure that IA hardware and software capabilities are assessed on and meet IA C&A requirements as established by DODI 8500.2 (reference o) and CJCSI 6510.01 (reference ll). Align early assessment and testing opportunities, as appropriate, to reduce integration and interoperability risk.

p. Ensure funding is planned for:

(1) I&S Re-Certification

(2) Incorporating the NR-KPP and required interfaces for legacy systems into their ISPs.

(3) IA Certification and Accreditation (C&A) (e.g. Designated Approving Authority (DAA), Authorization to Operate (ATO)).

q. USSOCOM, under its Title 10 authority and responsibilities for independent requirements approval, will establish I&S criteria for Special Operations (SO)-peculiar IT systems."

r. Participate in Capability Portfolio Management (CPM) focus areas and on capability analysis and assessment teams, as appropriate.

s. U.S. Special Operations Command (USSOCOM) will review any programs that facilitate Global Operations Against Terrorist Networks planning synchronization.

t. Establish access to the JCPAT-E.

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

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

b. Exercise the DISA's role as the DOD EA for IT standards 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 but coordinate with the Defense Standardization Office (DSO) on military standards, and the DISRonline is used to develop and publish all Technical Standards Profile (TV-1s) and Technical Standards Forecast (TV-2s) referenced in CDDs, CPD, ISPs & TISPs.

d. Lead a collaborative department-wide process to ensure stakeholder participation in development of and validation of GTG-based guidance and artifacts. This process will include working groups and Integrated Product Teams (IPTs) to develop products (principally GIG Enterprise Service Profiles) and a representative, properly chartered senior engineering board to review and approve the work of these groups. The senior engineering board will be empowered to approve for posting properly coordinated and validated GESPs where there is community agreement. Where there are substantive disagreements, issues will be raised to the IT Standards Oversight Committee (ISOP) for vetting and adjudication.

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

f. Provide an assessment of the suitability of standards and standards profiles identified in IT and NSS of TISPs/ISPs/CDDs/CPDs submitted under this instruction.

g. Establish and conduct, in collaboration with other DOD components, the JITC Joint Interoperability Testing and Certification program for applicable IT and NSS.

h. Provide testing standards (best practices, comments, recommendations and lessons learned), guiding principles, procedures, and developmental interoperability testing assistance to DOD components, agencies and system developers to implement solutions, ensure maximum interoperability and minimum duplication, and to ensure Service/Agency executed interoperability testing can be leveraged by JITC to fulfill JITC Certification requirements.

i. Review all available Test and Evaluation Master Plans and provide acquisition managers with recommended interoperability test and evaluation measures. Review recommendations for security test and evaluation criteria for inclusion in test plans as part of Test and Evaluation Master Plan Working Groups. Evaluate and recommend interoperability test and evaluation measures.

j. Coordinate with National Security Agency (NSA) regarding the inclusion of IA standards in the DISRonline.

k. Provide JITC Interoperability Test Certification results to the MCEB Interoperability Test Panel (ITP); post these results in the System Tracking Program (STP) and the JCPAT-E.

l. Notify the J-6 and PM NLT 180 days prior to any Test Certification expiration.

m. Publish an annual report to the Joint Staff J-6, USD (AT&L), ASD (NII)/DOD CIO, DOT&E, DOD EA for Space, USJFCOM, Military Services, and Program Offices containing an executive summary of systems tested for IT and NSS interoperability by functional area.

n. Provide for systems engineering, planning, community collaboration, and directive technical guidance to identify issues and provide design tenets or guidelines and associated standards that are required and need to be supported by individual IT and NSS programs. These solutions will be specified as part of the GIG Technical Guidance (GTG). This systems engineering construct provides the specific design guidance needed to ensure that the independently developed component programs of the GIG work in concert to provide a cohesive enterprise information environment.

o. 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.

p. In coordination with NSA, review and define IA standards.

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

r. Provide test tools and procedures, and support systems in support of interoperability and standards conformance testing. Verify test tools and procedures for interoperability and standards conformance testing. When directed, or requested, and resourced, verify interoperability and standards conformance test tools and procedures developed by other organizations.

s. Coordinate with the Designated Accrediting Authority (DAA), for any DOD system that collects, stores, transmits, or processes information, to ensure IA testing considerations are addressed in interoperability testing.

t. 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.

u. As the DOD Executive Agent for IT Standards, allocate resources to manage and develop, in accordance with DODI 5025.01 and ASD(NII) memorandum, 10 February 2006, "Establishment of Enterprise Documentation Framework Working Group (EDFWG)", GIG Technical Guidance (GTG) and supporting standards configuration management and test certifications in support of the ASD(NII)/DOD CIO and the Chairman of the Joint Chiefs of Staff.

v. 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.

w. Designate a central office to act as system manager of the JCPAT-E.

x. Ensure the DISA (JITC) utilizes and leverages adequate, coordinated C/S/A testing in the system's joint interoperability certification process, therefore combining valuable resources and ultimately testing once.

7. The Joint Staff, J-2, will:

a. Conduct the Intelligence Certification of JCIDS documents in a separate process related to the JCPAT-E process (IAW reference jj), that examines intelligence support needs for completeness, supportability, and impact on

joint intelligence planning. This certification also considers the sufficiency of horizontal integration (IAW reference kk).

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

c. Participate in Capability Portfolio Management (CPM) focus areas and on capability analysis and assessment teams, as appropriate.

d. Establish access to the JCPAT-E.

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 I&S of Crypto logic systems including U.S. 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 U.S. Special Operations Command to develop tactical SIGINT architectures, and provide standards compliance and interoperability assessment reports for SIGINT systems 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 I&S.

e. Develop policy and procedures for interoperable and supportable IT and NSS IA information releasability for joint, combined, and coalition forces and U.S. Government Departments and Agencies.

f. Ensure that interoperable and supportable IA products are available for the security of IT and NSS.

g. In cooperation with the DISA, identify, evaluate, and select IA and related standards for inclusion in the DISR.

h. Ensure interoperability, supportability, and security of NSA/CSS IT and NSS with those systems that provide direct support to the combatant commanders.

i. Ensure that technical, procedural and operational interfaces are specified and configuration managed in coordination with other DOD components so that U.S. DOD, non-DOD and coalition Cryptologic/ Cryptographic systems can interoperate with DOD IT and NSS.

j. Establish access to the JCPAT-E.

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 I&S 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 associated GESPs.

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. Participate in Capability Portfolio Management (CPM) focus areas and on capability analysis and assessment teams, as appropriate.

h. Establish access to the JCPAT-E.

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

a. Ensure that standards and specifications established for Defense Human Intelligence (HUMINT) support the I&S 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 U.S. 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 their system/subsystems are:

a. Compliant with the NR-KPP (IAW Enclosure E).

b. Compliant with applicable GIG Technical Guidance to include reflecting DISR mandated GIG IT standards in the TV-1.

c. Compliant with current DOD IA directives and policies.

d. Interoperable with other DOD, Joint and Coalition systems, implement the DOD Net--Centric Data Strategy and Net-Centric Services Strategy policies, including participating in applicable Communities of Interest, within security constraints.

e. Properly evaluated and certified for interoperability by the DISA (JITC) (unless they have obtained an ICTO IAW MCEB Pub 1, as required, until Joint Interoperability Test Certification completion, or a J-6 Interoperability Test Exemption).

f. 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). This information will be included in the Spectrum Supportability Assessment (SSA) which consists, at a minimum, of: (1) a Spectrum regulatory component, (2) a Technical component, to include an electromagnetic environmental effects (E3) assessment, and (3) an Operational component.

g. Funded sufficiently for interoperability testing and recertification testing.

12. Department of the Air Force. As the DOD Executive Agent (EA) for Space, the Under Secretary of the Air Force will review and confirm the sufficiency of the NR-KPP for all ACAT, non-ACAT and fielded National Security Space Program systems.

13. Department of the Army. As the DOD Executive Agent (EA) for Theater Joint Tactical Networks (EA-TJTN), the Under Secretary of the Army will:

a. Convene and chair the TJTN-CCB (IAW reference mm); establish its agenda; and coordinate joint interoperability issue resolution approved by the CCB. Issue resolution could impact tactics, techniques, procedures, policy, and doctrine documents.

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. Such venues currently available include:

(1) The Communications Electronic Command (CECOM) LifeCycle Management Command (LCMC) joint tactical operational network, called JOIN (Joint On-Demand Interoperability Network), is based on the CCB-approved Joint Task Force Operational Area Network. JOIN is available throughout the year to perform these assessments and support other TJTN-CCB joint interoperability efforts.

(2) The CECOM LCMC conducts an annual 3-4 week Joint Users Interoperability Communications Exercise (JUICE) to provide a venue for joint interoperability assessments. With coordination with DISA/JITC, both JUICE and JOIN are additional venues for obtaining joint interoperability certification.

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. JUICE and JOIN are venues available to assess new software versions.

d. Evaluate and provide recommendations to the DISA/JITC 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 JCPAT-E.

14. Other DOD Components will:

a. Coordinate on I&S 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 I&S capability requirements contained in CDD, CPD, ISP, and TISP proposals meet recognized standards and preferred best practices.

c. Establish processes to ensure OTAs include in any operational test, operationally mission-oriented interoperability assessments and evaluations that use common outcome-based assessment methodologies to test, assess, and report on the impact interoperability and information exchanges have on system effectiveness and mission accomplishment for all acquisition systems, regardless of ACAT level.

ENCLOSURE D

STAFFING PROCESS AND CERTIFICATION PROCEDURES

1. General. The Joint Staff J-6 performs an I&S Certification for all IT and NSS. C/S/A submit JCIDS documents to KM/DS IAW CJCSM 3170.01C, register the system in the DOD IT Portfolio Repository (DITPR), as applicable; and develop the program's IT Standards Profile and Forecast (TV-1, TV-2) in DISRonline. C/S/A submit Information Support Plans (ISP) IAW DODI 4630.8 to the JCPAT-E, register the system in the DITPR, as applicable; and develop the program's IT Standards Profile and Forecast (TV-1, TV-2) in DISRonline. Information on DITPR, DISRonline, JCPAT-E and additional references are available on the CJCSI 6212 Resource Page:
https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page

a. J-6 I&S Certification

(1) JCIDS Documents. J-8 staffs all JCIDS documents on KM/DS to the C/S/A. The Joint Staff J-6 reviews the NR-KPP and provides an I&S Certification to the J-8 via the KM/DS tool for those products requiring I&S certification (table A-1). J-6 I&S Certification occurs prior to acquisition Milestones B and C and additionally as required. Figure B-1 illustrates the general J-6 I&S Certification process alignment with JCIDS document coordination and the DOD Acquisition Process.

(a) CDD/CPD NR-KPP Technical Artifacts shall reside in the corresponding ISP and be readily available to all reviewers at the time of the CDD/CPD review (i.e. be included as an attachment or referenced as a hyperlink within the CDD/CPD). The use of the Enhanced Information Support Plan (EISP) tool is encouraged to facilitate the development of a standard ISP format and assist programs in risk mitigation. Current version, date, and title of ISP must be included. NR-KPP technical artifacts that need not be duplicated in the CDD/CPD include:

1. DOD Architecture Framework (DODAF) System & Technical Views

2. Verification of Data and/or Service Exposure

3. The NR-KPP Supportability elements identified in Encl. D.

(2) Information Support Plans (ISPs. ASD (NII)/DOD CIO reviews ISP documents for ACAT I and ACAT IA programs, and for other programs which

ASD (NII)/DOD CIO has designated as special interest. IAW the DOD 4630 series, the Joint Staff shall review and validate sufficiency of the NR-KPP for all ISPs in all ACAT levels. The J-6 accomplishes this by providing an I&S certification to ASD (NII)/DOD CIO. This certification is used by ASD (NII)/DOD CIO in making a final ISP acceptance determination.

(a) Incrementally Fielded Services and Applications. J-6 I&S Certification for services and applications is based on review and certification of a baseline ISP for the overall program and certification of ISP annexes for each follow-on increment. This streamlined process is designed to deliver incremental service and application capabilities more rapidly to the warfighter.

(b) Services and applications are defined as primarily software based components which perform specific functions using standard interfaces. A service is defined as a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description (reference w). A service is a function that is well-defined, self-contained, and does not depend on the context or state of other services. It easily allows for reuse in yet to be determined functions. Applications are designed to perform a specific function directly for the user or for another application.

2. Certification and Staffing Processes. Documents submitted by C/S/A 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 complies with the NR-KPP and delivers interoperable solutions. Verification of compliance is accomplished through I&S Certification. To support the I&S certification process, J-6 requests technical assessments from the DISA, combatant commands, and other DOD agencies.

a. JCIDS Documents. I&S certification is not required for Initial Capabilities Documents (ICDs). J-6 grants I&S certification for IT and NSS CDDs and CPDs with a JPD of JROC Interest, JCB Interest and Joint Integration. The J-6 staffing process follows (Figure D-1):

(1) J-8 staffs JCIDS documents using the J-8 KM/DS tool (IAW references a and b).

(2) The DISA transfers JCIDS documents to JCPAT-E.

(3) J-6 reviews comments received, determines whether an I&S Certification is warranted, and posts the Certification on JCPAT-E.

(4) The DISA posts the I&S Certification on KM/DS.

b. Information Support Plans (ISPs). C/S/A upload ISPs in JCPAT-E for all programs IAW references c, d, ss and this instruction. J-6 provides I&S certification (see Table A-1) to ASD(NII)/DOD CIO. ASD(NII)/DOD CIO determines final acceptance of each ISP using the J-6 certification and additional agency inputs. The use of the Enhanced Information Support Plan (EISP) tool is encouraged to facilitate the development of a standard ISP format and assist programs in risk mitigation. Information on the EISP tool is available on the CJCSI 6212 Resource Page: https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page. The following J-6 staffing processes differ by ISP type:

(1) ACAT I and OSD Special Interest 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 and the ASD(NII)/DOD CIO acceptance memorandum reside on the JCPAT-E (not KM/DS).

(2) ACAT II and below and Non-ACAT Program ISPs. These program ISPs will be posted to the JCPAT-E by the document sponsor and maintained in the JCPAT-E repository. These ISPs will be reviewed by the J-6, the DISA and the JITC and I&S certified only by J-6. They will not be staffed to the C/S/A for their review. The Joint Staff J-6 will post the certification in the JCPAT-E.

(3) Fielded Program ISPs. ISPs for fielded programs which are managed as an acquisition program per the DOD 5000 series and those seeking a four-year JITC recertification will be staffed and certified for I&S by ASD (NII)/DOD CIO and/or J-6 IAW the procedures for the appropriate ACAT level described above.

(4) TS/SCI ISPs. JCPAT-E does not exist on Joint World Wide Intelligence Communications System (JWICS); therefore a placeholder document will be loaded into JCPAT-E on the SIPRNET containing directions on where the TS/SCI ISP can be located on JWICS. Reviewer comments will be entered and adjudicated on JWICS. The J-6 I&S Certification will be maintained on JCPAT-E.

(5) ISP Review Process. There are four ISP reviews (an initial, revised, final and updated). ISPs for services and applications are discussed below. The tasks associated with each of these reviews are delineated (in reference ss). ISP reviews are tied to the acquisition milestones, the system engineering for the program and the associated 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. At subsequent increments (upgrades) additional reviews may be conducted.

(6) Legacy System ISP Waiver Process.

(a) General. This process establishes procedures for C/S/A to request a waiver from the DOD Instruction 4630.8, (reference d), requirement to produce an ISP and obtain JITC interoperability certification for legacy systems (ACAT II and below and non-ACAT programs) that meet all of the conditions outlined below. This process will increase accountability for low risk systems in the GIG and increase knowledge of systems employed and supporting our warfighters. Status, recommendations, and waiver memoranda are stored in the JITC STP, linked from the CJCSI 6212 resource page. Approval may result in exemption from interoperability testing also.

(b) Applicability. This process is not applicable to systems designated as ACAT I, ACAT IA or OSD Special Interest. All programs must still comply with NR-KPP requirements.

(c) Criteria for Legacy System ISP Waivers. Many legacy systems lack both J-6 I&S Certification and JITC Joint Interoperability Test Certification. The process described below provides two alternatives to the J-6 I&S Certification and JITC Joint Interoperability Test Certification processes.

1. Option A – Permanent Legacy ISP Waiver. Programs scheduled to terminate may not require interoperability testing and certification if they meet the following criteria:

a. Lack J-6 I&S Certification.

b. Lack a JITC Interoperability Test Certification.

c. Have no pre-existing critical interoperability deficiencies identified by the JITC.

d. Have no plan for funding beyond the Future Years Defense Plan (FYDP).

e. Will be out of the DOD inventory within 5 years.

2. Option B – Four-year Legacy ISP Waiver. Multiple legacy and employed IT and NSS maintaining a continued GIG connection, but do not require updated requirements documentation/re-certification/examination to maintain that connection to the GIG. Provides an ISP waiver process for legacy, non-ACAT I programs. At end of the waiver period, the program may apply for another waiver, provided the program meets the following waiver requirements.

a. Lack J-6 I&S Certified requirements documentation.

b. Lack a JITC Interoperability Test Certification.

c. Have no major planned updates, incremental changes, sprints, or spiral development changes planned.

d. Have no pre-existing critical interoperability deficiencies identified by the JITC.

e. Will be funded beyond FYDP, with no established retirement date.

f. Is currently connected to the GIG. A system connected to the GIG is considered GIG-enabled. A GIG enabled system is "any system that exchanges and/or disseminates information in the manner described in the GIG definition, and is in compliance with the capability requirements stated in the GIG Capstone Requirements Document to fulfill the system's operational purpose(s)/mission(s)".

(d) Procedures for Requesting a Waiver. Requests under either option A or B shall be sent via email to J-6 through the applicable C/S/A MCEB Interoperability Test Panel (ITP) representative. The request shall include: the program's name, version/increment number, the option being applied for, the capabilities it provides, the existing program funding, the identification of key connectivity requirements, and an OV-1 and SV-1. The submission process and waiver format are located on the ITP web page and linked from the CJCSI 6212 Resource page. J-6 will typically concur/non concur with the waiver request via e-mail within 30 calendar days.

1. Responsibilities:

a. Requestors (PMs/Sponsors) will:

(1) Provide a written description of the system and its intended operational use.

(2) Include diagrams, specifically the Operational View-1 (OV-1) and SV-1, identifying key operational nodes/system components. Including the OV-2 and/or System/Service View-2 (SV-2) is encouraged as they provide additional detail on the system's operational use. Submitting additional information (e.g., Concept of Operation, Mission Need Statement (MNS), Operational Requirements Documents (ORDs), TEMPs, ICDs, CDDs, C4ISPs) is encouraged to strengthen the case for a legacy waiver.

(3) Submit the request to the appropriate MCEB ITP representative. The current ITP member list can be found on the ITP web page linked on the CJCSI 6212 Resource page.

(4) Clearly show how the system meets the criteria for either option A or B above. If any joint interfaces/information exchanges are present (i.e., any connection to the GIG), requestors should address the criticality to the joint operational environment or risk to the warfighter of these joint interfaces/information exchanges. It is the Program Manager's (PM)/Sponsor's responsibility to make the case for a legacy waiver.

(5) May work through the ITP representative to provide additional documentation or rebuttal that provides a rationale in support of waiver requests if a disagreement occurs over a DISA/JITC recommendation.

b. ITP representatives will:

(1) Act as the interface between the PM/sponsor and JS for all legacy waiver related issues.

(2) Verify that the IT/NSS has been registered in DITPR. If not, return request to PM stating that all IT/NSS are required to be registered in DITPR.

(3) Ensure and validate all requests address the program criteria.

(4) Ensure requestor provides a complete and accurate waiver package.

(5) Forward the completed request package to the JITC for recommendation and to the J-6 for final evaluation/approval.

(6)

(4) Provide a recommendation for the waiver and for exemption from testing to the J-6 and ITP representative via email for forwarding to ASD (NII)/DOD CIO for review.

(5) Not address a program's costs in evaluating waiver requests.

d. ASD (NII)/DOD CIO will evaluate the requests and provide an approve/disapprove recommendation to the J-6.

e. J-6 will submit all requests to the ASD (NII)/DOD CIO via e-mail and after receiving all recommendations, J-6 will approve/disapprove the waiver.

f. J-6 will notify requesting PM and ITP representative whether the waiver has been approved / disapproved.

g. PM will update DITPR Interoperability status accordingly.

2. Guidelines. PMs/Sponsors must keep in mind that a certified subsystem does not guarantee proper integration into a larger program, nor is it an acceptable substitute for joint interoperability test & certification. The operational effectiveness of the information exchange must be verified. The overall system requirements (to include subsystems) are within the scope and responsibility of the integrating PM. Even when subsystems have met their own requirements, some level of testing is needed to confirm functionality and interoperability once integrated into a larger system. Regular communication between the PM/sponsor and the JITC SMEs researching the waiver request are encouraged in order to assist JITC in making the correct recommendation.

(e) The legacy systems ISP waiver process will assist programs in remaining compliant when they do not fit into the traditional categories for joint interoperability evaluation. The intent is to identify interoperability deficiencies to ensure that no system is fielded without achieving critical interoperability capabilities and to relieve programs of the interoperability requirement where no joint operational interests exist. Thorough and continuous coordination among the JS, ASD(NII), MCEB ITP, JITC, DOT&E (combatant command Assessments), and PMs/sponsors is required to ensure that systems provided to the warfighter have met the requisite interoperability requirements to support joint operations.

c. Services and Applications

(1) Services and Applications delivered incrementally must produce a baseline ISP supporting the overall program information requirements. This baseline ISP will be certified for I&S by the J-6, accepted by ASD (NII)/DOD

CIO and approved by the component through the normal ISP staffing process detailed in paragraph 2.b. above. The program shall produce an ISP annex for each follow-on increment prior to testing of that increment and its subsequent fielding decision. The ISP annex must provide system and technical view architectural artifacts which are traceable to the architectural products in the baseline ISP if such artifacts differ from those contained in the baseline ISP.

(2) Services and applications fielded incrementally require a reduced set of technical artifacts. Certification requirements for services and applications are detailed in Table A-1 and Table E-1 of this document.

(3) Unless a waiver has been obtained, services and applications which are not fielded in an incremental fashion are still required to complete an ISP IAW the DOD 4630 series; however, they may be certified earlier in the traditional acquisition timeline, provided the NR-KPP for the service or application is sufficiently developed.

d. 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 I&S 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 specified in the TISP procedures linked from the CJCSI 6212 Resource Page and any special needs identified by the J-6 for the I&S Certification process. The Component/PM will submit the final version of the TISP in JCPAT-E for review and certification. J-6 will have the final determination on I&S Certification of all TISPs.

(1) TISP Request Process. TISP requests shall be sent via email to the Joint Staff J-6 Interoperability Test Panel (ITP) Chair through the applicable (Service/Agency/JFCOM) ITP representative. The request format is linked from the CJCSI 6212 Resource Page and will include: the program's name, the capability it provides, funding allocated to the program, and identification of key connectivity requirements. The J-6 will respond to the request via e-mail with concur or non-concur. J-6 approval to enter the TISP process will be contingent on the following:

(a) The Joint Staff J-6 shall review the submitted TISP application and make recommendations on including the submission for TISP processing. The J-6 retains final approval authority for entry into the Tailored ISP process.

(b) ASD (NII)/DOD CIO will evaluate the requests and provide an approve/disapprove recommendation to the J-6.

(c) As the TISP program is intended to accelerate the J-6 I&S Certification and Joint Interoperability Testing Certification, programs should make early contact with the JITC to create a testing strategy and gain technical POCs for questions dealing with TISP testing.

(d) TISP I&S Certification requirements in IAW Table A-1, Table E-1, and Encl E.

(e) The TISP may also be developed using the EISP tool.

e. Exceptions and Other Considerations.

(1) Programs acquiring network infrastructure components IAW the procedures of CJCSI 6215.01C (reference uu) derive requirements from the Unified Capabilities Requirements (UCR). These requirements, where applicable, shall be similarly reflected in the GTG and used by system developers to identify and implement IT standards used in network infrastructure components. These may include:

(a) Defense Switch Network (DSN) switches/network components;

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

(c) Commercial Off the Shelf (COTS) Video Teleconference (VTC), network infrastructure components – derived from the UCR, based on international and commercial network and protocol standards.

(2) 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. Examples include:

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

(b) Satellite Communications (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).

(3) 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).

3. Staffing Details.

a. J-6 conducts I&S Certifications of capability documents in three distinct stages, summarized below (references c, d, and ss describe the process for ISPs).

(1) O-6 Level Review is the first assessment of JROC Interest and JCB 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).

(2) Flag Level Review (for JROC Interest and JCB 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.

(3) FCB Draft (JROC Interest and JCB Interest JCIDS documents) or Final stage (Joint Integration JCIDS documents) I&S 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).

b. The combatant commands 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.

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

d. J-6 forwards unresolved I&S issues to the MCEB or Military Intelligence Board (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. Unresolved issues will result in withholding of I&S Certification.

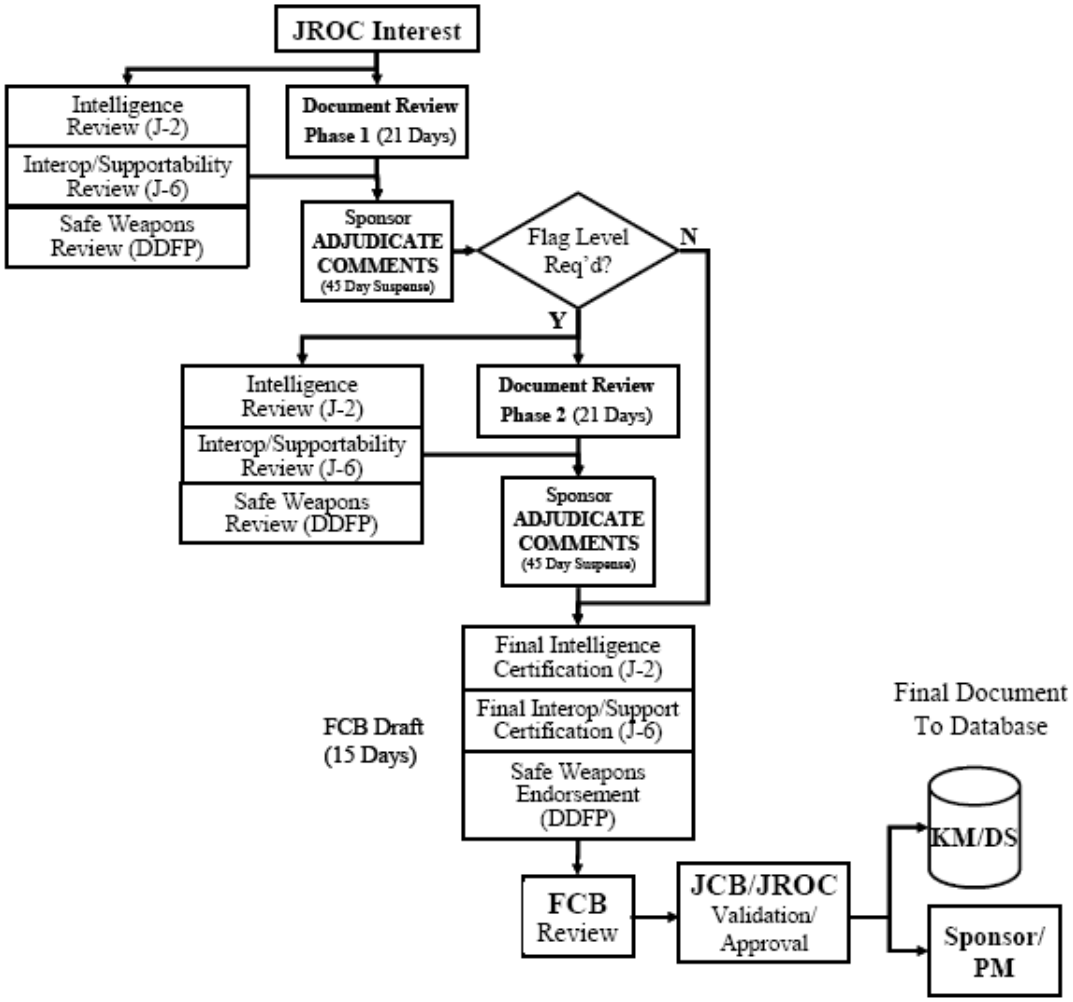


Figure D-1. CDD/CPD/JROC Interest Staffing Process

	Document Type	Stage	Days	Reference	Level	Comments
JCIDS JPD	JROC Interest	I	21	Reference (b)	O6	
	JROC Interest	II	21	Reference (b)	Flag	If Required
	JROC Interest	III	15	Reference (b)	Flag	
	JCB Interest	I	21	Reference (b)	O6	
	JCB Interest	II	21	Reference (b)	Flag	If Required
	JCB Interest	III	15	Reference (b)	Flag	
	Joint Integration	I	21	Reference (b)	O6	
	Joint Integration	II	21	Reference (b)	O6	
	Joint Integration	III	15	Reference (b)	O6	
	Independent	N/A	N/A	Reference (b)	N/A	If J-8 Directs Review
	Joint Information	I	21	Reference (b)	O6	If J-8 Directs Review
	Joint Information	II	21	Reference (b)	O6	If J-8 Directs Review, If Required
	Joint Information	III	15	Reference (b)	O6	If J-8 Directs Review
ISP (Pilot)	Initial	N/A	30	ASD(NII)/DOD CIO Memo	O6	Information Support Plan (ISP) Acquisition Streamlining Pilot Program, dated 26 August 2005 (Reference tt.)
	Revised	N/A	30	ASD(NII)/DOD CIO Memo	O6	
	Final ISP of Record	N/A	10	ASD(NII)/DOD CIO Memo	Flag / O6	
	Updated ISP of Record	N/A	30	ASD(NII)/DOD CIO Memo	O6	
TISP	TISP	I	21	CJCSI 6212.01E	O6	
	Final TISP of Record	II	10	CJCSI 6212.01E	O6	

Table D-1: Staffing Timelines

e. Review Timelines. Table D-1 details the timelines for reviews.

(1) The suspense for completing Stage I and Stage II JCIDS document reviews 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.

(2) The FCB Draft and Final Stage (Stage III) suspense's are ten 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.

4. Failure to meet Certification Requirements

a. If a program/system fails to meet or maintain I&S Certification and/or Joint Interoperability Test Certification requirements, the J-6 will:

(1) Withhold certification or revoke any existing Interim Certificate To Operate (ICTO) until the outstanding issue is corrected.

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

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

(2) The J-6 will make its recommendation to the USD(AT&L), USD(P), USD(C), USD(I), ASD(NII)/DOD CIO, DOD EA for Space, the MCEB, and the Joint Requirements Oversight Council (JROC). The J-6 may also request that the program and/or system be added to the MCEB ITP's Interoperability Test Watch List (ITWL) (IAW reference hh).

(INTENTIONALLY BLANK)

ENCLOSURE E

DETERMINING INTEROPERABILITY, SUPPORTABILITY, AND NET-READINESS

1. This enclosure provides the J-6 I&S Certification procedures.

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. Documentation of the five NR-KPP components is required for I&S Certification.

c. The I&S Assessor's Checklist provides 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. The I&S Assessors Checklist can be found on the CJCSI 6212 Resource Page at https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page

2. I&S Certification

a. JCIDS and ISP Document Considerations

(1) Initial Capabilities Documents (ICDs) do not require I&S Certification.

(2) Capability Development Documents (CDDs). J-6 will certify that all I&S requirements have been appropriately addressed in the capabilities development documents based on the criteria listed in the following section.

(3) Capability Production Documents (CPDs). All CPDs for systems that exchange information with external systems will be evaluated and their NR-KPP certified for I&S policy compliance 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 artifacts associated with the precursor CDD shall be refined with greater detail and be represented in the solution architecture to characterize the capabilities and performance of the proposed production system.

(4) CDD/CPD NR-KPP Technical Artifacts shall reside in the corresponding ISP and be readily available to all reviewers at the time of the CDD/CPD review (i.e., be included as an attachment or referenced as a hyperlink within the CDD/CPD). The use of the Enhanced Information Support Plan (EISP) tool is encouraged to facilitate the development of a standard ISP format and assist programs in risk mitigation. Current version, date, and title of ISP must be included. These artifacts need not be duplicated in the CDD/CPD. NR-KPP technical artifacts include:

(a) DODAF System/Service and Technical Views

(b) Verification of Data and/or Service Exposure

(c) The NR-KPP Supportability elements identified in this Enclosure

(5) Information Support Plans (ISPs). ASD (NII)/DOD CIO reviews ISP documents for ACAT I and ACAT IA programs, and for other programs which ASD (NII)/DOD CIO has designated as special interest. IAW the DOD 4630 series, the Joint Staff and USJFCOM shall review and Joint Staff shall validate sufficiency of the NR-KPP. The J-6 accomplishes this by providing an I&S certification to ASD (NII)/DOD CIO. This certification, among other factors such as compliance with records management requirements, is used by ASD (NII)/DOD CIO in making a final ISP acceptance determination.

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

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

a. The NR-KPP defines the performance attributes and creates the framework for identifying the information structure necessary to successfully enable the functional capabilities identified in the requirements documents.

b. The NR-KPP is composed of five elements: Compliant solution architectures, Compliance with Net-Centric Data and Services Strategy, Compliance with Applicable Technical Standards and Interfaces through the GIG Technical Guidance, Compliance with mandatory DOD IA Requirements, and DOD Supportability Requirements. Characterization and execution of these 5 elements must be in compliance with DOD policy and the following guidance to successfully meet the capability requirements:

(1) Solution architectures

(a) Develop a complaint solution architecture in accordance with the current version of the DOD Architecture Framework (DODAF) (reference l) and

as guided by the laws, regulations, and policies defined in the rules and constraints of the DOD Information Enterprise Architecture reference [DODD 8000.01], including the DOD Information Enterprise Architecture (DOD IEA) (reference tt). The non-GIG IT portions of systems are exempt from compliance with DOD IEA business rules and principles.

(b) The solution architecture will align with the DODAF and DOD IEA business rules and principles, show linkage to parent enterprise architectures where available, and fit within Component and DOD Capability Portfolio Management architecture descriptions as they emerge.

(c) The portion of the DOD IEA that encompasses the "Use the Net-Centric Environment" provides a common taxonomy and lexicon for describing the use of GIG services and capabilities, and shall be used in the development of activity models to describe the communications activities of systems that do not primarily provide services to the GIG. Systems that provide services to the GIG shall use the portion of the DOD IEA that describes service oriented architecture.

(d) The DOD IEA principles are applicable for all DOD programs delivering IT capabilities regardless of component or portfolio, and for any platform, program of record (POR), system, sub-system, component, or application that conducts communications. In today's information environment the DOD IEA rules apply within the persistently-connected Internet Protocol (IP) boundaries of the Global Information Grid (GIG). Outside of these boundaries, the principles shall still be considered, but the rules of the DOD IEA must yield to the state of technology, and the needs and imperatives of the Department's missions.

(e) All programs submitting an ICD, CDD, CPDs, ISPs, or TISPs will publish a DODAF All View-1 (AV-1) on the DARS to facilitate architecture registration and enable net-centric discovery capabilities. Joint Staff NR-KPP assessors will validate that a current AV-1 is available and appropriately registered in DARS for I&S certification purposes.

(f) All DODAF architecture artifacts developed in support of the NR-KPPs shall be registered and maintained in DARS. The DODAF provides specific interoperability and stakeholder analyses that need to be supported (e.g., analytical questions that the architectures must answer)

(g) DISRonline shall be used to develop and publish all Technical Standards Profile (TV-1s) and Technical Standards Forecast (TV-2s) referenced in CDDs, CPD, ISPs & TISPs. The DISA NR-KPP assessors will validate that a current TV-1 and TV-2 are available on DISRonline, correct, appropriately published for I&S certification purposes. Until the official release of the GTG, programs will be required to continue the usage of KIPs. DISRonline is located

at the following URL: https://www.disronline,disa.mil and is required to be accessed with a Public Key Infrastructure (PKI) certificate authority.

1. 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 submission date.

2. DISR-Retired Standards Waivers. In lieu of submitting a change request, the PM or sponsor will acknowledge in DISRonline 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.

(h) Interoperability hinges on the alignment of enterprise architectures and solution architectures. The DOD Information Enterprise Architecture provides the DOD-wide context and rules that pertain to each solution. Alignment with other relevant solution architectures enable a more detailed analysis of the information requirements. The solution architecture should describe the internal and external information flows in sufficient detail to enable the assessment of interoperability requirements..

(i) The Operational Views shall describe the tasks and activities, operational elements, and information exchange(s) required to conduct 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. Operational architecture re-use is highly encouraged. Operational Views must be physically present in all CDDs, CPDs, ISPs, and TISPs to clearly articulate the operational capability of the submission. For those operational capabilities that already exists and has an approved architecture, it is not necessary to duplicate those products within your solution architecture; simply provide a reference to where the approved architecture exists (ISP, DARS, etc..) and demonstrate where your architecture connects to it.

(j) The Systems views, which flow from the Operational Views, shall describe the systems and their interconnections that provide for or support DOD systems functions. Systems architecture re-use is highly encouraged. If an operational capability already exists and has an approved Systems architecture, it is not necessary to duplicate those products within your solution architecture; simply provide a reference to where the approved architecture exists (ISP, DARS, etc..) and demonstrate where your architecture connects to it. Systems views are technical artifacts that shall reside in the corresponding ISP or TISP and be readily available to all reviewers at the time

of review (i.e., be included as an attachment or referenced as a hyperlink within the CDD/CPD). These artifacts need not be duplicated in the CDD/CPD.

1. Use of the JCSFL as the vocabulary in system/service views is required, as applicable, for designating and describing system functionality of any platform, program of record (POR), system, sub-system, component, or application that provides functionality. Compliance can be satisfied by using JCSFL function names and descriptions to the maximum extent possible where subject architecture functions are common to those addressed in the JCSFL; for those not common, domain specific names and descriptions may be used in the SV-4 and SV-5 views.

2. Functions not addressed in the JCSFL shall be submitted to the JCSFL Manager for consideration as new function candidates in the JCSFL. An alternative method of compliance permits the use of domain specific functions in SV-4 and SV-5 products, but requires a cross-walk to the JCSFL where a relationship exists. Again, domain functions that have no JCSFL mapping shall be submitted to the JCSFL Manager for consideration as new function candidates in the JCSFL..

(k) Technical Standards Views (TV): The Technical Standards Profile (TV-1) provides the minimal set of rules, standards, and protocols governing the arrangement, interaction, and interdependence of system parts or elements. The TV-1 includes applicable DISR mandated standards. In addition to a collection of the technical standards, the TV may include implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture. The Technical Standards Forecast (TV-2) will be included to identify applicable emerging standards in the DISR and any standards not found in the DISR that that the program intends to use. The TV-2 will also be used to identify issues affecting program implementation (e.g. impacts of commercially available equipment or development of another program).

(l) The All-View (AV) products shall provide information pertinent to the entire architecture and set the scope and context of the architecture.

(m) Architecture products shall be submitted in data formats that support architecture staffing, distribution, and reuse. At a minimum, products must be submitted in formats that can be viewed without specialized or proprietary tools and must be legible for reviewers. As emerging architecture data exchange standards (such as the DODAF Meta Model [DM2] Physical Exchange Specification [PES] and Extensible Markup Language (XML) Metadata Interchange [XMI] standard) gain the support of commercial tool vendors, program managers are encouraged to adopt standards-compliant tools and make architecture data available in those formats for reuse by other programs.

(2) Net-Centric Data and Services Strategy

(a) Alignment with the DOD IEA represents the programs end-state for the GIG. This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services and/or data that enable operational capabilities across the range of military operations; DOD business operations; and Department-wide enterprise management operations.

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

1. The DOD is moving to Net-Centric operations. The vision is for all elements of the DOD to be networked and able to share information, resulting in dramatic improvements in operational effectiveness. CDDs, CPDs, and ISPs and TISPs will document/reference compliance with the DOD Net-Centric Data Strategy and DOD Net-Centric Services Strategy (as identified in references u through x). Tactical systems, control systems, and weapons systems with time critical constraints are exempted from the requirement to demonstrate compliance with the data strategy. However, after-action reporting should follow the data strategy where feasible

2. DOD Net-Centric Data Strategy. Compliance with the DODD 8320.02, "Data Sharing in a Net-Centric Department of Defense" (reference u), the DOD Net-Centric Data Strategy (reference v), and the DOD Net-Centric Services Strategy (reference w) is an essential prerequisite of Net-Centric operations. In order for a program to gain I&S Certification, program data and services, must be "exposed" by making data elements and provided services visible, accessible, and understandable to potential GIG users (subject to operational, security, and environmental constraints).

3. The DISA hosts a collection of services and tools to enable information sharing on the GIG. In order to meet directed exposure criteria, the following must be used as directed in subparagraph 4 Data and Service Requirements, below. Uniform Resource Locators (URL) for these services and tools are located on the CJCSI 6212 Resource Page at https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page

a. DOD Metadata Registry (MDR). An online repository that enables developers to reuse, understand, integrate with, and share existing data assets (metadata) – targeting Web services, databases and vocabularies and provides a portal for Web services for machine-to-machine access.

b. Service Registry. Net-Centric Enterprise Services (NCES) Service Registry is the system of record for offered services that provides a

foundation for the governance and lifecycle management of these assets. Fully supporting the Universal Description, Discovery and Integration (UDDI) registry standard, the NCES Service Registry captures descriptions of services offered and makes them discoverable from a centrally managed, reliable, and searchable location.

c. Enterprise Catalog. The Enterprise Catalog provides the capability to publish, update, and delete DOD Discovery Metadata Specification (DDMS) compliant metadata about content for later retrieval via a federated search service. The purpose of this catalog service is to allow disadvantaged users the ability to "post" content by placing it onto a network storage location and then publishing the metadata, along with a reference to the content location, to the Enterprise Catalog.

4. Data and Service Requirements.

a. Data and Services must be visible.

(1) Data assets shall be made visible by creating and associating metadata (“tagging”), including discovery metadata, for each asset using DOD Discovery Metadata Specification (DDMS) compliant metadata and posting it in the NCES Enterprise Catalog or another compatible/federated enterprise catalog. Data tags will include metadata extensions to the DDMS. Semantic and structural metadata shall then be registered in the DOD MDR.

(2) Services shall be made visible by registering them in the NCES Service Registry. This registration will enable all users in the GIG to find and understand what services already exist, thus facilitating reuse and avoiding investment in the creation of new capabilities.

(3) Web services Description Languages (WSDL), XML schema definitions (XSD), XML instances, data models (such as entity relationship diagrams) and other appropriate artifacts shall be registered in the MDR.

(4) Universal Resource Identifiers (URIs) as the operational end points for services shall be registered in the NCES Services Registry by referencing the WSDL in the MDR (note: WSDL must first be registered in the MDR).

b. Data and Services must be accessible (subject to applicable access restrictions, laws and regulations:

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

(2) If the program data is not accessible to all users, a written policy on how to gain access must be presented. Programs must ensure compliance as written and must keep the policy up to date to account for system changes.

(3) Services shall be made accessible whereby users must not only have the ability to discover services, but must also be able to access them in a timely, secure, and effective manner. Federated Search results provide an active link (e.g., Uniform Resource Identifier (URI)) to the specified data asset within the targeted security enclave (i.e., the Enterprise Catalog DDMS entry includes the active link to the data).

c. Data and Services must be understandable.

(1) Data assets shall be made understandable by publishing associated semantic and structural metadata in the Enterprise Catalog. The keywords entered in the DDMS record in the catalog should reflect common user terms, be appropriate for mission area or data type, be understandable, and conform with MDR requirements that map back to COI identified mission data.

(2) Services shall be made understandable by publishing associated metadata to the NCES Service Registry.

d. Data and Services must be secure.

(1) Data assets shall have associated security metadata, and an authoritative source for the data identified.

(2) Semantic, structural and security agreements for service sharing shall be promoted through communities (e.g., COIs), consisting of service users (producers and consumers) and system developers.

e. Data and Services must be interoperable.

(1) Semantic, structural and security artifacts for data sharing shall be derived from the Universal Core (Ucore), domain cores (e.g C2 Core), COIs, and other data standards in accordance with reference v.

(2) Service interoperability shall be supported by enabling mission processes and services to be reused whenever possible.

5. Verification of requirements documentation compliance with the DOD Net-Centric Data Strategy and DOD Net-Centric Services Strategy (references v and w) will be accomplished through the analysis of the sponsor-provided architecture and verification products with accompanying text detailing the program's compliance strategy. Documentation (in solution

architecture products or other forms) must clearly identify all net-centric services and data, including any adopted from the Ucore (reference ww), Domain Cores and COIs.

Compliance with data and service exposure verification tracking policy is required only when one or more of a program's IT and NSS nodes has identified, within its architecture views, a requirement to transport or store data/information over or through the use of the GIG. Only those programs with nodes connecting directly to the GIG will be required to incorporate DDMS-compliant metadata tagging for discoverability visibility, accessibility, and understandability. Those nodes will also be required to identify/expose any services if they have any. Compliance with data and service exposure verification tracking policy is not required for programs with point to point or platform centric information exchanges and does not apply to transmission devices such as radios, satellites, or to network equipment that is otherwise accounted for in the programs architecture views.

When applicable, in addition to the required architecture products submissions must include completed Exposure Verification Tracking Sheets (see templates in Appendix A to Enclosure E) to self-evaluate compliance with data and services exposure requirements.

a. A guide for selecting which type of Tracking Sheet is required for each program and instructions for the completion of each type is located on the CJCSI 6212 Resource Page at https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page.

(c) CPDs and Milestone-C ISPs (including ISP annexes for incrementally fielded capabilities) will include the Logical Data Model (OV-7) and the Physical Schema (SV-11) if the system being described shares any internal data with external systems. If the system accesses shared data from an external system, then the document may point to the external system's OV-7 and SV-11 (if available) by reference. 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, data derived from data models or other standards, such as the UCore.

(3) GIG Technical Guidance

(a) Purpose and Objectives

1. GIG Technical Guidance (GTG) is an evolving web enabled capability providing the technical guidance necessary for an interoperable and supportable GIG built on Net-Centric principles. It is being developed in stages and the content baselines are to be vetted through a collaborative department-wide process to ensure stakeholder participation in development of and

validation of GTG-based guidance and artifacts. GTG content will be evolutionary in nature and, as developed and validated, will be released for use through Joint Staff Memo or JROCM. Use of the GTG will be optional for programs reaching milestone review within six months of the GTG's release or in coordination with the J-6 to synchronize with the program's APB. The GTG will provide a one-stop, authoritative, configuration managed source of technical compliance guidance that synchronizes previously separate efforts. The GTG aids program managers, portfolio managers, engineers and others in answering two questions critical to any IT or NSS: (1) Where does the IT or NSS fit, as both a provider and user, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG? The GTG content listed below provides the technical information to use in answering such questions.

(b) GTG Content

1. The GTG is designed to enable users to decide which guidance is applicable and to find detailed information and artifacts on:

a. technical guidance needed to meet functional requirements (GIG features and capabilities)

b. DISR mandatory GIG net-centric IT standards

c. supporting GIG IT standards

d. associated profiles

e. reference implementations, and tests

2. The GTG contains a program characterization questionnaire and compliance matrices/declaration tables that point to applicable GIG Enterprise Service Profiles (GESPs) for use in the I&S certification process. The compliance matrix will be versioned, managed and synchronized by the DISA with the other components of the GTG. The GESPs are aligned with the DOD IEA priority areas and are determined on the following criteria for whether the capability:

a. Spans organizational boundaries

b. Is mandatory or mission critical across the GIG Enterprise

c. Can be characterized from a consistent solution architecture

d. Is essential for resolving GIG end-to end interoperability issues

e. Enables net-centric information sharing for multiple acquisition programs

f. Is important from a security perspective.

3. GESPs contain:

a. An Interoperability Reference Architecture and Service Description which contains:

(1) 1. An interoperability reference architecture and graphic to illustrate the context where the GESP architecture will fit within the overall GIG Reference Topology.

(2) 2. A Service Description which contains a description of the services provided by the GESP

b. An Interoperability Requirements Description which describes the interoperability requirements as defined in the Guidance Statements necessary to fulfill the Interoperability Reference Architecture. This section also describes security requirements in a Secured Availability section.

c. A technical implementation profile for critical GIG Technical Standards and interfaces that are part of the GESP. The Technical Implementation Profile includes the interoperability requirements, in the form of Guidance Statements, necessary for systems to correctly use the functions associated with the GESP. This section will also include the applicable Secured Availability Guidance Statements and Standards Profiles. Examples include such items as use of IPv6, QoS, and a structured IP addressing plan.

d. A Maturing Guidance section which describes the maturing guidance for program consideration for mid-term and far-term program planning and implementation. Maturing guidance is provided for Program planning consideration and will not be assessed against the NR-KPP.

e. A Compliance Testing section which defines how the system will be tested for compliance with the NR-KPP. This section identifies a verification method for each requirement. The five methods of verifying requirements are as follows: Analysis (A), Demonstration (D), Test (T), Similarity (S), and Inspection (I).

f. A Key Programs Implementing the GESP section which includes a list of DOD programs implementing this GESP for review and comparison of implementation.

g. A Data section which includes any data format, techniques, or exchange requirements necessary to ensure GESP capability functionality.

h. A References section which contains all sources used to develop the GESP (e.g., EWSE Issue Reference Papers).

(c) GTG Compliance. The GTG has a compliance process with granularity appropriate to the Milestone (MS) phase or maturity of a program.

1. At MS B, CDDs/ISPs will include a preliminary declaration of the functional implementation features and technical capabilities and identify which GESP technical implementation profiles are applicable.

2. At MS C, CPDs/ISPs and post MS C TISPs will include the final declaration of functional implementation features and technical capabilities and identify applicable GESP technical implementation profiles. The completeness and sufficiency of the program's citing of artifacts drawn from the GTG will be assessed and certified by J-6 in the ISP.

(d) DISRonline Standards Compliance

1. The DISRonline shall be used to develop and publish all TV-1s and TV-2s and they will be referenced in the ISP.

2. The PMs or sponsor may cite additional DISR standards in the TV-1 that are not designated as Mandated, provided the cited standards do not conflict with DISR standards found in GESPs.

3. All ISPs will have a TV-1 and TV-2, which is published by the DISRonline. The following conditions must be met in building TV-1s and TV-2s in an ISP:

a. All Standards for DOD use in assessing the NR-KPP will be drawn from the DISR. This includes implementation guidance of applicable IT standards found in the GESP standards profiles.

b. DISRonline is the system of record for development of TV-1s and TV-2s. A baseline TV-1 and TV-2 will be published by DISR and reflected in the CDD and ISP prior to Milestone B. This TV-1 and TV-2 will then be considered as the "system baseline" TV-1 and TV-2. Prior to Milestone C, the TV-1 and TV-2s will be re-examined in the CPD or ISP and consideration will be made to those change in standards since Milestone B certification. Three DISR baselines are published annually. A grace period for compliance with the latest DISR baseline will be granted to programs reaching Milestone review if they are within six months of the latest DISR baseline release. Program Managers may, at their discretion, update this final TV-1 and TV-2 and address all changes in the risk assessment rationale.

c. PMs will initially create TV-1s and TV-2s for their ISP in the DISRonline.

d. DISR sanctioned standard (Emerging, Mandated, Retired) may be used to complete a system's overall TV as part of their DOD Information Enterprise Architecture and solution architecture. Any version of a Standard cited in the DISR may be used though current versions are preferred, subject to the following paragraphs.

e. Emerging standards and standards that are not cited in the DISR but are planned to be implemented in a later program development cycle can be selected and placed in the TV-2.

f. Any DISR Emerging standards added to the TV-2 may be implemented at the program's risk. A statement of consideration of the risk will be included in the ISP.

g. Earlier retired versions of standards may be used with currently mandated standards to provide legacy support provided that a statement of consideration of the risk is included in the ISP.

(4) DOD IA and Critical Infrastructure Protection (CIP) Requirements.

(a) Information Assurance and Critical Infrastructure Protection. IA and CIP are critical elements in the GIG. The Department employs a defense-in-depth strategy to establish and maintain an acceptable IA and CIP 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. Programs Managers shall ensure that IA is fully integrated into all phases of their acquisition and upgrade, including initial design, development, testing, fielding, and operation as stated in DODI 8580.1 (reference p) and outlined in the Defense Acquisition Guidebook (reference aa).

(b) The CDD must:

1. Describe how the system will implement IA policies and procedures (contained in references n through s and bb through dd); and for SCI and Special Access Programs (references ee and ff). If encryption (including Public Key Infrastructure (PKI)) technology is required, include a statement that encryption 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 the following IA statement of compliance:

"This program or system will comply with the IA requirements in DOD 8500 series and CJCS 6510 series directives, instructions and manuals prior to IOC." Include the point of contact information for accreditation decision documentation (e.g. DIACAP Implementation Plan, 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 National Institute of Standards and Technology (NIST) SP 800-53 (reference oo) (for non-DOD) must also be met.

(c) The CPD must:

1. Describe in greater detail how the production system implements the IA policies and procedures cited in the CDD (and contained in references n through s and bb through dd); and in accordance with the Joint DODIIS / Cryptologic SCI Information Systems Security Standards (JDCSISSS) (references ee and ff for SCI and SAP). If encryption technology is required, include a statement that encryption 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 the following IA statement of compliance:

"This program or system complies 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. DIACAP Implementation Plan, accreditation decision, or other supporting documentation.

(d) Sponsors and program managers must specify their IA requirements and ensure these requirements (i.e., IA controls) are included in the architecture design, acquisition, installation, operation, upgrade, or replacement of all DOD IT and NSS (IAW references n through s and bb through dd and references ee and ff for SCI and SAP). Interoperability and integration of IA solutions within or supporting the DOD shall be achieved through the GIG Architecture.

(e) Test considerations to include operational test for IA must be included and documented in the TEMP (reference aa) or a TES. The TEMP or TES must:

1. Contain an Operational Test and Evaluation (OT&E) strategy for IA assessment addressing the test process, identification of required IA test resources and funding, and a reference to appropriate threat documentation.

2. Contain measures of performance to evaluate IA and support an assessment of system effectiveness, suitability, and survivability. TEMPs and Test Plans must evaluate IA end-to-end, whenever possible, including the links to other systems that accept, use, or provide data/information to the system being evaluated.

(f) IAW DODI 8580.1 (reference p), Program Managers shall ensure each assigned DOD information system has an IA Manager (IAM), designated in writing, with the support, authority and resources to satisfy the responsibilities established in DODI 8500.2 (reference o) and implement the DIACAP for the 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 DOD IA directives.

(g) IT and NSS, including commercial and non-developmental items, must comply with applicable DOD IA and Critical Infrastructure policies and regulations/instructions and Director Central Intelligence Directives (DCIDs). This includes implementation of encryption 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) and the DIA, the DISA and NSA CIO's. IA will be an integral part of net-centricity efforts thus allowing appropriate security measures to protect mission data and services 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.

(h) Program managers/Sponsors must provide a memorandum to DISA/JITC, signed by the proponent Designated Approving Authority (DAA), when claiming exemption from any IA requirements (e.g., weapon systems without platform IT interconnections).

(5) DOD Supportability. All IT and NSS must comply with the following:

(a) Electromagnetic Environmental Effects (E3) control and Spectrum Supportability Policy (references i and j). The spectrum supportability process includes national, international, and DOD policies and procedures for the management and use of the electromagnetic spectrum. The CDD/CPD must document that:

1. Permission has been or is expected to be obtained from designated authorities of sovereign ("host") nations (including the United States) to use that equipment within their respective borders; and the newly acquired equipment can operate compatibly with other spectrum-dependent

equipment already in the intended operational electromagnetic environment (EME). This information and the requirements of 2 and 3, below, will be included in the SSA, which shall be submitted prior to Milestone and Readiness Reviews.

2. 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).

3. All IT and NSS must comply with 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 Material Solution Analysis – 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. The DD 1494(s) will be attached to the Spectrum Supportability Assessment (SSA) as part of the request for Spectrum Supportability Determination (SSD) at the Material Development Decision (MDD). 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 ISP.[1] Programs will need to work with the J-6 spectrum office in order to determine justification and plan format.

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 (reference j) 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. Programs will need to work with the J-6 spectrum office in order to determine justification and plan format.

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 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. Programs will need to work with the J-6 spectrum office in order to determine justification and plan format.

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

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." Programs will need to work with the J-6 spectrum office in order to determine justification and plan format.

4. 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.

5. All proposed IT and NSS that include spectrum-dependent hardware must document spectrum certification (reference j).

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

7. 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.

8. Hazards of Electromagnetic Radiation to Ordnance (HERO). All proposed IT and NSS should be assessed to determine their effects on electro-explosive devices (ordnance).

9. Ordnance containing Electrically Initiated Devices (EIDs) will be compatible with the operational electromagnetic environment and will not be degraded by E3 (reference i).

10. 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).

11. CDDs, CPDs, ISPs and TISPs must contain a spectrum compliance statement. An example is provided below:

a. "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 Military Department (MILDEP) publications. An application for equipment frequency allocation (i.e., DD Form 1494) was (will be) initiated on (date). The DD Form 1494, Application for Equipment Frequency Allocation, 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."

12. Spectrum supportability should be addressed in the Initial Capabilities Document (ICD). Program managers/requirements proponents should consider including a statement similar to the following:

a. "This system will comply with DOD, national and international spectrum management policies."

(b) Joint Tactical Radio System (JTRS). All future requirements for radio-based communications that fall within the JTRS spectrum range (2MHz-2GHz) will be satisfied by the current JTRS requirements document unless ASD(NII)/DOD CIO grants authorization for a specific procurement, in accordance with DOD policies (references pp and qq).

(c) Selective Availability Anti-Spoofing Module (SAASM). All IT and NSS must comply with CJCSI 6130.01D, which directs specific measures to protect GPS. Each JCIDS document or ISP must include a statement on how the program complies with CJCSI 6130.01D.

(d) Tactical Data Link (TDL) Implementations. DOD has the joint family of TDL message standards, which includes Link 16, Link 22, Variable Message Format (VMF), and Integrated Broadcast Service (IBS). Interfaces for TDL dissemination across joint interfaces, and are often implemented through the use of Gateways between platforms. Joint Mission Area interoperability assessment of TDL participants requires identification of platform TDL implementation details. For example, for Link 16 this includes the Data Field Identifier/ Data Use Identifier (DFI/DUI) and Data Item implementation. This

detailed implementation information will be included in an I&S certified requirements document. There are methods, tool sets, and documentation available that can assist Program Managers in the integration and implementation of TDLs. Capability developers who are implementing tactical data standards within their IT and NSS solutions are encouraged to leverage the Interoperable Systems Management and Requirements Transformation (iSMART) processes and the Enhanced Systems Management and Requirements Transformation (eSMART) tool set, as well as the Joint Capabilities and Limitations (JC&L) document to improve tactical data and sensor interoperability.

(e) Bandwidth Analysis. The Milestone C submission shall address Bandwidth requirements. The submission must address the information sharing requirements and its potential impact to the Global Information Grid. In order for DOD Networks/resources to accommodate a program's future bandwidth considerations must be made addressed, i.e., Terrestrial Transport, Satellite Transport, Internet Protocol (IP), Voice and Video.

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

Document	Supportability Compliance	DOD Enterprise Architecture Products (IAW DODAF) (see Note 5)																Data/Service Exposure Sheets	IA Compliance	GTG Compliance
		AV-1 /AV-2	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			
ICD			X																	
CDD	X	3	X	X	X	X	X	X			X	X	X	X		2	2	1	X	X
CPD	X	3	X	X	X	X	X	X	1		X	X	X	X	1	2	2	1	X	X
ISP	X	3	X	X	X	X	X	X	4		X	X	X	X	4	2	2	1	X	X
TISP	X	3	X		X		X	X		X			X	X		2	2	1	X	X
ISP Annex (Svcs/ Apps)	X	3	X				X				X	X	X	X		2	2	1	X	X
X		Required (PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs, ISPs/TISPs. (e.g., HQDA requires the SV-10c)																		
Note 1		Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements shared services,																		
Note 2		The TV-1 and TV-2 are built using the DISRonline and must be posted for compliance.																		
Note 3		The AV-1 must be uploaded onto DARS and must be registered in DARS for compliance																		
Note 4		Only required for Milestone C, if applicable (see Note 1)																		
Note 5		The naming of the architecture views is expected to change with the release of DODAF v2.0 (e.g., StdV, SvcV, StdV, DIV). The requirements of this matrix will not change.																		

Table E-1. NR-KPP Products Matrix

c. The NR-KPP Compliance Statement in Table E-2 provides the NR-KPP Threshold and Objective Values and is a mandatory item of inclusion in the CDD, CPD, ISP, TISP, and for Services/Application J-6 I&S Certification.

KPP	Threshold (T)	Objective (O)
Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.	The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DOD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DOD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net -Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DOD Information Enterprise Architecture (DOD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization To Operate (ATO) by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.	The capability, system, and/or service must fully support execution of all operational activities and information exchanges identified in DOD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include 1 Solution architecture products compliant with DOD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net -Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DOD IEA, excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GESPs, necessary to meet all operational requirements specified in the DOD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an ATO by the DAA, and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.

Table E-2 NR-KPP Compliance Statement

d. The threshold value is determined by analysis of the system's DOD Information Enterprise Architecture and solution architecture 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 operational 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 DOD Information Enterprise Architecture and solution architectures from OV-6Cs to OV-5, OV-3, TV-1, SV-5, SV-4, and SV-6. 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. As high-level Joint Critical Mission Threads (JCMTs) are validated the ISP must trace how its system contributes to the appropriate JCMT.
.

(3) The applicable mandatory DISR GIG net-centric IT Standards are selected from the DISRonline and published in the TV-1 to ensure guidance contained in relevant GIG Enterprise Service Profiles is met.

(4) The information and data exchanges and mission critical performance attributes are identified and documented in the OV-3 and SV-6, including those derived from established joint critical mission threads. The following are examples of these critical performance attributes: Periodicity, Criticality, Timeliness, and Size.

(5) Include a discussion of the threshold IA requirements and IA attributes associated with the threshold information and data exchanges shown in the OV-3 and SV-6, including those derived from established 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.

(6) Compliance with the Net-Centric Data and Services Strategies is verified by reviewing applicable architecture views, textual explanations, and Data and Services Exposure Verification Tracking Sheets.

(a) Completion of Data and Service Exposure Verification Tracking Sheets are not required for the following systems:

1. Communications transmission systems.

2. Tactical systems operating exclusively in a "disadvantaged" communications environment.

3. Individual tactical remote sensors.

4. Systems employing only tactical message standards for data exchange.

5. Systems with legacy waivers.

(b) For joint or multi-Service systems, only the JPO or lead Service should be required to meet the reporting requirement.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE E

EXPOSURE VERIFICATION TRACKING SHEETS

General. This appendix provides the standard template for the Data Exposure Verification Tracking Sheet and Service Exposure Verification Tracking Sheet. Instructions for completing these tracking sheets are provided on the CJCSI 6212 Resource Page at https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page.

(INTENTIONALLY BLANK)

Data Exposure Verification Tracking Sheet for <program>

Key: N = Not Started | I = In-Progress | R = Progress at Risk | S = Progress Stopped | A = Objective Achieved | X = Not Applicable

Program Manager Telephone # email address		Project POC Telephone # email address		Visible	Accessible		Understandable	# of Objectives Achieved Since Previous Submission	
Web Page URL									
IT System DITPR Number				CD&D (1.a)	Policy (2.a)	Oper (2.b)	User (3.a)	Submission Date	

Top Level JCA	Data Asset	Description	(Note: Use above 'Key' to assign values for columns below)				Issues/Comments	Exposure Start / Complete Date	
(JCA Category)	Asset #1	Description #1							
	Asset #2	Description #2							
	Asset #n	Description #n							
(JCA Category)	Asset #1	Description #1							
	Asset #2	Description #2							
	Asset #n	Description #n							
(JCA Category)	Asset #1	Description #1							
	Asset #2	Description #2							
	Asset #n	Description #n							

<CLASSIFICATION>

Version 0.1, 7 DEC 07

Figure E-A-1 Data Exposure Verification Tracking Sheet

Service Exposure Verification Tracking Sheet for <program>

Key: N = Not Started | I = In-Progress | R = Progress at Risk | S = Progress Stopped | A = Objective Achieved | X = Not Applicable

Program Manager Telephone # email address		Project POC Telephone # email address			Visible		Accessible		Understandable		# of Objectives Achieved Since Previous Submission			
MDR Namespace		IT System DITPR Number			MDR (1.a)	UDDI (1.b)	UDDI (2.a)	Policy (2.b)	MDR (3.a)	COI (3.b)	Submission Date			
Top Level JCA	Service Name	Service Type	MDR Submission Pkg Name	Service Description	(Note: Use above Key to assign values for columns below)						Issues/Comments	Exposure Start / Complete Date		
(JCA Category)	Service Name #1													
	Service Name #2													
	Service Name #n													
(JCA Category)	Service Name #1													
	Service Name #2													
	Service Name #n													
(JCA Category)	Service Name #1													
	Service Name #2													
	Service Name #n													

<CLASSIFICATION>

Version 0.1, 7 DEC 07

Figure E-A-2 Service Exposure Verification Tracking Sheet

ENCLOSURE F

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 four (4) years. JITC Joint Interoperability Test Certification is based on Joint Staff J-6 certified I&S requirements, Net-Ready Key Performance Parameters (NR-KPPs), and other applicable 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. The JITC, as the Joint interoperability test certifier, will assist test and evaluation institutions with requirements for Joint Interoperability test certification so the test results from another testing organization (e.g., an EA-TJTN JUICE assessment/test, USJFCOM JSIC, Army FaNS, etc.) are utilized for Joint Interoperability Test Certification. Joint interoperability testing and certification is a continuous process that must be managed and resourced throughout the system lifecycle. JS may track and place any IT or NSS not making significant progress toward achieving Joint Interoperability Test Certification on the Interoperability Watch List.

a. The DOD is evolving toward a federated test environment based on high-level joint mission threads encompassing major mission area functions. As the repository of validated high-level joint mission threads is developed, and the federated test environment evolves and matures, identification and verification of the joint mission threads associated with a capability will become a major component of architecture-related I&S evaluation.

b. Developed and validated high-level joint mission threads will allow unambiguous tracking of these activities through the associated DODAF operational and system/service view products.

2. Applicability – Systems Requiring Certification. All systems effecting joint/enterprise information exchange will be certified for net-readiness before being placed into operation (references c and d). 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.

(3) Systems with hardware, software, or firmware modifications, affecting net-readiness or systems with expired or revoked certifications.

3. Joint Interoperability Test Certification. JITC will evaluate the five NR-KPP elements defined in Enclosure E of this instruction. In addition, the Joint Staff and JITC may use data from Service and Agency operational test agencies' evaluations of the interoperability and operational effectiveness of information exchanges based on 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 the expected interoperability capabilities in an operational environment and assesses the expected operational impact of any discrepancies. Testing using established Joint Mission Threads will verify the operational effectiveness of the information exchanges of the system under test with all its enabling systems. The J-6 I&S Certification is instrumental for the JITC interoperability test and evaluation process, and, in turn, JITC Interoperability Test Certifications provide input to the Milestone Decision Authority (MDA) (or equivalent) fielding decision.

c. JITC issues full joint interoperability test certifications when all critical interoperability requirements are met. Testing shall include, when feasible, system-of-system and family-of-system (federated) live events to complete interoperability certification. 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. A program receiving a limited certification must continue to work toward achieving a full joint interoperability test certification.

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. There may also be other certifications required in addition to Joint Interoperability Test Certification and the J-6 I&S Certification. Spectrum certifications, IA certifications or accreditations, network manager approval, and other validations/approvals may be required and are not necessarily satisfied by the JITC Joint Interoperability Test Certification.

5. Federated Testing. Maximum use of federated testing on federated networks (e.g. DREN, DISN, NIPR, SIPR and federated tracking (e.g. Federated Development & Certification Environment (FDCE)) will be employed to demonstrate a capability's performance, interoperability and contribution to the COI mission accomplishment when used in the integrated Mission Area (MA)/Capability Portfolio Management (CPM) architecture. Federated testing is the use of geographically dispersed live, virtual and constructive resources in order to create an operationally realistic joint test environment. Federated testing allows the test community to leverage assets in DOD labs, support contractor test beds, and ranges in lieu of and to complement scarce or limited operational systems and services.

a. Each MA/CPM should provide to the responsible operational test agencies, including JITC, the associated C/S/A and the PMs developing or procuring the mission area solution the following:

(1) The DOD Information Enterprise Architecture and solution architecture, to include the Service Oriented Architecture (SOA) components.

(2) Common data elements and network requirements, to include security profile, representing the operational context for the capability.

b. The MA/CPM, C/S/A, PMs and operational testers, including JITC, will determine the most efficient method to deliver the infrastructure required to create the MA/CPM architecture using the Joint Capability Areas (JCA) that represents the operational environment (including security profile) to a degree that can support, at a minimum, Joint Interoperability Test Certification.

c. Each PM and C/S/A that has systems in the MA/CPM architecture will provide access to either representative systems and/or verified and validated models. Model and simulations employed in the federated environment will be documented IAW MIL-STD-3022, Documentation of Verification, Validation, and Accreditation (VV&A) for Models and Simulations.

d. If not clearly identified in the CDD/CPD, the MA/CPM, C/S/A, PMs, and test organizations (to include JITC) will work together to develop the metrics and tools needed to evaluate to what degree a system under test contributes to a capability or to mission/task accomplishment.

e. Federated testing community members and possible venues for systems development and sustainment, operations and interoperability experimentation, and certification testing include many service and agency sites such as the DISA (JITC), the DOD Intelligence Information System (DODIIS) Independent Test Authority (ITA), and USJFCOM JSIC.

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

a. J-6 I&S Certification.

(1) Certified Capability Development Document (CDD), Capability Production Document (CPD), Information Support Plan (ISP), ISP Annex, Tailored ISP (TISP).

(2) Certified NR-KPP Annexes to previously approved/certified Requirements Generation System (RGS – predecessor to JCIDS) documents which are still valid (e.g., older Operational Requirements Documents (ORDs), C4I Support Plans (C4ISPs) allowed by ASD(NII)/DOD CIO when used as the source of requirements).

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 JITC has sufficient detail to develop a test methodology for each requirement (definable, testable and measurable).

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

(1) If applicable, approved Test and Evaluation Master Plan (TEMP), or a Test & Evaluation Strategy (TES), is available. As a minimum, all CPD/ISP enterprise-level and critical information exchanges will be used to develop the TEMP measures of effectiveness. Established Joint Threads will verify the operational effectiveness of information exchanges as documented in the OV-3 and SV-6.

(2) Coordination with JITC to develop an interoperability test and evaluation strategy, capitalizing on interoperability testing executed by C/S/A test organizations, as documented in an Interoperability Certification Evaluation Plan (ICEP), interoperability test plan, or equivalent documentation, as appropriate.

(3) 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 joint testing resources. 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 and shall be conducted prior to Joint Interoperability Testing with the JITC. Service PTUCs can also serve to coordinate participation of service resources in joint distributed federations that enable JITC joint interoperability testing.

(4) System standards in DISRonline have been validated, as applicable.

e. Results from standards conformance, Service testing, any assessments, etc. are available.

f. Coordination with JITC and/or Service level PTUC 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 to facilitate JITC leveraging C/S/A testing for use in the system's joint interoperability certification process.

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

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

7. 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 JITC orchestrates this process in concert with C/S/A.

a. The four basic steps to the certification process are:

(1) Identify (Interoperability) Requirements

(2) Develop Certification Approach (Planning)

(3) Perform Evaluation

(4) Report Certifications and Statuses

b. 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.

Requirements/capabilities are outlined in CPDs, ISPs, ISP Annexes, TISPs and must be detailed enough for testing. After the documents receive a J-6 I&S Certification, JITC can then plan for joint interoperability testing. The JITC provides input during the J-6 I&S 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 the JITC has sufficient time to define appropriate methodology for measuring and testing the warfighter's established and defined requirements and/or capabilities.

c. 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. This includes employing production representative systems, members of the user community as operators when feasible, 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. C/S/A on-going interoperability test activities will be leveraged to provide necessary test data when possible. Sponsors will coordinate with JITC to integrate interoperability and standards conformance test needs into the system's Test and Evaluation (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. Additionally, complex systems that depend on multiple evaluation events will require JITC to develop an Interoperability Certification Evaluation Plan (ICEP).

(1) Some systems and programs will have a TEMP (reference f) 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). The sponsor and JITC will work closely to establish a viable testing program that satisfies testing requirements in the most efficient and effective manner.

(2) JITC works with the system sponsor to develop an ICEP. The ICEP outlines how the system will be tested against the J-6 I&S Certification of the CPD/ISP/TISP. The testing may be conducted during DT&E, OT&E, service level interoperability and mil standard compliance testing, and various joint exercises and deployments.

(3) In support of test planning and JITC development of a certification approach and ICEP, system sponsor and developers will provide necessary

system technical data, architecture products, and interface specifications, and coordinate with JITC to identify test data collection requirements.

d. Perform Evaluation. Interoperability evaluation often spans Developmental Testing (DT) and Operational Testing (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 to leverage C/S/A testing to reduce costs and schedule impacts of interoperability testing.

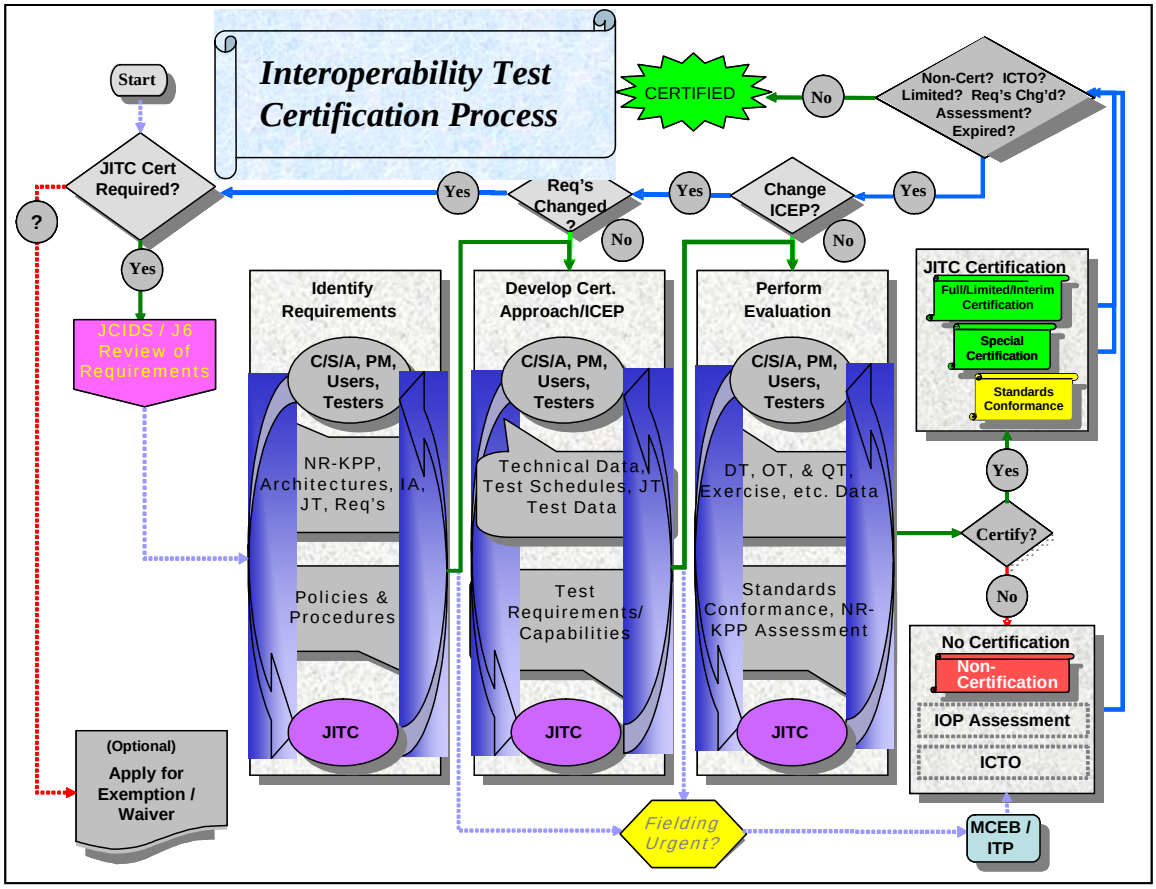


Figure F-1 Joint Interoperability Test Certification Process

Legend:			
Cert	Certification	JT	Joint Threads
DT	Developmental Test	MCEB/ITP	Military Communications-Electronics Board/Interoperability 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) When the DISA/JITC is not the responsible testing organization, the DISA/JITC will provide recommended provisions for incorporation in the DT or OT entrance and exit criteria relating to joint interoperability test certification to the system sponsor (for DT) or appropriate Operational Test Agency (OTA) (for OT). JITC will coordinate with the system sponsor or OTA to ensure test plans, analysis, and reports have sufficient data and information available to support a joint test certification determination, including the degree the system hardware and/or software is production representative, operationally realistic test configurations and environments, joint interfaces, etc. Sponsors must coordinate testing changes (e.g., schedule, locations, scope, methodology, etc.) with the JITC, since such changes may impact the JITC's ability to evaluate and certify.

(2) When the JITC is the responsible lead test organization, the 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 is scheduled and coordinated through the Service level PTUC and shall be conducted prior to Joint Interoperability Testing at the JITC. However, those systems that do not have a Service level PTUC should coordinate early with the 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 the JITC. The 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).

e. Report Certifications and Statuses. The JITC uses and accepts data from the various types of tests (DT/OT) 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.

(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 five NR-KPP elements (Encl D). The certification will also specify if it applies only to special operational environments, and will also indicate the expiration period.

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

8. 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., a different requirements document may be used in place of CPD).

a. Initiation of development/acquisition/procurement.

(1) Sponsor contacts JITC; POCs established, JITC STP entry made. JITC provides a cost estimate to the sponsor at no expense to the sponsor.

(2) Interoperability requirements established and test plans developed.

(a) Initial Capabilities Document (ICD)/CDD used to create test plans (ICEP, ITP, etc.) in conjunction with ISP, ISP Annex or TISP requirements coordinated with J-6.

(b) Any interoperability requirements issues resolved by J-6 and MCEB/ITP, with those related to intelligence resolved by the Military Intelligence Board (MIB).

b. Standards conformance and interoperability assessments may be performed (if system components are available).

(1) Standards Conformance Certifications issued.

(2) Interoperability Assessments produced, if needed.

c. 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.

d. Standards profiles validated, other validations and certifications occur.

e. Standards conformance and interoperability assessments continue throughout the development phase.

f. The JITC provides input to OTRR process, as requested.

g. The JITC provides testing status to J-6, MCEB/ITP, etc., as requested.

h. Interoperability testing conducted, usually in conjunction with OT.

i. The JITC interoperability evaluation performed.

(1) Joint Interoperability Test Certification issued. Full, limited, interim, or non-certification. Alternatively, an interoperability assessment letter/report may be produced.

(2) Interoperability status posted to the JITC STP, and distributed to appropriate parties (J-6, MCEB/ITP, and sponsor).

j. 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.

9. JITC Interoperability Products. The 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 Testing (OT) or 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. The 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. Joint Interoperability Test Certifications: All JITC joint interoperability test certifications expire upon changes that may affect interoperability. Additionally, all certifications expire four (4) years from original date of issue. PMs will ensure certification is current and valid and notify the JITC of system changes affecting interoperability. Whether recertification is granted following initial certification is based on changes to the IT and/or NSS changes. JITC may grant recertification with or without additional testing based on analysis of the impact of changes.

(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 need individual requirements certified by J-6 (e.g., commercial switches being procured to operate in the DSN, in-line encryption devices). Requirements for such systems are derived from the Unified Communications Requirements (UCR) as directed by CJCSI 6215.01 (reference uu). For systems not currently covered by the UCR, the JITC will work with J-6 to determine whether J-6 I&S Certification is required.

(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 an approval for fielding and the MCEB/ITP for an Interim Certificate to Operate (ICTO). The ICTO will specify the way ahead, but programs will strive for completing the Joint Interoperability Test Certification.

(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.

(4) Interim Joint Interoperability Test Certification. Issued when a capability module, that will be fielded in an incremental fashion, has adequately demonstrated interoperability for at least all critical threshold requirements identified for the increment. This interim certification attests that the capability's interoperability is sufficient to support a fielding decision. When the capability is fully mature and meets all critical threshold requirements for the entire module, it may qualify for a Joint Interoperability Test Certification. An Interim Joint Interoperability Test Certification expires whenever the incremental module will be replaced or revised, resulting in changes to NR KPP attributes, but no later than four years from original date of issue.

10. Interoperability Evaluation and Certification.

a. The following are applicable to all types of interoperability test certifications:

(1) The J-6 I&S Certification process. The JITC shall evaluate and make a certification determination based on the NR-KPP components in J-6 I&S certified documents.

(2) Interoperability requirements shall be used for evaluation and the status reported, not merely the capabilities that have been implemented. This includes all critical threshold requirements and all critical and 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 may require re-certification by J-6.

(3) ISPs and TISPs will address all enterprise level and external information exchanges, but as a minimum – due to test limitations and/or funding – all enterprise level and external joint critical 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 DOD Information Enterprise Architecture and solution architecture products, such as a capability to communicate on two channels simultaneously. Other interoperability-related requirements may be separate from the NR-KPP, such as the tagging of data, reliability of certain types of communications, etc.). Reasons for not evaluating all enterprise level and external information exchanges will be documented by the PM.

(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, to include the expected joint operating environment. 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 exchange and use of information to include established joint mission threads where these have been

defined and included in J-6 I&S certified documents. 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, reliability, completeness, and timing (i.e., QoS attributes); 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 and net-centric components (both services and data) to be certified and any interfacing capabilities and net-centric components.

(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), and the expected operational impact of any discrepancies. Expected operational impact includes the impacts to the system's ability to achieve the stated capability, and/or accomplish the operational task, the mission and 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 has 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 the NR-KPP, the evaluation will determine the operational status of the NR-KPP requirements (including interfaces, exchange requirements and other interoperability requirements). Test requirements shall be obtained from the NR-KPP in a J-6 I&S certified

document. The joint interoperability test certification must address the NR-KPP compliance statement, with the five primary elements of the NR-KPP and associated performance attributes, and provide the status of standards conformance. Specific guidance pertaining to the NR-KPP includes:

(1) DOD Information Enterprise Architecture and solution 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, defined in architecture products, and by exchange requirements. Interface status will include an identification of any GESPs associated with the interface and associated compliance status.

(2) Net-centric data and service strategies and the provisions of the DOD IEA (i.e., net-readiness). Evaluation of the net-centric data and services element to determine whether a system is net-ready:

(a) That applicable data and service metadata have been registered in the MDR, service registry, and enterprise catalogue, as appropriate.

(b) That the registered metadata is syntactically correct and incorporates the content necessary to establish data and service visibility, availability, and understandability.

(c) That the provider and consumer service descriptions, when exercised, enable appropriate data and service access and execution as described, and as constrained by access policies.

(d) That data and services provided by the capability may be discovered, accessed, and/or obtained by anticipated consumers.

(3) GIG Technical Guidance (GTG). Evaluation of compliance with GTG provisions includes verification:

(a) That standards declared in the TV-1 and deemed to pose greater operational risk due to associated information or system data exchange critically, product, protocol, or technology immaturity, or novelty or rarity of implementation, have been correctly implemented in the capability as evidenced by some combination of developmental and operational test results, separate government or commercial test laboratory conformance or compliance verifications, or JITC conformance certifications.

(b) That standards declared in the TV-1 and deemed not to pose greater operational risk as described in the preceding paragraph have been correctly implemented in the capability as evidenced by one of the means previously noted, or by letters or memoranda of conformance or compliance issued by a responsible officer of the program office, or vendor executive.

(c) That standards incorporated in the TV-1 as part of a GESP called for by the capability requirements correspond to the GESP versions and, where applicable, have been implemented in accordance with the standards profiles mandated by the cited GESP, as dictated by potential operational risk associated with the exchanges implemented using the GESP. The status of implementation of the cited GESPs will be reported separately as part of the certification evaluation.

(d) That interoperability testing demonstrates no performance limitations or discrepancies with significant operational impact attributable to non-conformance to standards.

(4) Information Assurance (IA). Compliance with IA requirements may be determined through IA processes defined as:

(a) DOD Information Assurance Certification and Accreditation Process (DIACAP). Verification consists of determining whether certification and accreditation (C&A) has been accomplished and, if so, what final C&A determination was made, e.g., Authorization to Operate (ATO), Interim ATO, (IATO), Interim Authorization to Test (IATT), or Denial of Authorization to Operate (DATO).

(b) C&A in accordance with Intelligence Community Directive Number 503 under either the National Security Agency/Central Security Service (NSA/CSS) Information System Certification and Accreditation Process (NISCAP), or in accordance with the C&A procedures defined by the Defense Intelligence Agency for the DOD Intelligence Information System (DODIIS). For capabilities evaluated with these processes, the JITC shall verify, determine and report the status accorded.

(c) For systems granted an exemption from DIACAP processes by a Designated Accrediting Authority (DAA), the program office or other proponent will provide a copy of the exemption memorandum to the JITC. IA requirements for these systems will be incorporated as part of normal design and test processes. Status will be reported in terms of accomplishment of the stated IA requirements.

(d) For all systems, determination shall be made regarding whether the IA configuration of the capability as tested corresponds to the IA configuration requirements asserted for the capability.

(e) For systems connecting to an enterprise network, e.g., NIPRNet, SIPRNet, JWICS, DSN, DRSN, etc., appropriate IA configuration and security scan testing dictated by the network manager for approval to connect shall be performed, and the status reported.

(5) Supportability requirements to include:

(a) Verification that the program developing the capability has completed the processes necessary to comply with applicable policies regarding:

1. Spectrum certification, achieved through submission and approval of a DD Form 1494.

2. Completion of applicable requirements of DOD Directive 3222.3, "DOD Electromagnetic Environmental Effects (E3) Program", including verification of Electromagnetic Compatibility (EMC), Electromagnetic Interference (EMI), and Electromagnetic Vulnerability (EMV), and other aspects as dictated by the capability and its operational environment.

(b) Verification that any GPS receiver equipment acquired for use as part of the capability conforms to the requirements of CJCSI 6130.01 for incorporation of a Selective Availability Anti-Spoofing Module (SAASM).

(c) Verification that any radio-based communications requirement to be satisfied as part of the capability under evaluation and operating in the Joint Tactical Radio System (JTRS) spectrum, 2 MHz-2 GHz, is acquired as a component capability from a JTRS-based program source. Exceptions to this policy may only be made by ASD (NII)/DOD CIO.

c. JITC Certification Determination – Joint Interoperability Test Certification. Interoperability test and evaluation quantifies the degree to which a system interoperates with other systems as required to provide a critical capability or to accomplish a mission or task. The status also conveys the level of risk associated with the system meeting requirements by identifying the expected operational impact of any discrepancies.

d. Foreign Systems. 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.

e. Homeland Security-Related Systems. The 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 I&S Certification, JITC cannot issue an interoperability test certification. However, JITC may produce assessments or standards conformance certifications, as appropriate.

f. 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 and documented in accordance with applicable policy before issuing any certification.

(1) The JITC certifies stimulator/simulator and training systems and may certify them in the same manner as operational systems. These systems must have J-6 I&S Certification first before the JITC joint interoperability test certification. The JITC does not certify that these systems provide an accurate model of any particular environment.

g. Validation of Test Tools and Standards. Test tools (and any associated components such as test suites) and standards/standards profiles will be validated before T&E use. The JITC does not have the unique mission to validate test tools or standards. However, the 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.

h. Testing Resources include:

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

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

i. Information Assurance (IA). The 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, the JITC shall confer with the National Security Agency (NSA) and user community, to confirm that IA characteristics of the environment are operationally realistic.

j. Recertification of Certification. Joint interoperability re-certification is required upon any of the following:

(1) When materiel changes (e.g., hardware or software modifications, including firmware) and similar changes to interfacing systems affect interoperability. The C/S/A is responsible for determining whether minor system version changes/updates affect interoperability;

(2) Upon revocation of joint interoperability test certifications;

(3) Upon automatic expiration four years after the date of the certification;

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

k. 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 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 four-year validity period. This "re-issued" certification may not require additional interoperability testing. However, requirements certification status shall be reconfirmed. Contact Joint Staff J-6 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 (other than a minor modification as specified in section k above), 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 the JITC to independently make a determination of the impact of changes. The extended certification will expire four 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).

l. Revocation and Re-issuance of the 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 JS 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.

m. Standards and Standards Profiles Conformance Test Methodology. Standards conformance testing is resource intensive. Testing is only practical for a fraction of the standards in a well-formed TV-1. Maximum use must be made of available developmental testing and commercial verification activities, in addition to formal DOD conformance certification. For standards that are critical to the capability being evaluated, and that may be high risk due to relative immaturity of the standard or the underlying technology, formal conformance certification is the preferred approach.

(1) 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. Other types of products may be extremely useful to the PM/proponent; however, they do not satisfy DOD requirements for having standards conformance and interoperability certifications.

(a) 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 must be based on a test plan that has procedures to test all requirements. Reporting of results must include 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.

(b) Standards identify mandatory and optional items without distinguishing their criticality. Complete conformance with complex standards is rare; therefore a status of "limited conformance" or "not met, but minor impact or workaround exists" may be appropriate and incorporate criticality.

(2) Verification of conformance achieved through other sources, such as developmental test results, commercial certification, or vendor letters of conformance may be used to substantiate conformance for standards less critical to the capability being evaluated, or that are more mature and pose minimal risk of incomplete or defective implementation. Given one or more of

these types of information, and an absence of significant discrepancies in interoperability testing of the affected interfaces and exchanges, testers may assert with low risk that the implementations evaluated have achieved acceptable conformance.

11. 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 test fund planning.

b. There may also be other certifications, validations, or accreditations required prior to fielding a system (e.g., DODI 8510.01 (DIACAP), electromagnetic spectrum, and authorization to connect to specific networks).

12. Other Considerations:

a. 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.

b. 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.

c. The MCEB/ITP may grant a temporary waiver from interoperability test certification requirements – an Interim Certificate to Operate (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).

d. 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:

(1) DIACAP/IA accreditation/certification requirements.

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

(3) TJTN approval for certain tactical networks.

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

e. Life-cycle support.

(1) The 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.

(2) The 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.

13. Joint Interoperability Testing Exemption Process.

a. General. Establishes procedures for Program Managers, Sponsors, C/S/A to request joint interoperability test exemption for systems that do not require Joint Interoperability Test Certification (e.g., single Service systems and systems with no joint interfaces). Systems enrolled in this program may be reviewed to ensure continued eligibility. Status, recommendations, and exemption memorandums are stored in the JITC STP, linked from the CJCSI 6212 Resource page.

(1) Applicability – Systems Exempt from Joint Interoperability Testing Certification. All systems that are used by a single C/S/A and possess no joint interfaces/information exchanges whether in development or already fielded do not require Joint Interoperability Testing.

(a) DAA approved IATO/ATO shall be obtained prior to requesting exemption from JITC interoperability testing and certification.

(b) Programs that have submitted capability documents for review will request a testing exemption only after receiving J-6 I&S certification.

(c) Already fielded IT and NSS, meeting the exemption criteria and without capability documents may request a testing exemption.

b. Testing Exemption Criteria.

(1) Single C/S/A system with no joint interfaces and no joint information exchanges, or

(2) Multi C/S/A systems with no joint interfaces or information exchanges, or

(3) Single or Multi C/S/A system whose only joint interface is a Global Positioning System (GPS) receiver. A GPS interface will only be construed as a joint interface when Precise Positioning Service (PPS) data is received, processed, and retransmitted on other joint interfaces for use by inter-C/S/A (joint) users. Such reception, processing, and retransmission of PPS data constitutes a valid joint interoperability concern for the larger warfighting enterprise and makes joint interoperability testing of such GPS interfaces a

value added proposition. A system that receives GPS data for incorporation into its own position and navigation computations would not require evaluation so long as:

(a) The user determines the positional/time accuracies provided by the receiver selected meets mission needs, and

(b) The proponent procures a Selective Availability Anti-Spoofing Module (SAASM) compliant receiver in accordance with Chairman of the Joint Chiefs of Staff Instruction (reference zz), or

(4) IT or NSS capability employed by different C/S/A's but only having information exchange within its C/S/A organization.

c. Process for Requesting an Exemption. Requests shall be forwarded to the appropriate MCEB Interoperability Test Panel (ITP) representative. Specific instructions and format are linked from the CJCSI 6212 Resource Page. Joint Staff J-6 will concur or non-concur with the request typically within 30 calendar days of receipt.

(1) Responsibilities:

(a) Requestors (C/S/A/PMs/Sponsors) will:

1. Download and completely fill out the request form located on the Interoperability Test Panel (ITP) web page.

2. Provide a written description of the system and its intended operational use.

3. Submit the request to the appropriate MCEB ITP representative. The current ITP member list can be found on the ITP web page.

4. Demonstrate the system has no joint interfaces/information exchanges. If any joint interfaces/information exchanges are present, requestors shall address the criticality to the joint operational environment and the risk to the warfighter of these joint interfaces/information exchanges. It is the PM's/Sponsor's responsibility to make the case for testing exemption.

5. Work through the ITP representative to provide additional documentation or rebuttal that provides a rationale in support of the exemption requests, if a disagreement occurs over a DISA/JITC recommendation.

(b) ITP representatives will:

1. Act as the interface between the PM/sponsor and JITC for all testing exemption related issues.

2. Ensure and validate submitted requests address the program criteria.

3. Obtain a JITC testing exemption recommendation by submitting the request via email to the JITC for evaluation and recommendation using the JITC Testing Exemption Recommendation Mailbox address. Include the J-6 when submitting the request.

4. Upon receiving JITC recommendation, forward the approved request package to J-6 for final evaluation/approval.

5. If JITC does not approve the exemption, return the request to the PM/Sponsor for additional documentation/rebuttal if necessary.

(c) JITC will:

1. Evaluate only exemption requests or requests for amending a recommendation that are provided by the ITP representative to the JITC Testing Exemption Recommendation Mailbox.

2. Create an STP entry for the system if it does not already exist.

3. Review the request and any other documentation provided by the PMs or obtained through other sources (JCPAT-E, www, etc.).

4. Provide a recommendation to the ITP representative and JS.

5. Return requests received directly from the PM/Sponsor with direction to submit the requests through the appropriate ITP Representative.

6. Distribute recommendation to J-6, the requesting ITP Representative, JITC, and the STP via the JITC's Electronic Report Distribution (ERD) system via e-mail.

7. Not address a program's costs in evaluating exemption requests.

8. The JITC's focus is joint interoperability concerns for the warfighter.

(d) J-6 will review/approve/disapprove requests on exempting the system from Joint Interoperability Testing. The J-65B Division Chief retains final approval authority.

(2) Guidelines. Requests and supporting documentation must show the system has no joint interfaces/information exchanges and will be/is used by a single C/S/A. Requests must be complete and valid prior to submission to the MCEB ITP Representative. Submitting additional information (e.g.,

Concept of Operation, MNS, ORDS, TEMPs, ICDs, CDDs, C4ISPs) is encouraged to strengthen the case for testing exemption. Regular information exchanges between the PM/sponsor and the JITC SMEs researching the exemption request are encouraged in order to assist JITC in making the correct recommendation

(a) PMs/Sponsors must keep in mind that a certified subsystem does not guarantee proper integration into a larger program, nor is it an acceptable substitute for joint interoperability test & certification. The operational effectiveness of the information exchange must be verified. The overall system requirements (to include subsystems) are within the scope and responsibility of the integrating PM. Even when subsystems have met their own requirements, some level of testing is virtually always needed to confirm functionality and interoperability once integrated into a larger system. As such, the use of certified systems on a platform or within a larger program is not on its own a valid argument for testing exemption.

(b) ITP Representative Guidelines. ITP representatives must ensure that requests are complete and address the program criteria. Incomplete and/or invalid requests will be sent back to the requesting agent.

(c) JITC Guidelines. The JITC Subject Matter Experts (SMEs) will thoroughly review testing exemption requests and any supporting documentation to identify any interoperability issues in the system.

(d) Operational Centers (OCs) Guidelines.

1. C/S/As frequently integrate capabilities to plan, manage, and execute ongoing operations, i.e., OCs hosting various non-embedded subsystems or components. The integrated capabilities consist of a combination of personnel, communications and computing capability, shelter, mobility, environmental and power assets which will be tailored to the operational construct in which they are employed

2. The PM or Material Developer for the OC hosting various non-embedded subsystems or components may request a Test Exemption. The subsystems or components within the OC must satisfy Service and JITC interoperability requirements prior to being hosted. In requesting the Test Exemption, the PM or Material Developer for the OC must provide a list of hosted non-embedded subsystems or components, including system or component version numbers and their interoperability status. Where a subsystem or component provides options enabling a wide range of capabilities, configuration information sufficient to indicate the options available shall be provided for the component or subsystem.

14. 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 database.

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 CJCSI 6212 Resource page for instructions on requesting access.

ENCLOSURE G

REFERENCES

a. CJCSI 3170.01F, 1 May 2007, "Joint Capabilities Integration and Development System"

b. "Manual for the Operation of the Joint Capabilities Integration and Development System" Note: Replaces CJCSM 3170 with web based content upon release of CJCSI 3170.01G. Once established, a link to the reference will be maintained on the CJCSI 6212 Resources Page

c. DODD 4630.05, 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 5000.01, 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 (DISR) located on the NIPRNET at https:// DISRonline.disa.mil/ and on the SIPRNET at http:// DISRonline.disa.smil.mil/

h. DODD 8100.01, 19 September 2002, "Global Information Grid (GIG) Overarching Policy"

i. DODD 3222.03, 8 September 2004, "DOD Electromagnetic Environmental Effects (E3) Program"

j. DODD 4650.01, 8 June 2004, "Policy for Management and Use of the Electromagnetic Spectrum"

k. U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management," January 2008 Edition

l. DOD Architecture Framework (DODAF) 1.5 (2.0 when available)

m. Global Information Grid (GIG) Architecture, Version 2.0, 9 December 2003

n. DODD 8500.01E, 24 October 2002, "Information Assurance (IA)" Certified Current as of 23 April 2007

o. DODI 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"

p. DODI 8580.1, 9 July 2004, "Information Assurance (IA) in the Defense Acquisition System"

q. DODI 8510.01, 28 November 2007, "DOD Information Assurance Certification and Accreditation Process (DIACAP)

r. Information Assurance (IA) Component of the Global Information Grid (GIG) Integrated Architecture, Increment 1, Version 1.1, 16 November 2006

s. Net-Centric IA Strategy, 30 June 2004

t. National Security Space Acquisition Policy 03-01, 27 December 2004

u. DODD 8320.02, 2 December 2004, "Data Sharing in a Net-Centric Department of Defense" Certified Current as of 23 April 2007

v. DOD Chief Information Officer memorandum, 9 May 2003, "DOD Net-Centric Data Strategy"

w. DOD Chief Information Officer, "DOD Net-Centric Services Strategy," 4 May 2007

x. JROCM 010-08, 14 January 2008, "Approval to Incorporate Data and Service Exposure Criteria into the Interoperability and Supportability Certification Process"

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 Management Act of 2002, E-Government Act (Public Law 107-347), title III

aa. Defense Acquisition Guidebook November 2006

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)"

dd. DODD 8581.1, 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. ODD 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 3312.01A, 23 February 2007, "Joint Military Intelligence Requirements Certification"

kk. Horizontal Integration JROCM 124-04

ll. CJCSI 6510.01E, 15 August 2007, "Information Assurance (IA) and Computer Network Defense (CND)"

mm. CJCSI 5122.01C, 31 May 2007, "Theater Joint Tactical Networks Configuration Control Board Charter"

nn. CJCSI 3470.01, 15 July 2005, "Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) In The Year of Execution" Current as of 09 July 2007

oo. NIST SP 800-53, Recommended Security Controls for Federal Information Systems, December 2007

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

qq. ASD(NII)/DOD CIO memorandum, 12 January 2007 "Reinstatement of the Joint Tactical Radio, (JTRS) Waiver Process for Handheld Radio Procurements"

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

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

tt. Defense Information Enterprise Architecture 1.0 (DOD IEA 1.0)

uu. CJCSI 6215.01C, 9 November 2007, Policy for Department of Defense (DOD) Voice Networks With Real Time Services (RTS)

vv. DOT&E memorandum, 21 November 2006, Policy for Operational Test and Evaluation of Information Assurance in Acquisition Programs

ww. DOD and IC memorandum, 17 April 2008, Department of Defense (DOD) and Intelligence Community (IC) Initial Release of Universal Core (UCore)

xx. DOT&E Policy for Operational Test and Evaluation of Information Assurance (IA) in Acquisition Programs, 21 November 2006

yy. ICPG 105 Acquisition Policy, 12 July 2007, and Top Secret/Sensitive Compartmented Information (SCI) And Below Interoperability Policy (TSABI), 7 February 2000

zz. CJCSI 6130.01D Master Positioning, Navigation and Timing Plan (MPNTP),13 April 2007

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
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
C/S/A	Combatant Commands, Services, Agencies
CCB	Configuration Control Board
CDD	Capability Development Document
CDR	Critical Design Review
CECOM	Communications-Electronics Command
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
CM	Capability Module
CND	Computer Network Defense

COCOM	Combatant Command
COI	Communities of Interest
COTS	Commercial off the Shelf
CPD	Capabilities Production Document
CPM	Capability Portfolio Manager/Management
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
DDMS	DOD Discovery Metadata Specification
DIA	Defense Intelligence Agency
DIACAP	Defense Information Assurance Certification and Accreditation Process
DICE	DOD Interoperability Communications Exercise
DOD IEA	Defense Information Enterprise Architecture
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DOD Information Technology Standards Registry
DITPR	DOD Information Technology Portfolio Repository
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
DREN	Defense Research and Engineering Network
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
EISP	Enhanced Information Support Plan
EIE	Enterprise Information Environment
EMC	Electromagnetic Compatibility
eSMART	Enhanced Systems Management and Requirements Transformation

F

FCB	Functional Capabilities Board
FDCE	Federated Development & Certification Environment
FISMA	Federal Information Security Management Act
FRP DR	Full-Rate Production Decision Review
FY	Fiscal Year

G

GEOINT	Geospatial Intelligence
GESP	GIG Enterprise Services Profile
GIG	Global Information Grid
GIG-ES	GIG Enterprise Services
GPS	Global Positioning System
GTG	GIG Technical Guidance

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 Authorization to Operate
IAW	In Accordance With
IC	Intelligence Community
ICD	Initial Capabilities Document
ICEP	Interoperability Certification Evaluation Plan
ICTO	Interim Certificate To Operate
IOC	Initial Operational Capability
IP	Internet Protocol
ISOP	IT Standards Oversight Panel
iSMART	Interoperable Systems Management and Requirements Transformation

ISP	Information Support Plan
ISSE	Information System Security Engineering
IT	Information Technology
ITP	Interoperability Test Panel
ITP	Interoperability Test Plan
ITWL	Interoperability Test Watch List
IWL	Interoperability Watch List

J

JCA	Joint Capability Area
JCIDS	Joint Capabilities Integration and Development System
JCMT	Joint Critical Mission Threads
JCPAT	Joint C4I Program Assessment Tool
JCPAT-E	Joint C4I Program Assessment Tool - Empowered
JCSFL	Joint Common System Function List
JITC	Joint Interoperability Test Command
JPD	Joint Potential Designator
JROC	Joint Requirements Oversight Council
JRFL	Joint Restricted Frequency List
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

KM/DS	Knowledge Management/Decision Support
KDP-B	Key Decision Point Milestone B
KPP	Key Performance Parameter

M

MA	Mission Area
MAC	Mission Assurance Category
MASINT	Measurement and Signature Intelligence
MCEB	Military Communications-Electronics Board
MDA	Milestone Decision Authority
MDR	DOD Metadata Registry
MIB	Military Intelligence Board
MOSA	Modular Open Systems Approach
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
NSG	National System for Geospatial Intelligence
NSS	National Security Systems

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
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
RSS	Real Simple Syndication

S

SAASM	Selective Availability Anti-Spoofing Module
SAP	Special Access Program
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
SOA	Service Oriented Architecture
SSAA	System Security Authorization Agreement
STP	System Tracking Program
SV	System / Service View

T

T	Threshold
T&E	Test and Evaluation
TDL	Tactical Data Link
TEMP	Test and Evaluation Master Plan
TES	Test and Evaluation Strategy
TISP	Tailored Information Support Plan (ISP)
TJTN	Theater Joint Tactical Networks
TV	Technical Standards View

U

UCR	Unified Capabilities Requirements
UCore	Universal Core
UDDI	Universal Description, Discovery and Integration
USA	United States Army
USAFRICOM	United States Africa Command
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
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

W

WSDL	Web services Description Languages
WWW	World Wide Web

X

XML	Extensible Markup Language
XSD	XML schema definitions

(INTENTIONALLY BLANK)

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.

All Views AV-1 and AV2. These two products are defined as Overview and Summary Information (AV-1) and Integrated Dictionary (AV-2). The AV-1 provides executive level summary information to support quick reference and comparison among architectures. The AV-2 contains definitions and terms used in the given architecture.

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.

CPM – Capability Portfolio Managers: Established to manage like capabilities, as defined by the Tier 1 Joint Capability Areas, across the DOD enterprise in order to improve interoperability, minimize capability redundancies and gaps, and maximize capability effectiveness.

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 U.S. IT and NSS and one or more coalition partner IT and NSS.

Combined interface. Any interface that passes information between one or more U.S. 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 v)

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 Enterprise Architecture. A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define: (a) the people,

processes, and technology required in the "current" and "target" environments, and (b) the roadmap for transition to the target environment.

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 Standards Registry (DISR). 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, 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 Information Technology Standards Registry (DISR) online. DISRonline is a collection of web-based applications (Standards Profile building, registry Configuration Management and change tracking), which have been developed to provide the support necessary for the continued evolution of the DISR and the automation of the processes that use it. The use of DISRonline is required to identify DISR mandatory standards and develop and publish TV-1's for a program's DOD Information Enterprise Architecture and solution architecture.

DOD Interoperability Communications Exercise (DICE). A global exercise conducted three times a year 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.

Enhanced Information Support Plan (EISP). Use of the EISP is encouraged to facilitate the development of standard ISP and TISP formats and assist programs in risk mitigation. The EISP tool is a desktop software application that provides a standard methodology for discovery, analysis, and management of an acquisition program’s information dependencies. Data entered into the EISP tool will be tagged with XML. The tagging is transparent to the user and requires no PM’s actions but enables the data to be easily stored, searched, retrieved, and reused. The EISP process uses a predefined output script that automatically creates a PDF ISP or TISP document. Information on the EISP tool is available on the CJCSI 6212 Resource Page, https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page

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; electro-static discharge; hazards of radiation to personnel, ordnance, and volatile materiel's; and natural phenomena effects, of lightning and precipitation static.

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, e.g., business organization, command, component, service, or agency.

Federated Test Environment. A live, virtual, constructive distributed environment for testing.

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 Technical Guidance (GTG). GIG Technical Guidance (GTG) is an evolving web enabled capability providing the technical guidance necessary for an interoperable and supportable GIG built on Net-Centric principles. It is being developed in stages and the content baselines are to be vetted and released for use by the Joint Staff as they are developed. It aids program managers, portfolio managers, engineers and others in answering two questions critical to any IT or NSS: (1) Where does the IT or NSS fit, as both a provider and user, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability (2) What must an IT or NSS do to ensure technical interoperability with the GIG? The GTG incorporates reference tools for the DISRonline to facilitate access and use of DISR approved standards in development of technical views. The GTG will only reference standards that are posted in the DISR. The GTG will incorporate the DISRonline to facilitate PM's access and use of DISR standards in developing the Technical Views supporting their DOD Information Enterprise Architecture and solution

architectures. The GTG-DISRonline interface is a mechanism that allows the PM's to find standards that are specifically related to GTG content.

Global Information Grid (GIG). The globally interconnected, 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.

Global Information Grid (GIG) Enterprise Service Profiles. GIG ESPs (GESP)provide a net-centric oriented approach for managing interoperability across the GIG based on the definition and configuration control of key interfaces and enterprise services. The GESP is the set of guiding documentation produced as a result of enterprise wide engineering analysis based upon consideration of the following criteria:

- The capability spans organizational boundaries
- The capability is mandatory or mission critical across the GIG Enterprise
- The capability can be characterized in a consistent DOD Information Enterprise Architecture and solution architecture
- The capability is essential for resolving GIG end-to end interoperability issues
- The capability enables net-centric information sharing for multiple acquisition programs

GESPs provide a description of required operational functionality, and technical specifications for using and interfacing GIG enterprise services. A GESP contains:

An Interoperability Reference Architecture and Service Description section which contains an interoperability reference architecture and graphic and a service description; an interoperability requirements and secured availability section; a technical implementation profile for critical GIG Technical Standards

and interfaces that are part of the GESP; a maturing guidance section; a compliance testing section; a key programs implementing the GESP section; a data section; and a references section.

IA Component of the GIG Architecture. Documents the Enterprise IA protection strategy, technical framework and recommended IA transition strategy to securely enable net-centric operational capabilities. The IA Component, Version 1.1, is intended to influence Office of the Secretary of Defense (OSD), Agency and Service architectures, as well as the GIG constituent programs and IA solution developers.

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.

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 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 IA.

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 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.

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

Joint Capability Area (JCA). Collections of like DOD activities functionally grouped to support capability analysis, strategy development, investment decision making, capability portfolio management, and capabilities-based force development and operational planning.

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 composed of Flag Officer/General Officer representatives of the Services.

Joint Capabilities Board Interest. ACAT II and below programs where the capabilities and/or systems associated with the document affect the joint force and an expanded joint review is required. These documents will receive all applicable certifications, including a weapon safety endorsement when appropriate, and be staffed through the JCB for validation and approval.

Joint Capabilities Document (JCD). *Note: This document was deleted from the JCIDS process and will no longer be produced*. 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 DOD Information Enterprise Architecture and solution architectures to identify prioritized capability gaps and integrated DOTMLPF solutions (materiel and non-materiel) to resolve those gaps.

Joint Common System Function List (JCSFL): provides a common lexicon of system functions supporting development of DOD Information Enterprise Architecture and solution architecture and horizontal / vertical assessment of capability across an enterprise.

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, JCB Interest or Joint Integration.

Joint Interoperability Test Certification. Provided by JITC upon completion of testing, valid for four 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; 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.

Joint Mission Thread. An operational and technical description of the end to end set of activities and systems that accomplish the execution of a joint mission.

Joint Systems Integration Command (JSIC). Located in Suffolk, Va. and is assigned as a subordinate command to the U. S. Joint Forces Command (USJFCOM). JSIC provides a unique environment that brings together operational and technical expertise, technology, state-of-the-art facilities, defendable and repeatable scientific methodology to enhance joint command and control (C2) capabilities, and solve joint interoperability problems. JSIC's core competencies include: Interoperability Assessments**,** Capability Assessments, and Capability Integration. The JSIC directly supports all the combatant commands by validating current and proposed warfighter C2 systems. This process identifies systems that clearly demonstrate joint utility.

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 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.

Legacy System. Any existing system that works satisfactorily and the owner sees no reason to change it; in other words, replacing it with a new system would have a prohibitive attendant cost in time and/or money.

Metadata. Is descriptive information about the meaning of other data. Metadata can be provided in many forms, including XML 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.

Military Communications-Electronics Board (MCEB). As directed by DODD 5100.35, the MCEB considers military communications-electronics matters including those associated with National Security Systems by the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the DOD Chief Information Officer, and other designated officials. MCEB functions and responsibilities include coordination among DOD Components and other Governmental Departments and Agencies on matters related to military communications-electronics, provide frequency spectrum management solutions, and to develop, review, and implement procedures in the DOD EMC 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; IA; 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).

With: Net-Centric. The ability to provide a framework for full human and technical connectivity and interoperability that allows all DOD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.

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). *Note: NCOW RM element of the NR-KPP has been removed from this instruction. Its components have been integrated into the other elements of the NR-KPP.* 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 and NSS that meets required information needs, information timeliness requirements, has IA accreditation, and meets the attributes required for both the technical exchange of information and the operational effectiveness of that exchange. DOD IT and 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 and 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 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 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 U.S., Allied, and Coalition forces.

g. Across current and future systems.

Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP is a key, parameter stating a system's information needs, information timeliness, IA, and net-ready attributes required for both the technical exchange of information needs, information timeliness, IA, and net-ready attributes required for both the technical exchange of information and the operational effectiveness of that exchange. The NR-KPP consists of information 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 composed of the following elements: 1) Compliant solution architecture, 2) compliance with DOD Net-centric Data and Services strategies, including data and services exposure criteria (references u through x), 3) compliant with applicable GIG Technical Direction to include DISR mandated IT Standards reflected in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Information Enterprise Architecture and solution architecture system/service views, 4) verification of compliance with DOD IA requirements (references n through s), and 5) compliance with Supportability elements to include, Spectrum analysis, Selective Availability Anti-Spoofing Module (SAASM) and the Joint Tactical Radio System (JTRS).

Open Standard. Widely accepted and supported standards set by recognized standards organizations. 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.

Shared Space. A mechanism that provides storage of and access to data for users within a bounded network space. Enterprise-shared space refers to a store of data that is accessible by all users within or across security domains in the GIG. A shared space provides virtual or physical access to any number of data assets (e.g., catalogs, web sites, registries, document storage, and databases). As described in this strategy, any user, system, or application that posts data uses shared space. (Appendix A. Terminology, DOD Net-Centric Data Strategy, May 9, 2003)

Solution Architecture. The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.

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).

Standard Conformance Testing. Testing the extent to which a system or subsystem adheres to or implements a standard.

Standard Conformance Certification. Confirmation that an IT, including NSS, has undergone IT standards conformance testing with respect to a given standard, and correctly implements the standard, with specified profiles and options, where applicable.

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.

Supportability. The ability of systems and infrastructure components, external to IT or NSS, to achieve, aid, protect, complement, or sustain design, development, testing, training, or operations of the IT or NSS to its required capability.

Systems/Services 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.

Tailored Information Support Plan (TISP). The purpose of the TISP process is to provide a dynamic and efficient vehicle for certain programs (ACAT II and below) to produce requirements necessary for I&S Certification. Select program managers may request to tailor the content of their ISP (ref ss). For programs not designated OSD special interest by ASD (NII)/DOD CIO, the component will make final decision on details of the tailored plan subject to minimums specified in the TISP procedures linked from the CJCSI 6212 resource page and any special needs identified by the J-6 for the I&S certification process.

Technical Standards View (TV). 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.

Test and Evaluation Strategy (TES). An early test and evaluation planning document that describes test and evaluation activities starting with Technology Development and continuing through System Development and Demonstration into Production and Deployment. The TES describes how component technologies being developed will be demonstrated in a relevant environment to support the program's transition into the System Development and Demonstration Phase. Over time, the scope of this document will expand and evolve into the Test and Evaluation Master Plan (TEMP) due at Milestone B.

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

Universal Core (UCore). Designed to improve information sharing by defining and exchanging a small number of important, universally understandable concepts across a broad stakeholder base. Establishment of formal data sharing communities (i.e., Communities of Interest or domains) is improving the situation by developing common vocabularies within specific mission or business areas. Sharing information outside these communities remains a challenge typically requiring complex mediations. The goal of UCore is to make it easier for programs to share information within and across communities.

(INTENTIONALLY BLANK)