



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-8
DISTRIBUTION: A, B, C, S

CJCSI 6212.01F
21 March 2012

NET READY KEY PERFORMANCE PARAMETER (NR KPP)

Reference: See Enclosure F.

1. Purpose. This instruction:

a. Defines responsibilities and establishes policy and procedures to develop the NR KPP and NR KPP certification requirement for all information technology (IT) and national security systems (NSS) that contain joint interfaces or joint information exchanges (hereafter referred to as IT and defined as 'used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, or transmission or reception of DoD data of information regardless of classification or sensitivity) (references a and b). (Enclosures A and B).

b. Establishes procedures for the NR KPP certification requirement for Joint Requirements Oversight Council (JROC) Joint Capabilities Integration and Development System (JCIDS) (Enclosures C and D).

c. Establishes procedures to certify the NR KPP, with accompanying architecture data, and compliance with spectrum requirements for all Capability Development Documents (CDDs) and Capability Production Documents (CPDs). Additionally, establishes procedures for the review of the architecture data, as applicable, in JCIDS documents, including Capability-Based Assessments; Initial Capability Documents (ICDs); Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) Change Recommendations (DCRs); Concepts of Operations (CONOPS); CDDs; and CPDs. (Enclosures C and D).

d. Establishes NR KPP architecture data development methodology compliant with the current DOD Architecture Framework (DODAF) guidance (reference g) and provides an optional NR KPP Architecture Data Assessment

Template and alignment to Global Information Grid 2.0 (reference h), DoD IT Standards Registry (DISR) (reference p), and Joint Information Environment Operational Reference Architecture (JIE ORA)/ Warfighting Enterprise Architecture (WEA) guidance (reference z). (Enclosures C and D).

2. Cancellation. CJCSI 6212.01E, 15 December 2008, "Interoperability and Supportability of Information Technology and National Security Systems" is canceled.

3. Applicability. Per references a through d, this instruction applies to:

a. The Joint Staff, Military Departments and Services, Combatant Commands, Defense Agencies, DOD field activities, and joint and combined activities (hereafter referred to as DOD Components) (reference a).

b. Federal agencies preparing and submitting JCIDS documents (references c and d).

c. All IT acquired, procured, or operated by any DOD Component. In this instruction, IT includes, but is not limited to: NSS, IT acquisition programs, information systems, IT initiatives, IT services, software, electronic warfare devices, DBS, prototypes (reference e), Commercial-Off-the-Shelf (COTS), leased, Government Off-the-Shelf, Rapid Fielding (reference dd), Special Access Program, Joint Capability Technology Demonstration, Coalition Warrior Interoperability Demonstration, Combatant Command Initiatives Fund (CCIF), IT systems and subsystems that are integral to embedded weapons platforms and non-program of record materiel solution efforts. It does not apply to non-Global Information Grid (GIG) IT as defined by reference i. Hereafter, the term IT will be used in this document.

d. Compliance. New JCIDS documents, not already in the system, must comply with this instruction. All documents submitted 6 months after the signature date of this instruction must comply with this instruction. JCIDS documents entering their review cycle within 6 months of this instruction's release date may request permission from the Joint Staff to comply with the previous version of this instruction.

4. Policy

a. It is Joint Staff policy to ensure DOD Components develop, acquire, test, deploy, and maintain IT that:

(1) Meets the essential operational needs of U.S. forces;

(2) Uses architecture data to develop the NR KPP that is certified in JCIDS documents and reviewed in Information Support Plans (ISPs) (reference d).

(3) Are interoperable and supportable with existing, developing, and proposed (pre-MS A) IT through architecture, standards, defined interfaces, modular design, and reuse of existing IT solutions;

(4) Are supportable over the DOD GIG (see reference h and r);

(5) Are interoperable with host nation, multinational coalition, and federal, state, local, and tribal agency partners;

(6) Provides global authentication, access control, and directory services; provide information and services from the edge; utilize joint infrastructure; provide unity of command; and comply with common policies and standards (reference h and v);

(7) Leverages emerging capability-based references and methods, including the Joint Capability Areas (JCA) (references c, d, and m (as a common language to discuss and describe capabilities across many related DOD activities and processes)), Joint Mission Threads (JMT), and the Joint Common System Function List (JCSFL) (reference k).

(8) Complies with spectrum requirements throughout the system's life cycle. Combatant Commands/Services/Agencies (C/S/A) ensure capabilities are aligned and interoperable during the development cycle; and

(9) Complies with DOD Interoperability and Supportability (I&S) policy and instruction (references a and b).

b. NR KPP Attributes for Certification. The NR KPP is based on three attributes and JROC validated performance measures and metrics (reference d) identified by the IT's sponsor. Detailed NR KPP attributes and metric development guidance is in Enclosures C and D and on the NR KPP Manual Wiki page (reference gg). The three NR KPP attributes are:

(1) IT must be able to support military operations.

(2) IT must be able to be entered and managed on the network.

(3) IT must effectively exchange information.

c. NR KPP Certification and Revalidation of Certification. All JCIDS documents are to be developed using the Capability Development Tracking and Management (reference y) and reviewed via KM/DS to certify the NR KPP and

21 March 2012

spectrum requirements. In addition, supporting architecture data is reviewed for compliance with the current DODAF. If DODAF Meta-model (DM2) Physical Exchange Specification (PES) compliant tools are not available to develop architectures, the optional NR KPP Architecture Data Assessment Template can be used for the architecture development process described in Enclosure D and on the NR KPP Manual Wiki page. The optional NR KPP Architecture Data Assessment Template provides a fit-for-purpose view in compliance with the current DODAF.

(1) ISP Reviews. NR KPP contained in the ISP is reviewed for recommendation to DOD CIO, including current DODAF architecture data or the optional NR KPP Architecture Data Assessment Template, and spectrum requirements compliance.

(2) Other IT. NR KPP certification of non-JCIDS/non-acquisition IT (i.e., fielded IT) is mandatory as described in Enclosure C and on the NR KPP Manual Wiki page.

(3) Baseline Capabilities Lifecycle (BCL) Documents. All BCL documents (reference f) entered by the JCIDS gatekeeper into KM/DS are reviewed (references e and f). The Business Case should include how the proposed capability supports military operations from the problem statement and identify if the proposed capability can be entered and managed on the network and can effectively exchange information. The solution architectures will also be evaluated for alignment with the most current DODAF and the JIE ORA/WEA (reference z). Business systems determined to not have a Joint Interest by the JROC do not carry a NR KPP certification requirement.

d. NR KPP Review and Certification Requirement. NR KPP review and certification requirement in this instruction and the NR KPP Manual align to the JCIDS process (references c and d).

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes

a. Renames the instruction from “Interoperability and Supportability of Information Technology and National Security Systems” to “Net Ready Key Performance Parameter (NR KPP).”

b. This revision eliminates previous elements and activities (information assurance, data and services strategy, GIG Technical Guidance compliance, supportability compliance) from the NR KPP that are accomplished through

other processes. The discussion of these former NR KPP elements is described below.

(1) Compliant solution architecture—within the context of the refined NR KPP—now DODAF Architecture data.

(2) The requirement to comply with the Net Centric Data and Services Strategies remains, but is no longer part of the NR-KPP. For NR KPP purposes compliance verification information (Data/Service Exposure Verification Tracking Sheet – “Bluesheet” – data) is provided DIV-3 submissions.

(3) GIG Technical Guidance (GTG) – exists in the ISP.

(4) DOD Information Assurance (IA) requirement – exist as a DAA responsibility.

(5) Supportability requirements – exists in the ISP but spectrum requirements compliance will continue to be analyzed within the refined NR KPP.

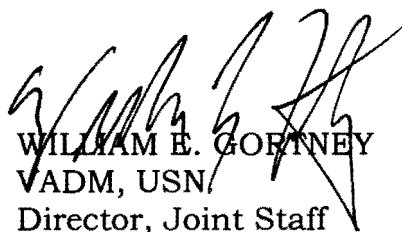
c. The NR KPP was redefined as three attributes focused on program-specific, validated, verifiable performance measures and metrics.

d. NR KPP architecture development methodology (based on DODAF architecture or the optional NR KPP Architecture Data Assessment Template) was added with a requirement to align with DOD Information Enterprise Architecture (IEA) (reference m), the current DODAF, JIE ORA/WEA and JCSFL.

e. Process details were removed from the instruction and added to the NR KPP Manual Wiki page to allow for more rapid dissemination of changes.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.

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


WILLIAM E. GORNEY
VADM, USN
Director, Joint Staff

Enclosures:

- A - Responsibilities
- B - Process Overview and Staffing Procedures
- C - NR KPP Development and NR KPP Certification
- D - NR KPP Architecture Development Methodology
- E - References
- GL - Glossary

DISTRIBUTION

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

	<u>Copies</u>
Under Secretary of Defense for Acquisition, Technology, and Logistics	2
Under Secretary of Defense for Personnel and Readiness	2
Under Secretary of Defense for Policy	2
Under Secretary of Defense for Intelligence	2
Deputy Chief Management Officer	2
DOD CIO	2
Director, Operational Test and Evaluation	2
Director, National Intelligence	2
United States Coast Guard	2
National Guard Bureau	2

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	Page
ENCLOSURE A RESPONSIBILITIES	
The Joint Staff J8	A-1
DOD Components.....	A-3
Sponsors	A-4
PMs.....	A-5
Combatant Commands.....	A-7
DISA.....	A-8
Director, NGA.....	A-9
Director, NSA	A-9
ENCLOSURE B PROCESS OVERVIEW AND STAFFING PROCEDURES	
Overview.....	B-1
Process Relationships.....	B-1
NR KPP Certification Process	B-2
NR KPP Staffing Levels and Timelines	B-5
C4/Cyber FCB Adjudication	B-6
Review Timelines	B-6
Failure to Meet Certification Requirements	B-7
Recommendations	B-7
Uniform Resource Locators.....	B-7
ENCLOSURE C NR KPP DEVELOPMENT AND NR KPP CERTIFICATION PROCEDURES	
NR KPP Overview.....	C-1
Types of NR KPP Certification	C-1
Attribute Characteristics	C-1
NR KPP Functions	C-4
NR KPP Development.....	C-4
NR KPP 3-Step Process.....	C-4
NR KPP Example	C-6
Supportability Requirements Compliance	C-6
ENCLOSURE D NR KPP ARCHITECTURE DEVELOPMENT METHODOLOGY	
Architecture Development Methodology and Interoperability	D-1
DOD IEA Alignment.....	D-3
NR KPP Information and Architecture Views	D-4
ENCLOSURE E REFERENCES	E-1
ENCLOSURE GL GLOSSARY	
Abbreviations and Acronyms	GL-1
Definitions	GL-5

(INTENTIONALLY BLANK)

ENCLOSURE A
RESPONSIBILITIES

1. The Joint Staff J8, Deputy Director, Command, Control, Communications, and Computers (DDC4):

a. Assistant Deputy Director (ADD), Command and Control (C2) Integration will:

(1) Review ICDs, DCRs, CDDs, CPDs, CONOPS, and ISPs for C2 interoperability, integration, and sustainability, and provide recommendations and comments.

(2) Maintain JCSFL for use in reference and solution architectures required for JCIDS documents and ISPs. Maintenance and updates will be done in coordination with Services and capability developers. The JCSFL provides a common lexicon of warfighter system functionality. This information can be accessed on Intelink (NIPRNET: <https://www.intelink.gov/wiki/JCSFL>; SIPRNET: http://www.intelink.sgov.gov/wiki/Joint-Common_Systems_Function_List_1) (reference k).

(3) Direct Joint Mission Thread Architecture & Test Working Group JMT development activities and provide recommendations to develop selected JMTs to support the Joint Staff J-8's objectives. JMTs provide decomposition of the mission elements necessary to support expeditious and efficient joint force mission and capability analysis.

(4) Conduct C2 interoperability assessments on selected IT. These assessments do not replace the joint interoperability test certification; however, Joint Interoperability Test Command (JITC) may elect to use J-8 DDC4 assessment results to issue the joint interoperability test certification.

(5) Maintain the Command and Control On-the-Move (C2OTM) Reference Architecture to inform Service Sponsors and Program Managers Capability Developers that are developing C2OTM capabilities for commanders at the operational and tactical level. C2OTM Reference Architecture can be accessed on Intelink (SIPRNET: [http://www.intelink.sgov.gov/wiki/\(C2OTM\)](http://www.intelink.sgov.gov/wiki/(C2OTM))).

(6) Manage, verify, and track exposure of authoritative data sources supporting net-enabled warfighter capabilities leveraging NR KPP documentation. Report the authoritative data source exposure progress to the JROC and DoD CIO.

(7) Review and analyze NR KPP architectures, KPPs, key system attributes, and capabilities for interoperability and integration and provide a certification recommendation.

(8) Manage, verify, and track exposure of C2 and non-C2 system bit-level data implementation using the Interoperability Enhancement Process supporting net-enabled warfighter capabilities leveraging NR KPP documentation. Report the bit level implementation progress, as annotated in the DOD IEA DIV-3, to the Functional Capabilities Board (FCB).

b. ADD, C4/Cyber will:

(1) Review all JCIDS and BCL documents in KM/DS and ISPs in the DOD CIO repository for the NR KPP certification requirements according to Enclosures B and C, and references a through d. This includes:

(a) Reviewing ICDs, DCRs, CONOPs, Statements of Capability, and BCL documents to validate current DODAF architecture data or the optional NR KPP Architecture Data Assessment Template and spectrum requirements via KM/DS.

(b) Confirming, through current DODAF architecture data or the optional NR KPP Architecture Data Assessment Template, whether IT has joint interfaces or joint information exchanges and requires NR KPP certification.

(c) Providing an NR KPP certification memo for CDDs, CPDs, after certifying the NR KPP.

(d) Determining whether IT portfolio management recommendations and network operations (NetOps) for the GIG direction (reference j) and GIG 2.0 goals and characteristics (reference h) were reviewed and included.

(2) If applicable, for all IT/NSS, staff JCIDS documents, BCL documents, and IC documents to the C/S/As for NR KPP certification determination. Provide comments and where applicable, provide the NR KPP certification memo to KM/DS (according to references c and d).

(3) Provide the Joint Staff NR KPP ISP review to DOD CIO for ACAT I, Office of the Secretary of Defense (OSD) Special Interest, and DOD CIO special interest programs according to references b and f for their final acceptance or rejection.

(4) When required, attend JCB and JROC meetings to provide Joint Staff NR KPP certification results.

(5) Coordinate NR KPP policies, procedures, and programs with C/S/As.

(6) Maintain the CJCSI 6212 Resource Page (reference n).

(7) Maintain the NR KPP Manual Wiki page (reference gg).

c. ADD, Communications and Networks (CN) will:

(1) Review selected JCIDS and BCL documents, and ISP architecture artifacts, for compliance and integration with DOD enterprise level architectures, reference architectures, and IT and NSS standards.

(2) Review JCIDS, BCL, and ISP documents and architecture for compliance to the spectrum requirements in Enclosure D of the NR KPP Manual.

2. DOD Components will:

a. Review and provide comments on JCIDS and IC documents via KM/DS during the NR KPP certification process. Review and provide NR KPP related comments on BCL documents provided via KM/DS.

b. Ensure NR KPP activities required by this policy are implemented within DOD Component interoperability strategies, policies, processes, and procedures.

c. Ensure the Component Developmental Test and Evaluation (DT&E), Operational Test and Evaluation (OT&E) processes include mission-oriented NR KPP assessments as discussed in Enclosure C. Ensure the assessment uses common outcome-based methodologies to report on the impact that NR KPP and information exchanges have on system effectiveness and mission accomplishment (reference e and u).

d. Ensure IT solution architectures comply with the current DODAF (reference g), the DOD IEA (reference m), the DISR (reference p), and the JIE ORA/WEA. Ensure solution architectures are aligned to available JMTs and the JCSFL, and are resourced, developed, managed, discoverable, searchable, and retrievable (references q through y).

e. Ensure Authoritative Data Sources (ADS) are registered in the Department's Enterprise ADS Registry.

4. Sponsors (reference c) will:

a. Include NR KPP certification requirements in JCIDS and for DBS Business Case (references b and d). Ensure the requirements provide validated, verifiable, performance measures and metrics.

b. Include NR KPP requirements with coalition, intergovernmental, and non-government systems in JCIDS documents when the IT must interoperate in those environments.

c. Include requirements to comply with spectrum management policy (references x through aa) and DOD IT standards policy (reference b) in JCIDS documents.

d. Ensure solution architectures align with the current DODAF (reference g), are aligned to JMTs and the JCSFL, and are resourced, developed, managed, discoverable, searchable, and retrievable (references w through y). Ensure DOD IC Components IT solution architectures comply with the IC Joint Architecture Reference Model (reference hh).

e. Comply with the joint interoperability test certification requirement.

f. Plan, program, budget for, and develop for DODAF architecture data or the optional NR KPP Architecture Data Assessment Template.

g. Initiate process for NR KPP recertification where changes to the NR KPP objective and/or threshold values occur as a result of hardware or software updates or information exchanges are changed.

5. PMs (as defined in references e and f) will:

a. Develop and provide access to NR KPP architecture data for JCIDS/BCL documents according to table B-1. Architecture data access may be provided via a Web page link where the architecture is registered or other accessible format versus inserting actual architecture products in the documents. Align the architecture data to the current DODAF (reference g), the DOD IEA (reference m), Global Information Grid 2.0 (reference h), JIE ORA/WEA, and the DISR (reference p).

b. Ensure IT is NR KPP certified according to Enclosures C and D. This includes ensuring IT provides:

- (1) The NR KPP.

(2) DODAF-compliant NR KPP architecture data or the optional NR KPP Architecture Data Assessment Template which provides the foundation for NR KPP development (Enclosures C and D).

(3) Compliance to spectrum requirements (references t through aa).

c. Plan, program, budget, execute, and provide resources according to agreed-to schedules. Ensure funding is planned for:

(1) NR KPP certification, to include NR KPP architectures data or the optional NR KPP Architecture Data Assessment Template data.

(2) NR KPP re-certification.

(3) Spectrum requirements risk assessments, required certification processes, and control of electromagnetic environmental effects (E3).

d. Populate a DISR generated Standards View (StdV)-1(Technical View (TV)-1), using the information developed from the integrated architectures (Systems View (SV)-2, SV-6 and StdV-1(TV-1)) (Enclosures C and D).

e. Provide the program's non-technical portion of the StdV-1 and StdV-2 with the NR KPP architecture data or the optional NR KPP Architecture Data Assessment Template.

f. Develop, publish, and maintain ICAs using the ICA template available on the NR KPP Manual page (reference n).

g. Register and maintain approved DODAF architecture data (reference g) or the optional filled out NR KPP architecture data assessment template in a federated repository. When architecture data resides in a military Service, agency, or Combatant Command repository, ensure architectures are aligned to JMTs (when available) and the JCSFL, and are resourced, developed, managed, discoverable, searchable, and retrievable (reference q through y). Include the Web page link where the architecture is registered in the JCIDS/BCL Business Case documents.

h. Ensure an All View (AV)-1 is registered and exposed to public users in the DOD Architecture Registry System (reference ee) to enable its discovery.

i. Use IT mission-thread analysis to enable operational capabilities in coalition environment by identifying all potential system interfaces.

j. Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information

21 March 2012

technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in reference 1.

6. Combatant Commands, in addition to Component responsibilities above, will:

a. Prioritize interoperability requirements using approved attributes, (references d and m) to support capability-focused joint assessment, design, development, and testing.

b. Identify and submit significant joint interoperability deficiencies observed during operational exercises or real world operations as integrated priority list inputs during the capability gap assessment process (reference bb).

c. USSOCOM, in addition to component responsibilities above, will:

(1) Establish NR KPP criteria for Special Operations Peculiar (SO-P) IT. According to reference ff, USSOCOM approves all SO-P capability documents below a JROC interest JPD. USSOCOM accomplishes NR KPP certifications according to this publication and established standards. The standards will be used for interoperability testing for programs under their Title 10 authority.

(2) Review programs that facilitate global operations against terrorist networks.

d. USSTRATCOM, in addition to the responsibilities above, will:

(1) Review programs supporting global strike, missile defense, intelligence, surveillance and reconnaissance, information operations, and space operations.

(2) Ensure United States Cyber Command will assist DISA and the National Geospatial Intelligence Agency (NGA) in reviewing and defining IA standards.

7. DISA will:

a. Comply with sponsor, PM, and DOD Component responsibilities.

b. Ensure JITC leverages previous, planned and executed DT&E and OT&E tests and results to support joint interoperability test certification and eliminate test duplication (reference cc). DASD(DT&E) shall approve Developmental Test and Evaluation plans in support of Joint Interoperability Test Certification as documented in the TEMP. JITC shall advise DASD (DT&E)

regarding the adequacy of test planning in support of Joint Interoperability Test Certification.

8. Director, NGA, will, in coordination with JITC, the RTO, the OTAs, and the appropriate intelligence functional manager(s), develop interoperability test and evaluation criteria, measures, and requirements related to GEOINT. The criteria, measures, and requirements shall identify the expected cyber threat environment and be included in acquisition documents, TES, TEMP, and other test plan submissions. Prior to a fielding decision for all new or modified IT (regardless of the JPD), the military Services, Defense Agencies, Combatant Commands, and participating test unit coordinators will ensure those systems or net-centric capabilities undergo and successfully complete joint interoperability test and evaluation according to these criteria. This includes any limited or prototype fielding.

9. Director, NSA/Chief, Central Security Service, will:

a. As the Community Functional Lead for Cryptology, coordinate matters involving Interoperability and Supportability of Cryptologic Systems and U.S. Signals Intelligence Directives (USSIDs) across DoD Components.

b. Serve as the DoD Lead for approving and enforcing tactical Signals Intelligence (SIGINT) architectures and standards, which are coordinated with DoD Components, the U.S. Special Operations Command, and the Intelligence Community CIO; as the basis for Cryptologic System interoperability.

c. Provide architectural standards compliance and interoperability assessments to assist Milestone Decision Authorities in Cryptologic System production decisions.

d. Develop policy and procedures so that IA information for interoperable IT/NSS is releasable to joint, combined, and coalition forces and U.S. Government Departments and Agencies.

e. Ensure that interoperable and supportable IA products are available for IT/NSS.

f. In cooperation with the DISA, identify, evaluate, and select appropriate IA standards which support interoperability of IT/NSS, to be included in the DoD IT Standards Registry.

g. Ensure that technical, procedural, and operational interfaces are specified and configuration managed in coordination with other DoD components, so that DoD, non-DoD, and coalition cryptologic/cryptographic systems can interoperate with DoD IT and NSS.

21 March 2012

h. In coordination with JITC, the RTO, the OTAs, and the appropriate intelligence functional manager(s), develop interoperability test and evaluation criteria, measures, and requirements related to cyber security. The criteria, measures, and requirements should be developed and maintained to identify the expected cyber threat environment with the further expectation that they will be included in acquisition documents, TES, TEMP, and other test plan submissions for IT/NSS which are DoD ACAT II or above.

ENCLOSURE B

PROCESS OVERVIEW AND STAFFING PROCEDURES

1. Overview. This enclosure provides an NR KPP certification process overview within the DOD IT life cycle. NR KPP assessments are conducted throughout the IT life cycle to identify and resolve potential interoperability and/or emerging net-centricity challenges and mitigate the risk of delivering non-interoperable capabilities to the Warfighter.
2. Types of NR KPP Certifications. NR KPP certification is provided via a Joint Staff J-8 signed memo. The four NR KPP certifications are:
 - a. Certified. Certified IT has completed all NR KPP requirements and/or stages and all comments were successfully adjudicated.
 - b. Not Certified. Not certified IT has completed all NR KPP requirements and/or the stages, but has unresolved critical comments that deny certification.
 - c. Not Applicable. After the JCIDS documents are reviewed it is determined by the Joint Staff the NR KPP does not apply because it lacks joint interface or doesn't exchange joint information.
 - d. Not Required. JCIDS documents are reviewed it is determined a NR KPP certification is not required for this stage or type of document by regulation or guidance (reference d).
3. Process Relationships. Figure B-1 depicts the DOD acquisition, JCIDS, NR KPP certification, and spectrum requirement compliance process relationships.

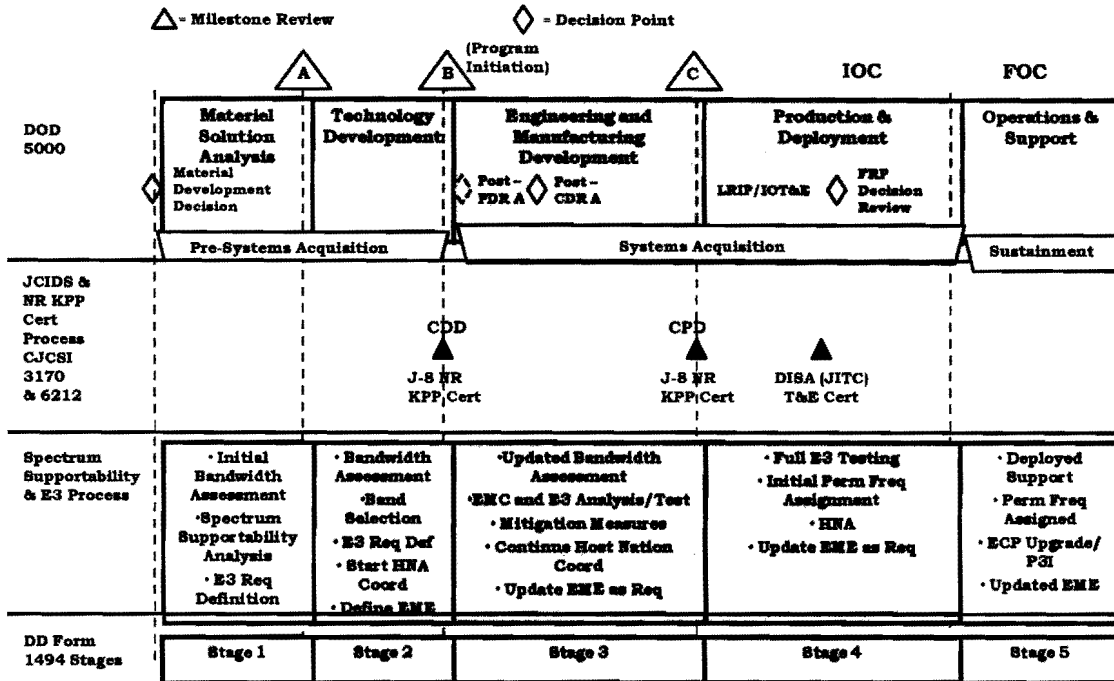


Figure B-1. DOD Acquisition, JCIDS, NR KPP Certification Relationship Overview

3. NR KPP Certification Process. The Joint Staff reviews and grants NR KPP certification (via a certification memo) on sponsor approved JCIDS documents. The Joint Staff certifies the NR KPP, using the DODAF architecture data or the optional NR KPP Architecture Data Assessment Template, and spectrum requirements compliance. The Joint Staff reviews and comments on the ISP NR KPP, DODAF architecture data, or the optional NR KPP Architecture Data Assessment Template, and spectrum requirements compliance. The architecture data identified in table B-1 is required to support the various JCIDS documents for systems that have joint interfaces or joint information exchanges. BCL documents comply with the BEA.

a. Pre-DOD Acquisition System MS A Documents. Prior to MS A, ICDs, DCRs, and CONOPS are reviewed to determine which JCA, JMT, associated mission areas, and Universal Joint Task List (UJTL) are identified; to determine if interoperability with other developing capabilities is considered; to determine if GIG 2.0 goals and characteristics and NetOps for the GIG direction (references j and l) are addressed, and to ensure spectrum requirements are identified (references x through aa).

Document/ Architecture	AV-1	AV-2	CV-1	CV-2	CV-3	CV-4	CV-5	CV-6	DIV-1	DIV-2 (OV-7)	DIV-3 (SV-11)	OV-1	OV-2	OV-3	OV-4	OV-5a	OV-5b	OV-6a	OV-6c	PV-2	SV-1 or SvcV-1	SV-2 or SvcV-2	SV-4 or SvcV-4	SV-5a or SvcV-5	SV-6 or SvcV-6	SV-7 or SvcV-7b	SvcV-10a	SvcV-10b	SvcV-10c	StdV-1 (TV-1)	StdV-2 (TV-2)		
DCR	R ¹		R	R	R	R						R																					
CONOPS	R ¹		R	R	R	R		R				R	R		R	R										R							
ICD	X ¹	X	R	R	R	R		R				X	X		X	X	O									R							
CDD	X ¹	X	X	X	X	X	X	X		X		X	X	X	X	X	X		X	X	X	X	X	X	X	X					X ²	X ²	
CPD	X ¹	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X					X ²	X ²	
IC ^{3,4}	X	X	X	X			X		X	X		X	X	X		X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	X
Legend	X - Required O - Optional R - Recommended, PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs. (e.g., HQDA requires the SV-10c, USMC requires the SV-3, IC requires the SvcV-10a and SvcV-8)																																
Note 1	The AV-1 must be registered, must be "public" and "released" at the lowest classification level possible in DARS for compliance.																																
Note 2	The technical portion of the StdV-1 and StdV-2 are built using GTG-F DISR standards profiling resources and, within six months of submitting JCIDS documentation, must be current and published for compliance. Use of non-mandated DISR standards in the StdV-1 must be approved by the PM or other duly designated Component representative official and documented by a waiver notification provided to the DoD CIO."																																
Note 3	Intelligence Community (IC) requirements IAW the IC Enterprise Architecture Program Architecture Guide and development phase which clarifies the IC Policy Guidance 801.1 Acquisition.																																
Note 4	Service Views (SvcV) only																																
Note 5	<ol style="list-style-type: none"> The Sponsor⁴ and the Program are jointly responsible for the AV-1, AV-2, CV-1, CV-2, CV-3, CV-4, CV-5, CV6, SV-6 or SvcV-7. The Sponsor⁴ is responsible for the development of the architecture data for the OV-1, OV-2, OV-4, OV-5a, OV6c, DIV-2, and the SV-6 or SvcV-6. The Program is responsible for the development of the architecture data for the DIV-1, DIV-3, OV-3, OV-5b, OV-6a, PV-2, SV-1 or SvcV-1, SV-2 or SvcV-2, SV-4 or SvcV-4, SV-5a or SvcV-5, SvcV-10a, SvcV-10b, SvcV-10c, StdV-1, and StdV-2. ⁴ Operational user (or representative). 																																
Note 6	The NR-KPP Measures data is captured in the SV-7 or the SvcV-7.																																

Table B-1. Required Architecture Data by Document

CJCSI 6212.01F
21 March 2012

B-4

Enclosure B

b. Post-DOD Acquisition System MS A Documents

(1) CDDs and CPDs are reviewed and the NR KPP certified via KM/DS, using DODAF architecture data or the optional NR KPP Architecture Data Assessment Template and spectrum requirement compliance to support NR KPP certification by the JROC. The post MS-A document certification evaluates compliance with NR KPP attributes, GIG 2.0 goals and characteristics, IT portfolio management recommendations, and alignment to the current DODAF. Certification occurs prior to acquisition MS B and C and when capability changes result in updates to the NR KPP. Architecture data is provided via Web page link where the architecture is registered or repository access versus incorporating the architecture products in the document.

(2) NR KPP certification also applies to IT approved by the JROC to use the modified JCIDS process (referred to as IT box in reference d).

(3) The NR KPP within the ISP is reviewed by the Joint Staff.

c. BCL Document Reviews and NR KPP Certification. BCL documents are reviewed to determine if JROC interest exists (reference d and f) and to provide comments. If joint interest exists, the documents are evaluated using the most current BEA and assessed to ensure the planned acquisition is consistent with GIG policies, including spectrum compliance. Finally, the IT Acquisition Program Baseline NR KPP (reference e) is evaluated for NR KPP certification and BEA.

4. NR KPP Staffing

a. JCIDS Document Review and Certification. Pre-MS A JCIDS document reviews CDD and CPD certification of the NR KPP, using the DODAF architecture data or the optional NR KPP Architecture Data Assessment Template, and spectrum compliance is accomplished in concert with the three JCIDS phases (reference d). Interoperability issues may be identified by DOD Component via KM/DS.

5. C4/CYBER FCB Adjudication. Unresolved NR KPP, DODAF architecture data or the optional NR KPP Architecture Data Assessment Template, and spectrum compliance issues are forwarded to the C4/CYBER FCB or Military Intelligence Board (MIB) for resolution and their decisions provided to the lead DOD Component to complete the JROC approval process. The C4/CYBER FCB and MIB ensure unresolved issues are presented to the JROC for resolution via the appropriate FCB. Unresolved issues will prevent JCIDS document NR KPP certification.

6. Review Timelines. The current version of CJCSI 3170 contains the JCIDS document review timelines (reference d).

7. Failure to Meet NR KPP Certification Requirements. Failure to meet or maintain NR KPP certification or joint interoperability test certification may result in:

a. No JROC validation of the program CDD, CPD, or DOD CIO approval of the ISP.

b. Recommending the IT not proceed to the next MS (if currently in the DOD 5000 acquisition process).

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

d. Withholding NR KPP certification and recommend revoking any existing Interim Certificate to Operate (ICTO) until the issue is corrected.

8. Recommendations. Failed NR KPP certification recommendations are provided to USD(AT&L); USD(P); USD(C); USD(I); Director, CAPE; DOD CIO; DOD EA for Space; and the JROC.

9. Uniform Resource Locators (URL). URLs for NR KPP internet resources and NR KPP Manual are located on the CJCSI 6212 Resource Page (reference n). This page will be kept up-to-date as Web sites change. Contact the Joint Staff lead if unable to access the resource page

ENCLOSURE C

NR KPP DEVELOPMENT AND NR KPP CERTIFICATION PROCEDURES

1. NR KPP Overview. All IT will follow the NR KPP development process. Net-ready attributes determine specific measurable and testable criteria for interoperability, and operationally effective end-to-end information exchanges. The NR KPP identifies operational, net-centric requirements with threshold and objective values that determine its measure of effectiveness (MOE) and measure of performance (MOP). The NR KPP covers all communication, computing, and electromagnetic spectrum requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service exchanges. These exchanges enable successful completion of the Warfighter mission or joint business processes. The NR KPP identified in the CDD or CPD will also be used in the ISP to identify support required from external IT. The NR KPP is a mandatory KPP for all program increments. The NR KPP includes three attributes and the MOP/MOE that is derived through a three-step process of mission analysis, information analysis, and systems engineering. MOP/MOE are validated in solution architecture data developed according to the current DODAF or the optional NR KPP Architecture Data Assessment Template. The attributes depict how planned or operational IT:

- a. Attribute 1. Supports military operations,
- b. Attribute 2. Is entered and managed on the network, and
- c. Attribute 3. Effectively exchanges information.

2. Attribute Characteristics. A general attribute description is below followed by detailed steps to develop each attribute. Enclosure D provides detailed direction to develop solution architectures for each attribute.

- a. Support Military Operations. This attribute specifies which military operations (e.g., missions or mission threads) a system supports. MOEs are used to measure mission success and are specific to the conditions under which a mission will be executed. The MOEs are the basis of the NR KPP threshold and objective measures. This attribute should also specify which operational tasks the IT supports; the MOPs are used to measure task performance and the conditions under which the tasks are performed. Since the NR KPP focuses on exchanging information, products, or services with external IT, these tasks should only be net-centric operational tasks. Operational tasks are net-centric if they produce information, products, or

services for or consume information, products, or services from external IT (including storing information on external IT).

b. Entered and Be Managed On the Network. This attribute specifies which networks the IT must connect to in order to support its net-centric military operations. The attribute must also specify performance requirements for these connections. To determine these performance requirements, answer the following questions in the context of the missions and tasks supported:

(1) What types of networks will the IT connect to (this is more than internet protocol (IP) networks)?

(2) What MOPs do the required networks use to measure network entrance and management performance? This includes MOPs to measure the time from system start up to when the system is connected to the network and is supporting military operations.

(3) Who manages the system as it connects to various networks?

(4) How is system managed? Will management be distributed, centralized, local, or remote?

(5) What configuration parameters does the network have?

c. Effective Information Exchanges. This attribute specifies the information elements produced and consumed by each mission and net-ready operational task identified above. Since the NR KPP focuses on a system's interactions with external systems, information elements the IT produces, sends, or makes available to an external system and information elements the IT receives from an external system are identified. For each information element, MOPs are used to measure the information element's production or consumption effectiveness. NR KPP MOPs should describe how the information elements will support unanticipated uses as described by the DOD Data and Services Strategy criteria of visible, accessible, usable, trusted, and interoperable.

d. Summary Table. Table C-1 summarizes the NR KPP attributes and their associated metrics in terms of a standardized framework and data sources to leverage when developing attributes and their threshold and objective values.

NR KPP Development Step	NR KPP Attribute	Attribute Details	Measures	Sample Data Sources	NR KPP MOE/MOP
Mission Analysis	Support to Military Operations Support to Military Operations	Military Operation (e.g., mission areas or mission threads)	MOEs used to determine the success of the military operation	JMETL, JMT, UJTL, and METL	MOE
			Conditions under which the military operations must be executed		
		Operational tasks required by the military operations	MOPs used to determine activity performance	JMETL, JMT, UJTL, and METL	MOP
			Conditions under which the activity must be performed		
Information Analysis	Entered and managed on the network	Which networks do the net-centric military operations require	MOP for entering the network	N/A	MOP
			MOP for management in the network	N/A	MOP
	Effectively exchanges information	Information produced and consumed by each military operation and operational task	MOP to ensure information exchanges are: Continuous Survivable Interoperable Secure Operationally Effective	DODAF OV-3, Operational Resource Flow Matrix	MOP
Systems Engineering and Architecture	Supports all 3 attributes	Ensures that IT satisfies the attribute requirements	Provides traceability from the IT MOPs to the derived operational requirements	OVs and SVs	N/A

Table C-1. NR KPP Development

3. NR KPP Functions. The NR KPP is used to:

a. Requirements. Evaluate interoperability and net-centric requirements for the system.

b. Information Exchanges. Verify IT supports operationally effective producer to consumer information exchanges according to the sponsor's validated capability requirements and applicable reference models and reference architectures (reference b).

c. MOEs and MOPs. Provide MOEs and MOPs to evaluate IT's ability to meet the threshold and objective or initial minimum values when testing the system for joint interoperability certification.

d. Interoperability Issues. Analyze and identify potential interoperability issues early in the IT's life cycle and identify joint interfaces or joint information exchanges through systems engineering and architecture development. IT architecture in JCIDS documents is developed according to current. In addition, the architecture must align with JMTs (as available), JCSFL, DOD IEA (reference m), JIE ORA/WEA, and Data Services Environment (DSE) to identify potential interoperability disconnects with interdependent systems or services as well as detailed information exchange and information sharing strategies.

e. Compliance. Determine whether IT complies with netops for the GIG direction (reference l), GIG 2.0 goals and characteristics (reference h), and is integrated into system development.

f. Spectrum Requirements. Ensure compliance with joint, DOD, national, and international spectrum utilization requirements, E3, information bandwidth requirements, bandwidth analysis (references x through aa), tactical data links (reference y), selective availability anti-spoofing module (references ee and ff), and the joint tactical radio system (references gg and hh).

4. NR KPP Development. All IT requires a NR KPP that specifies measurable and testable interoperability requirements. Interoperability requirements include both the technical information exchanges and the operational effectiveness of those exchanges. NR KPP development uses a three-step question/answer process to develop threshold and objective values and initial minimum values.

5. The Net Ready Key Performance Parameter (NR KPP) Manual Wiki page is located here: [https://www.intelink.gov/wiki/Net_Ready_Key_Performance_Parameter_\(NR_KPP\)_Manual](https://www.intelink.gov/wiki/Net_Ready_Key_Performance_Parameter_(NR_KPP)_Manual).

6. NR KPP Example. Table C-2 is an example of completed NR KPP using notional values.

NR-KPP Attribute	Key Performance Parameter	Threshold	Objective
Support net-centric military operations	Mission: Tracking and locating (Finding, Fixing, Finishing) High-Value Target (HVT) --Measure: Dissemination of acquisition data for HVT --Conditions: C 2.3.1.6 Communications Connectivity	--10 minutes --Continuous	--Near-Real-Time --Continuous
	Mission Activities: Find HVT --Measure: Location accuracy --Conditions: C 2.4.6 Certitude of Data	--100 Meter circle --High	--25 Meter circle --Absolute
Enter and be managed in the network	Network: SIPRNET --Measure: Time to connect to an operational network from power up --Conditions: C 2.3.1.6 Communications Connectivity	--2 minutes --Continuous	--1 minute --Continuous
	Network: NIPRNET --Measure: Time to connect to an operational network from power up --Conditions: C 2.3.1.6 Communications Connectivity	--2 minutes --Continuous	--1 minute --Continuous
Exchange information	Information Element: Target Data --Measure: Dissemination of HVT biographic and physical data	--10 seconds	--5 seconds
	--Measure: Latency of HVT biographic and physical data	--5 seconds	--2 seconds
	--Conditions: C 1.3.5 RF Spectrum	--Unrestricted	--Unrestricted

Table C-2. NR KPP Example

7. Spectrum Requirements Compliance. To obtain an I&S NR KPP certification, all spectrum dependent devices must comply and be developed with the spectrum management and electromagnetic environment effects (E3) direction in references a, e, t, u, and hh. The assessment of equipment or systems needing spectrum is the receipt of equipment spectrum certification, availability of frequencies for operation, and consideration of EMC. The spectrum process includes joint, DoD, national, and international policies and

procedures for the management and use of the electromagnetic spectrum. The spectrum process is detailed in Enclosure D and on the NR KPP Manual Wiki page. The Supportability Requirements Compliance is located on the NR KPP Manual Wiki page.

ENCLOSURE D

NR KPP ARCHITECTURE DEVELOPMENT METHODOLOGY

1. NR KPP Architecture Development Methodology. Architecture development enables development of the NR KPP. Architecture-based solutions, developed through a strict verification and validation process, are fundamental for improved interoperability, better information sharing, stricter compliance, and leaner processes. They also feed into system engineering processes and ultimately result in reduced costs and more effective mission accomplishment. The DODAF (reference g) describes the 6-step architecture development process for DOD (figure D-1). The 6-step architecture development process supports the 3 step of NR KPP development process in Enclosure C. Solution architectures, conforming to the current DODAF, are developed, registered, and used as tools to improve joint operational processes, infrastructure, and solutions and to promote common vocabulary, reuse, and integration. Additionally, architecture development enables compliance with the NR KPP certification requirements. Figure D-2 displays the NR KPP development steps in relation to the JCIDS and acquisition processes.

a. Background. With the release of DODAF version 2.0, the architecture focus switched from "products" to "data". Similarly, the NR KPP certification process changes NR KPP architecture development from an architecture product process to a data focus to enable analysis among programs, systems, and services. Architectures for NR KPP certification will be developed using the most current DODAF version or the optional NR KPP Architecture Data Assessment Template. NR KPP Architecture Data Assessment Template instructions are on the CJCSI 6212 Resource Page (reference n).

b. DODAF Use. Develop architectures for NR KPP certification using the most current DODAF version. Existing architectures will be updated to the most current DODAF version before the next JCIDS document is submitted. Data sharing and data interoperability are enabled through architectures. Table B-1 above depicts required architecture data by JCIDS documents.

c. Architecture Tools. Produce architectures using a tool that creates data. Use of commercially available architecture tools is encouraged.

d. Submitting Architectures. Include the web link to the required architecture data, wherein the data formats will support staffing, analysis, distribution, and reuse. Architecture data should be submitted in formats that can be viewed without specialized or proprietary tools and must be legible for reviewers. Until DM2 PES compliant tools are available with architecture data exchange standards, submit required architecture data, from table B-1, using

Microsoft products or the optional the NR KPP architecture data assessment template. Whether using Microsoft products or the optional NR-KPP Architecture Data Assessment Template to submit the architecture data, the required data is specified on the CJCSI 6212 Manual Page (reference gg). When DM2 PES compliant commercial architecture tools are available, they will be used to develop and submit architectures for NR KPP certification.

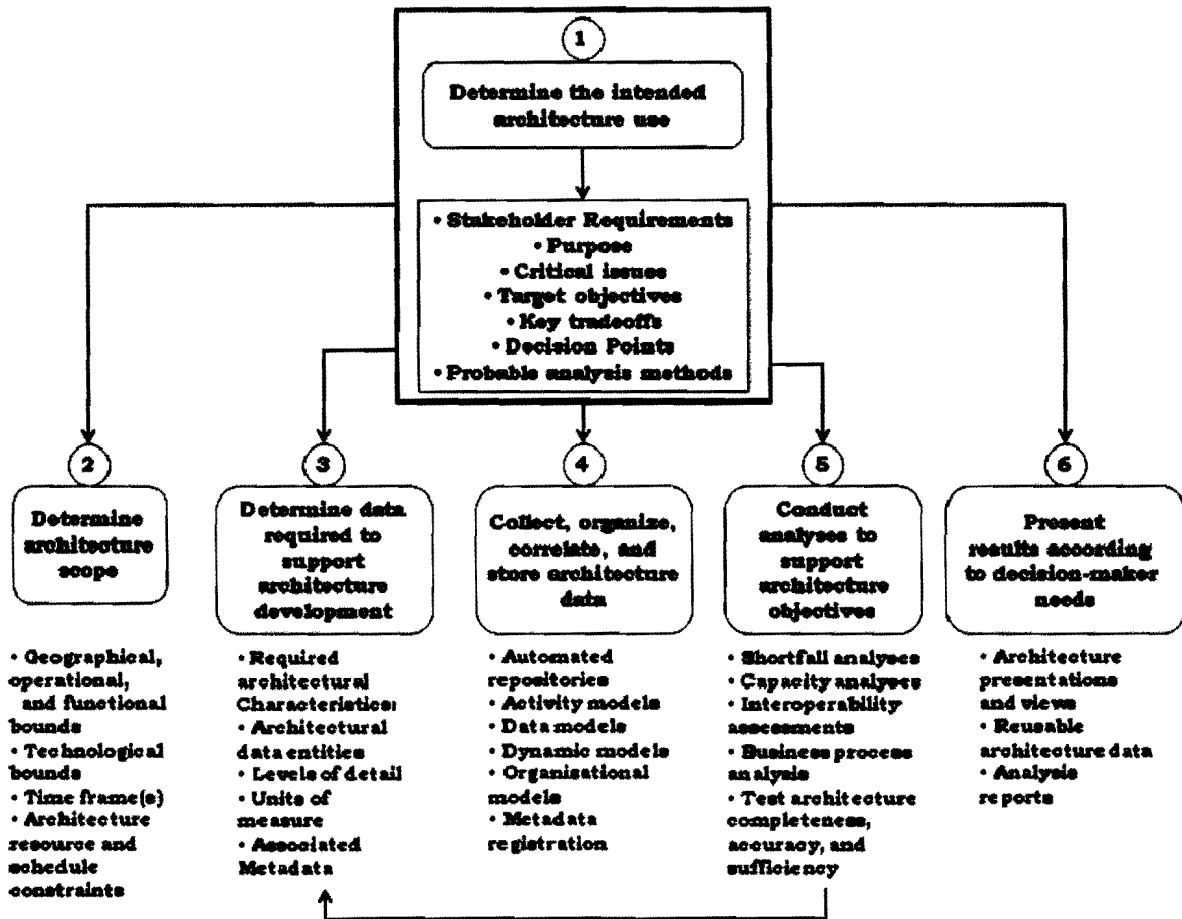


Figure D-1. DOD 6-Step Architecture Development Process

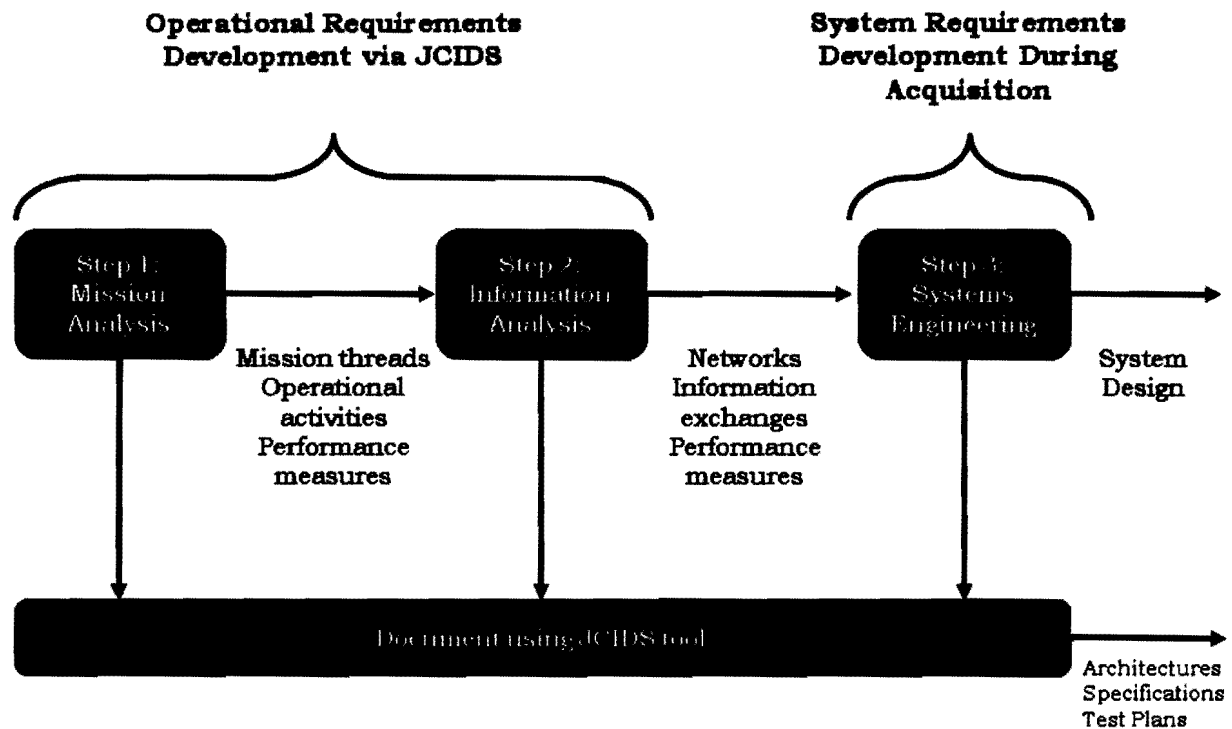


Figure D-2. NR KPP Development Applied to the JCIDS and Acquisition Processes

2. DOD IEA Alignment. The DOD IEA provides a common taxonomy and lexicon to describe required communications capabilities and align solution architecture with the GIG as required by reference x. The DOD IEA provides the DOD-wide context and rules for IT solution architectures. Alignment with the DOD IEA and other relevant architectures provides context for solution architectures.

a. Architecture Alignment. Align solution architectures to the laws, regulations, and policies identified in the DOD IEA (reference m) and according to the compliance criteria in the DOD IEA. Show linkage to parent enterprise architectures, and fit within Component and DOD architecture descriptions, using appropriate reference model and reference architectures (DOD IEA, JIE ORA/WEA, and IT infrastructure ORA).

b. Activity Models. For aligning with DOD IEA, within the activity model, address activities and information inputs/outputs. This activity model will be built in compliance with the DOD IEA. Use DOD IEA activity names and descriptions to the maximum extent possible. An alternative method of compliance permits the use of system unique communications activities in the OV-5b, but requires a cross-walk table to the DOD IEA activities where a relationship exists and is included in the ISP.

21 March 2012

c. NR KPP Information and Architecture Views. The NR KPP architectural developmental process and template is located on the Net Ready Key Performance Parameter (NR KPP) Manual Wiki page located here: [https://www.intelink.gov/wiki/Net_Ready_Key_Performance_Parameter_\(NR_KPP\)_Manual](https://www.intelink.gov/wiki/Net_Ready_Key_Performance_Parameter_(NR_KPP)_Manual).

ENCLOSURE E

REFERENCES

- a. DOD Directive 4630.05, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- b. DOD Instruction 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"
- c. CJCSI 3170.01 Series, "Joint Capabilities Integration and Development System"
- d. Manual for the Operation of the Joint Capabilities Integration and Development System, see https://www.intelink.gov/wiki/JCIDS_Manual to access the JCIDS Manual
- e. DOD Instruction 5000.02, 8 December 2008, "Operation of the Defense Acquisition System"
- f. DTM 11-009 (Acquisition Policy for Defense Business Systems).
- g. DOD Architecture Framework (DODAF), Version 2.0, see <http://dodcio.defense.gov/sites/dodaf20/>
- h. JROCM 095-09, "Global Information Grid 2.0 Initial Capabilities Document"
- i. DOD Directive 8000.01, 10 February 2010, "Management of the Department of Defense Information Enterprise"
- j. DOD Instruction 8410.02, 19 December 2008, "NETOPS for the Global Information Grid"
- k. Joint Common System Function List, Defense Knowledge Online see <https://www.us.army.mil/suite/page/419489>
- l. DOD Instruction 8510.01, 28 November 2007, "DOD Information Assurance Certification and Accreditation Process (DIACAP)"
- m. Defense Information Enterprise Architecture 1.2 (DOD IEA 1.2), May 2010, see <http://dodcio.defense.gov/sites/diea/>

- n. CJCSI 6212 Resource Page, see https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page
- o. DOD Acquisition Guidebook see <https://dag.dau.mil/Pages/Default.aspx>
- p. Department of Defense Information Technology Standards Registry (DISR) see NIPRNET at [https:// DISRonline.disa.mil/](https://DISRonline.disa.mil/) and on the SIPRNET at <http://DISRonline.disa.smil.mil>
- q. DOD Directive 8320.02, 23 April 2007, "Data Sharing in a Net-Centric Department of Defense"
- r. DOD CIO Memorandum, 9 May 2003, "DOD Net-Centric Data Strategy"
- s. DOD Chief Information Officer, 4 May 2007, "DOD Net-Centric Services Strategy,"
- t. DOD Directive 3222.3, 8 September 2004, "DOD Electromagnetic Environmental Effects (E3) Program"
- u. DODI 4650.01, January 9, 2009, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum,"
- v. DOD 4650.1-R1, 26, April 2005, "Link 16 Electromagnetic Compatibility (EMC) Features Certification Process and Requirements"
- w. DOD Instruction 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"
- x. CJCSI 6215.01 Series, "Policy for Department of Defense (DOD) Voice Networks with Real Time Services"
- y. Chairman of the Joint Chiefs of Staff, Director for Force Structure, Resources, and Assessments (J8) memorandum, 6 June 2011, "Capability Development Tracking and Management (CDTM) Implementation Plan"
- z. JIE ORA/WEA at https://www.intelink.gov/wiki/Joint_Information_Environment
- aa. DOD Directive 5000.01, November 20, 2007, "The Defense Acquisition System"
- bb. DOD 7000.14-R, Volume 2B, Chapter 18, July 2010, "DOD Financial Management Regulation: Information Technology"

- cc. DOD Instruction 8100.04, 09 December 2010, "DoD Unified Capabilities (UC)"
- dd. Secretary of Defense DTM 11-006, June 14, 2011, "Establishment of the Senior Integration Group (SIG) for the Resolution of Joint Urgent Operational Needs (JUONs)"
- ee. DOD CIO DTM 09-013, Change 2, March 10, 2011, "Registration of Architecture Descriptions in the DoD Architecture Registry System (DARS)"
- ff. JROCM 079-09, 2 November 2009, "Delegation of Authority for Special Operations Command"
- gg. Ready Key Performance Parameter (NR KPP) Manual Wiki located here: [https://www.intelink.gov/wiki/Net_Ready_Key_Performance_Parameter_\(NR_KPP\)_Manual](https://www.intelink.gov/wiki/Net_Ready_Key_Performance_Parameter_(NR_KPP)_Manual)
- hh. Intelligence Community Joint Architecture Reference Model, see https://www.intelink.gov/wiki/Joint_Architecture_Working_Group
- ii. DoDI O-3115.7, September 2008, Change 1 19 November 2010, "Signals Intelligence (SIGINT)."
- jj. DoDD 5000.01, May 12, 2003 (Certified Current as of November 20, 2007), "The Defense Acquisition System"

(INTENTIONALLY BLANK)

GLOSSARY

ACAT	Acquisition Category
AV	All View
BCL	Baseline Capabilities Lifecycle
C2	Command and Control
C4	Command, Control, Communications, and Computers
C/S/A	Combatant Commands, Services, Agencies
CDD	Capability Development Document
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COI	Communities of Interest
CONOPS	Concept of Operations
COTS	Commercial-Off-the-Shelf
CPD	Capabilities Production Document
CRM	Comments Resolution Matrix
DAA	Designated Approving Authority
DARS	DOD Architecture Registry System
DBS	Defense Business System
DCR	DOTMLPF Change Recommendations
DDC4	Deputy Director, Command, Control, Communications, and Computers
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISR	DOD Information Technology Standards Registry
DIV	Data and Information View
DITPR	DOD Information Technology Portfolio Repository
DM2	DODAF Meta-model
DOD	Department of Defense
DOD CIO	Department of Defense Chief Information Officer
DOD IEA	Defense Information Enterprise Architecture
DODAF	DOD Architecture Framework
DODD	Department of Defense Directive
DODI	DOD Instruction
DOT&E	Director, Operational Test and Evaluation
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
DRRS	Defense Readiness Reporting System
DRSN	Defense Red Switch Network
DT&E	Developmental Test and Evaluation

E3	Electromagnetic Environmental Effects
EA	Executive Agent
EISP	Enhanced Information Support Plan
EMC	Electromagnetic Compatibility
EME	Electromagnetic Environment
ERAM	Enterprise Risk Assessment Methodology
FCB	Functional Capabilities Board
FDD	Full Deployment Decision
FRP	Full-Rate Production
FYDP	Future Years Defense Program
GIG	Global Information Grid
GPS	Global Positioning System
GTP	GIG Technical Profile
HVT	High Value Target
IA	Information Assurance
IATO	Interim Authorization to Operate
ICA	Interface Control Agreement
ICD	Initial Capabilities Document
ICP	Interoperability Certification Panel
ICTO	Interim Certificate To Operate
IOC	Initial Operational Capability
IP	Internet Protocol
IRB	Investment Review Board
ISP	Information Support Plan
IT	Information Technology
ITP	Interoperability Test Plan
JCA	Joint Capability Area
JCB	Joint Capabilities Board
JCIDS	Joint Capabilities Integration and Development System
JCSFL	Joint Common System Function List
JIE	Joint Information Environment
JITC	Joint Interoperability Test Command
JMT	Joint Mission Threads
JMETL	Joint Mission Essential Task List
JPD	Joint Potential Designator
JROC	Joint Requirements Oversight Council
JROCM	JROC Memorandum
JUON	Joint Urgent Operational Need
JWICS	Joint World Wide Intelligence Communications System

KM/DS	Knowledge Management/Decision Support
KPP	Key Performance Parameter
MCEB	Military Communications-Electronics Board
MDA	Milestone Decision Authority
MDR	DOD Metadata Registry
METL	Mission Essential Task List
MIB	Military Intelligence Board
MILDEP	Military Department
MOA	Memorandum of Agreement
MOE	Measure of Effectiveness
MOP	Measure of Performance
MS	Milestone
NGA	National Geospatial Intelligence Agency
NetOps	Network Operations
NIPRNET	Non-secure Internet Protocol Router Network
NR KPP	Net Ready Key Performance Parameter
NSA	National Security Agency
NSS	National Security Systems
NTIA	National Telecommunications and Information Administration
OA	Operational Assessment
OPLAN	Operations Plan
ORA	Operational Reference Architecture
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review
OV	Operational View
PES	Physical Exchange Specification
PM	Program Manager
POC	Point Of Contact
RTO	Responsible Test Organization
SATCOM	Satellite Communications
SIPRNET	SECRET Internet Protocol Router Network
SMO	Spectrum Management Office
SO-P	SOCOM Peculiar
StdV	Standards View
SvcV	Services View
STP	System Tracking Program

SV	System / Service View
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TES	Test and Evaluation Strategy
TS/SCI	Top Secret/Special Compartmentalized Information
TV	Technical Standards View
UCR	Unified Capabilities Requirements
UJTL	Universal Joint Task List
URL	Uniform Resource Locator
US&P	U.S. and its Possessions
USD (AT&L)	Under Secretary of Defense (Acquisition, Technology, and Logistics)
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command
WWW	World Wide Web
XML	Extensible Markup Language

PART II - DEFINITIONS

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

All View (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.

Attributes. A quantitative or qualitative characteristic of an element or its actions. Defined in CJCSI 3170.01G.

Capability. The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) to perform a set of tasks to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a joint DOTMLPF change recommendation. In the case of materiel proposals/documents, the definition will progressively evolve to DOTMLPF performance attributes identified in the capability development document and the capability production document. Defined in CJCSI 3170.01G.

Capability Architecture. A set of descriptions that portrays the context and rules required to achieve a desired effect through a combination of doctrine, organization, training, materiel, leadership and education, personnel, and facilities. (DODAF 2.0)

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 (reference c).

Coalition interface. Any interface that passes information between one or more U.S. IT and one or more coalition partner IT.

Communities of Interest. 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 (reference q)

Capabilities Production Document. A document that addresses the production elements specific to a single increment of an acquisition program (reference c).

Defense Business System. An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management (reference f).

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.

DOD Architecture Registry System (DARS). The DOD architecture registry that provides a web based access to architecture artifact for sharing and collaboration. (reference gg).

DOD Components. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DOD Field Activities, and all other organizational entities within the Department of Defense (reference a).

DOD Enterprise. Relating to policy, guidance, or other overarching leadership provided by OSD Officials and the Chairman of the Joint Chiefs of Staff in exercising authority, direction, and control of their respective elements of the Department of Defense on behalf of the Secretary of Defense.

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 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 profile guidance 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 systems throughout the Department of Defense. The use of GTG Federation resources and GIG Technical Profiles is required to identify DISR standards and to develop and publish StdV-1/TV-'s and StdV-2/TV-2's for a program's integrated architecture/ solution architecture. The GTG Federation includes interoperability information and web-based applications and resources (Standards Profile building, registry Configuration Management and change tracking) developed to provide the necessary support for continued DISR evolution and automation of the processes that use it. .

Enhanced Information Support Plan (EISP). Use of the EISP is encouraged to facilitate the development of standard ISP 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 document. Information on the EISP tool is available on the 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; electrostatic discharge; hazards of radiation to personnel, ordnance, and volatile materiel's; and natural phenomena effects, of lightning and precipitation static (reference t).

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". (Reference u). Essential Operational Needs. Capability determined by the provided of forces or the combatant command as necessary to accomplish their assigned missions.

External IT. Any systems outside the scope of the program or Program of Record (POR) referenced in the JCIDS document, BCL document, IC document, or ISP (i.e. with information flowing into or out of the program). As an example, an external system to a DOD space system is the widely shared communications backbone or data network that a space system might interface with for communications or data services.

Fielded System. Post acquisition IT in use by operational or headquarters units (regardless of the process used to put it into operational use). Fielded systems may be modified or improved through standard DOD processes.

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. A permanently established body that is responsible for the organization, analysis, and prioritization of joint warfighting capabilities within an assigned functional area. (References c and dd).

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. (Reference i).

GIG Technical Profiles. GTPs contain:

a. General Information: GTP title, reference identification, version number, DOD IEA area, applicable JCA, JMT, associated mission areas, and Universal Joint Task List (UJTL) are JCSFL items and date.

- b. Interoperability Reference Architecture and Service Description: a description and graphic to illustrate the context where the GTP will fit within the overall
- c. GIG Reference Topology and description of the services provided by the GTP.
- d. Interoperability Requirements Description: defined in Guidance Statements necessary to fulfill Interoperability Reference Architecture, security requirements, and best practices.
- e. Technical Implementation Profile: interoperability requirements, in the form of Guidance Statements necessary for systems to correctly use the functions associated with the GTP and Standards Profile.
- f. Secured Availability: information assurance (IA) guidance for securely connecting to and/or operating within the GIG.
- g. Maturing Guidance: mid and far term program planning and implementation.
- h. Compliance Testing: describes possible test methods for compliance.

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

Initial Capabilities Document. 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. (Reference c).

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.

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

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

Information Technology (IT). Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or used by a contractor under contract with the executive agency that requires the use of -

- a. Of that equipment, or
- b. Of that equipment to a significant extent in the performance of a service or the furnishing of a product;
- c. Includes computers, ancillary equipment, software, firmware and similar procedures, services, (including support service), and related resources, but IT does not include any equipment acquired by a federal contractor incidental to a federal contract (reference f). For the purpose of this instruction IT includes, NSS, IT acquisition programs, information systems, IT initiatives, IT services, software, electronic warfare devices, DBS, qualified prototypes, Commercial-Off-the-Shelf (COTS), Government Off-the-Shelf, Rapid Acquisition, Joint Urgent Operational Needs (JUON), Special Access Program, Joint Capability Technology Demonstration, Coalition Warrior Interoperability Demonstration, Combatant Command Initiatives Fund, and non-program of record materiel solution efforts.

IT Acquisition Program. A directed, funded effort that provides a new, improved, or continuing materiel, weapon or information system, or service capability in response to an approved need. (reference cc)

IT Initiative. IT initiatives can be systems, programs, projects, organizations, activities or grouping of systems. (reference dd)

IT Services. The performance of any work related to IT and the operation of IT, including NSS. This includes outsourced IT-based business processes, outsourced IT, and outsourced information functions. (reference e)

Information System. 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, and includes computers and computer

networks, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term information technology (IT) does not include any equipment that is acquired by a federal contractor incidental to a federal contract. The term information systems is used synonymously with IT (to include National Security Systems). (reference c)

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

Increment. Whether an evolutionary, incremental, or spiral acquisition, an increment is a militarily useful, logistically supportable, and technically mature increase in operational capability that can be developed, produced, deployed, and sustained. Each increment will have its own set of threshold and objective values set by the user. Increments include block upgrades, pre-planned product improvement, and similar efforts providing an increase in operational capability.

Interoperability. The ability to operate in synergy in the execution of assigned tasks. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific. (JP 1-02) For IT (and NSS), interoperability is 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 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.

Joint Capability Area. 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. (Reference d and dd).

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

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 (reference c).

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

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. (Reference d).

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., DOTLPP) occur that may affect interoperability).

Joint Interface. An IT 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.

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. (Reference d).

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. (Reference d).

Knowledge Management/Decision Support (KM/DS). The KM/DS tool is the authoritative Joint Staff automated tool for processing, coordinating, tasking, and archiving JCIDS documents and related JCIDS action items. The KM/DS Tool is located on the SIPRNet Web site at <https://jrockmnds1.js.smil.mil/guestjrcz/gbase.guesthome>. (Reference d).

Military Communications-Electronics Board (MCEB). 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. (Reference o).

Milestone Decision Authority (MDA). The individual designated in accordance with criteria established by the USD(AT&L), or by the DOD CIO for acquisition programs, to approve entry of an acquisition program into the next phase. (Reference e). The MDA for IT that involves equipment that is an integral part of a weapon or weapon system, or is an acquisition of services program is or will be designated by the USD (AT&L).

Milestones. Major decision points that separate the phases of an acquisition program. (Reference e).

Mission. A mission can be defined in four ways: 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore; 2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task; 3. An assignment with a purpose that clearly indicates the action to be taken and the reason therefore; 4. The dispatching of one or more aircraft to one particular task. Defined in CJCSM 3500.03B.

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.

Mission Systems Engineering. A process for conducting Systems Engineering that is based on the principle that Operational Requirements are defined by missions (and their associated Operational Tasks) that warfighters must perform.

Mission Thread. A specific sequence of tasks performed by operational nodes to accomplish a mission in a given scenario.

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). 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 Military Operations. The military exploitation of the human and technical networking of all elements of an appropriately trained joint force by fully integrating collective capabilities, awareness, knowledge, experience, and superior decision making to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic and uncertain military operational environments. Adapted from the definition in Net-Centric Environment JFC, v1.0, 7 April 2005.

Net-Ready. DOD IT that meets required information needs, information timeliness requirements, has IA accreditation, and meets the attributes required to support military operations, to be entered and managed on the network, and to effectively exchange information for both the technical exchange of information and the operational effectiveness of that exchange.

DOD IT 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 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 documents sponsor identified and JROC validated verifiable performance measures and metrics for interoperability engineering, design, and testing. To meet NR KPP attributes, IT must be able to support military operations, to be entered and managed on the network, and to effectively exchange information. The NR KPP development process will help verify operationally effective provider to consumer, end-to-end information exchanges according to the sponsor's stated capability requirements and applicable reference models and reference architectures. It informs the solution architecture according to the DOD Information Enterprise Architecture (IEA).

NR-KPP Effectiveness and Performance Measures. Portion of the NR-KPP that describes the measurable and testable Operational Requirements for the NR-KPP. These Operational Requirements are the Threshold and Objective performance values for each of the NR-KPP Attributes. The full description

from the NR-KPP Compliance Statement is as follows: 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.

Net-Ready Operational Task. An Operational Task that produces information for an external system or consumes information from an external system.

Node. Operational unit (e.g. ship, submarine, airplane, shore site, etc.) that can perform an Operational Task.

NR-KPP Attributes. The three attributes listed in the NR-KPP Description that are used to determine if a system satisfies the NR-KPP. These attributes are: support net-centric military operations, enter and be managed in the network, and exchange information. These are the same thing as net-ready attributes.

Network. A group of interconnected IT systems and subsystems (e.g. computers and peripherals) that share IT software and hardware resources to enter, store, manage and exchange data and information between multiple users. Networks are normally governed by defined rules and standards that make shared data discoverable and available to users per specific caveats and procedures.

Non-GIG IT. Stand-alone, self-contained, or embedded IT that is not, and will not be connected to the enterprise network. (reference DODI 4630.8)

National Security Systems (NSS). Information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, 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). NSS include any information system (including any telecommunications system) protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy (reference i).

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.

Program of Record. IT with a program element funded through the program objective memorandum process and included in the FYDP.

Reference Architecture. An authoritative source of architecture information (within a domain) that guides and constrains the instantiations of solution architectures by providing rules, principles and holistic models and patterns of the abstract architectural elements together with a common vocabulary, and sets of technical standards/specifications (Derived from OASIS, OMB, and Joint Pub 1-02 References).

Reference Model. An abstract framework for understanding significant relationships among the entities of some environment. (Reference Model for Service Oriented Architecture 1.0, Organization for the Advancement of Structured Information Standards (OASIS))

Solution Architecture. A framework or structure that portrays the relationships among all the elements of something that answers a problem. This architecture type is used to define a particular project to create, update, revise, or delete established activities in the Department. Solution architecture may be developed to update or extend another architecture. A solution architecture is the most common type of architecture developed in the Department. (DODAF V2.0)

Spectrum Requirements. The determination as to whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or system during its expected life cycle 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 requirements is based upon, as a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of EMC.

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

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 has undergone IT standards conformance testing with respect to a given standard and it correctly implements the standard, with specified profiles and options.

System / Service 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.

System Design. The portion of the Systems Engineering Process used for top-down design. This part of Systems Engineering ultimately develops various detailed specifications and other products that describe system solutions. System Design includes the System Engineering Technical Processes of Requirements Development, Logical Analysis, and Design Solution. Defined in Defense Acquisition Course SYS 101.

System Performance Requirements. Performance requirements the system must meet in order to satisfy its Operational Requirements.

System Realization. Providing the physical design solution in a product form suitable for meeting the applicable acquisition phase exit criteria, including product verification and validation and transitioning the product to the next level up of the system structure or ultimately, to the customer. System Realization includes the Systems Engineering Technical Processes of Implementation, Integration, Verification, Validation, and Transition. Defined in Defense Acquisition Course SYS 101.

Systems Engineering Process. The overarching process that a program team applies to transition from a stated capability need to an operationally effective and suitable system. Systems engineering encompasses the application of systems engineering processes across the acquisition life cycle (adapted to each and every phase) and is intended to be the integrating mechanism for balanced solutions addressing capability needs, design considerations and constraints, as well as limitations imposed by technology, budget, and schedule. The systems engineering processes are applied early in concept definition, and then continuously throughout the total life cycle. Defined in the Defense Acquisition Guidebook.

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

Unanticipated Use. Any use of the data or services described in an architecture which have not previously been defined as an operational use in the ICD, DCR, CONOPS, CDD, and CPD.

Unanticipated Users. Users who do not provide advance warning they will use data.

(INTENTIONALLY BLANK)