DISA

Defense Information Systems Agency

A Combat Support Agency

Test & Evaluation of the NR-KPP

Danielle Mackenzie Koester
Chief, Engineering and Policy Branch

March 15, 2011

"The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government."

Purpose

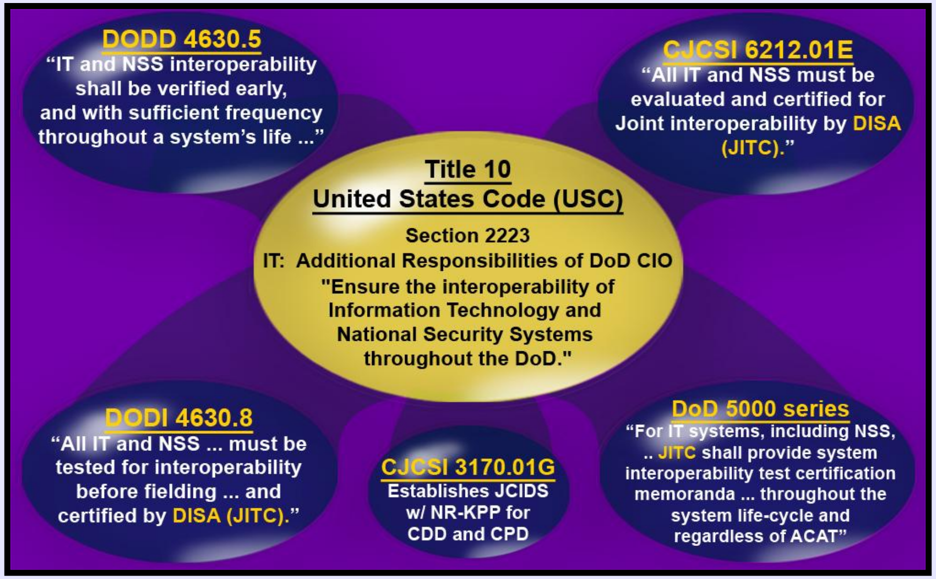
Provide an overview of the policies, processes and procedures for assessing compliance with the Net-Ready Key Performance Parameter

Goal: Establish a measurable, testable, and operationally relevant approach to Joint interoperability (IOP) engineering, test, evaluation & certification (TE&C)

Policy Overview

JS - Interoperability Certification

DOT&E - Operational Test Reports



DODD 4630.5
"IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life ..."

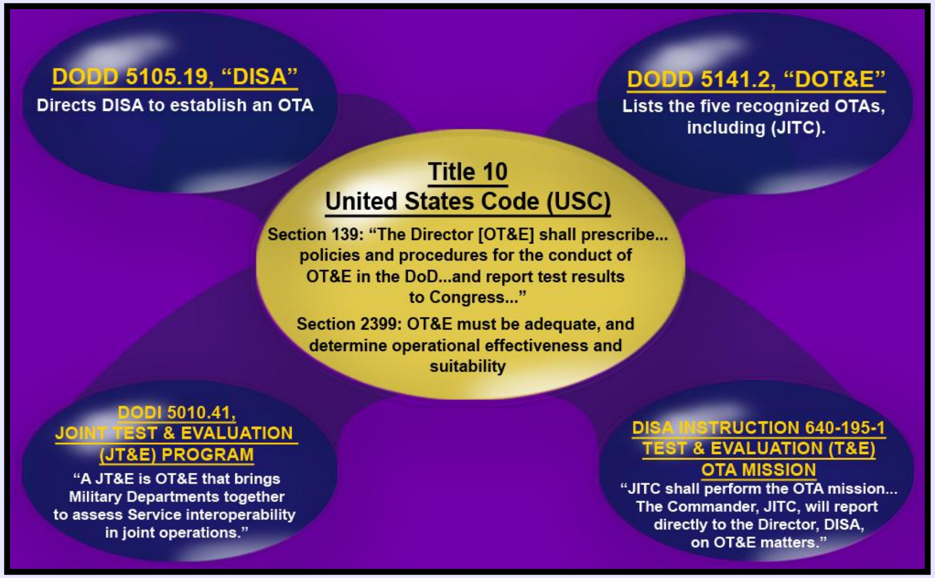
CJCSI 6212.01E
"All IT and NSS must be evaluated and certified for Joint interoperability by DISA (JITC)."

Title 10
United States Code (USC)
Section 2223
IT: Additional Responsibilities of DoD CIO
"Ensure the interoperability of Information Technology and National Security Systems throughout the DoD."

DODI 4630.8
"All IT and NSS ... must be tested for interoperability before fielding ... and certified by DISA (JITC)."

CJCSI 3170.01G
Establishes JCIDS w/ NR-KPP for CDD and CPD

DoD 5000 series
"For IT systems, including NSS, .. JITC shall provide system interoperability test certification memoranda ... throughout the system life-cycle and regardless of ACAT"



DODD 5105.19, "DISA"
Directs DISA to establish an OTA

DODD 5141.2, "DOT&E"
Lists the five recognized OTAs, including (JITC).

Title 10
United States Code (USC)
Section 139: "The Director [OT&E] shall prescribe... policies and procedures for the conduct of OT&E in the DoD...and report test results to Congress..."

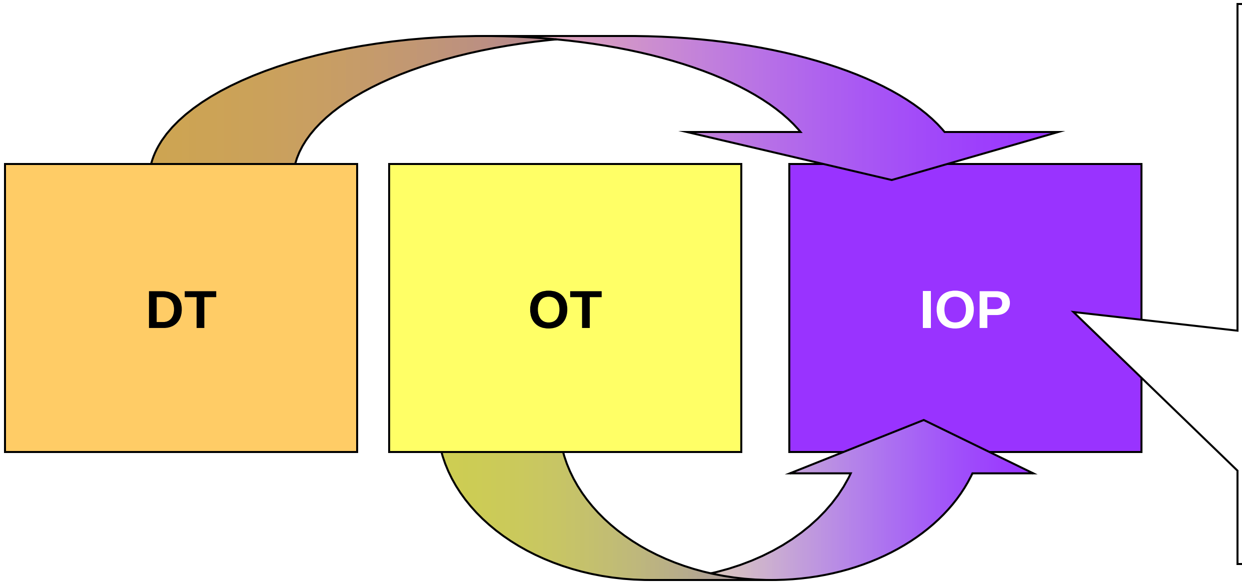
Section 2399: OT&E must be adequate, and determine operational effectiveness and suitability

DODI 5010.41, JOINT TEST & EVALUATION (JT&E) PROGRAM
"A JT&E is OT&E that brings Military Departments together to assess Service interoperability in joint operations."

DISA INSTRUCTION 640-195-1 TEST & EVALUATION (T&E) OTA MISSION
"JITC shall perform the OTA mission... The Commander, JITC, will report directly to the Director, DISA, on OT&E matters."

DISA
A Combat Support Agency

Joint Interoperability Test Certification Overview



NR-KPP Elements:

Compliant Solution Architectures

Net-Centric Data and Services Strategy

GIG Technical Guidance

Information Assurance

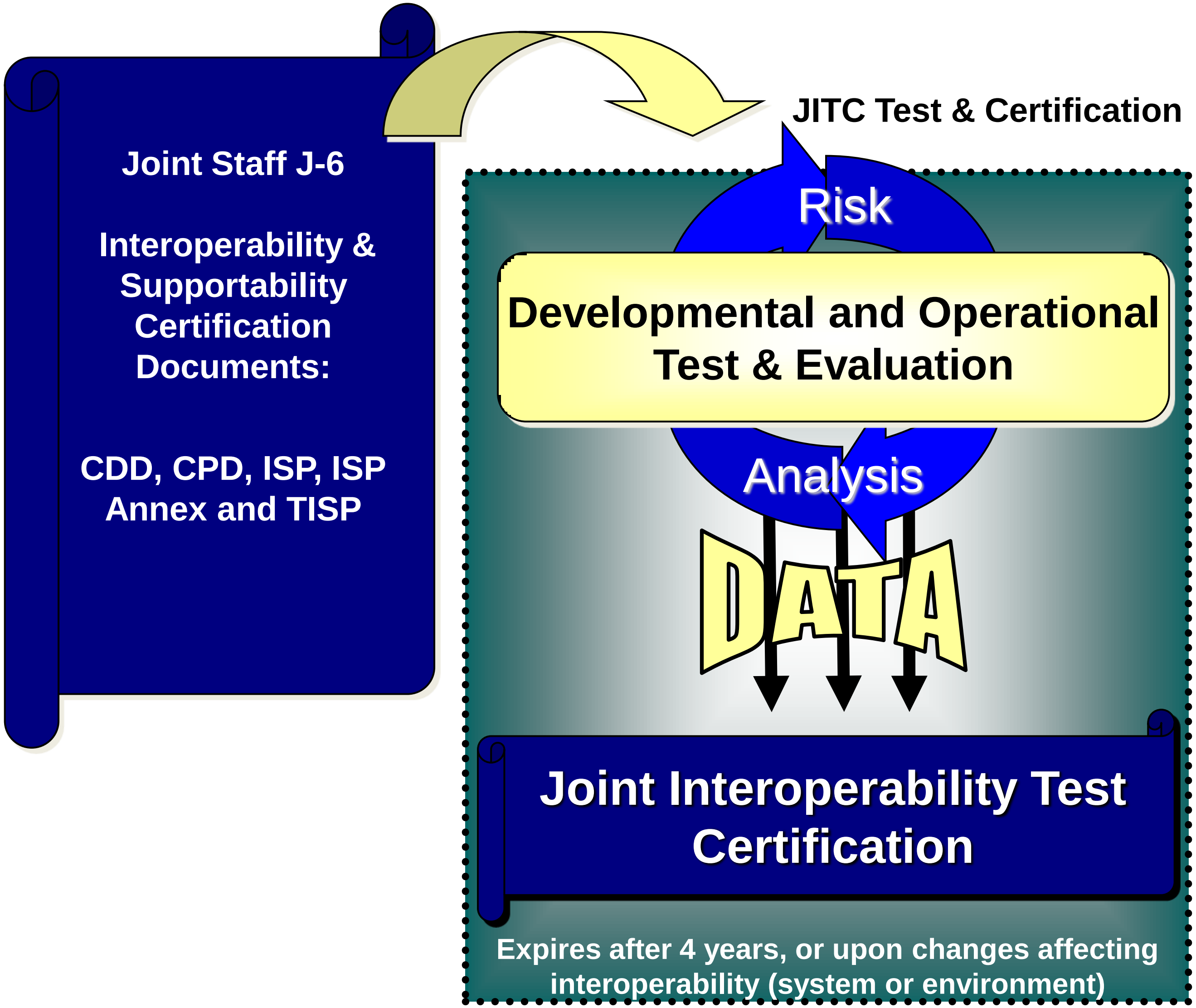
Supportability

- **The NR-KPP elements define the areas JITC evaluates for interoperability certification**
- **JITC uses data collected during DT, OT, demonstrations, exercises, or other reliable sources for interoperability evaluations**

Success = Minimizing separate interoperability testing by leveraging DT/OT

A Combat Support Agency

Joint Interoperability Certification Process



Joint Staff J-6

Interoperability & Supportability Certification Documents:

CDD, CPD, ISP, ISP Annex and TISP

JITC Test & Certification

Risk

Developmental and Operational Test & Evaluation

Analysis

DATA

Joint Interoperability Test Certification

Expires after 4 years, or upon changes affecting interoperability (system or environment)

NOTE: Interoperability changes require reentering process at appropriate point:

- ✓ Requirements updates
- ✓ J-6 I&S Certification
- ✓ JITC Test & Certification

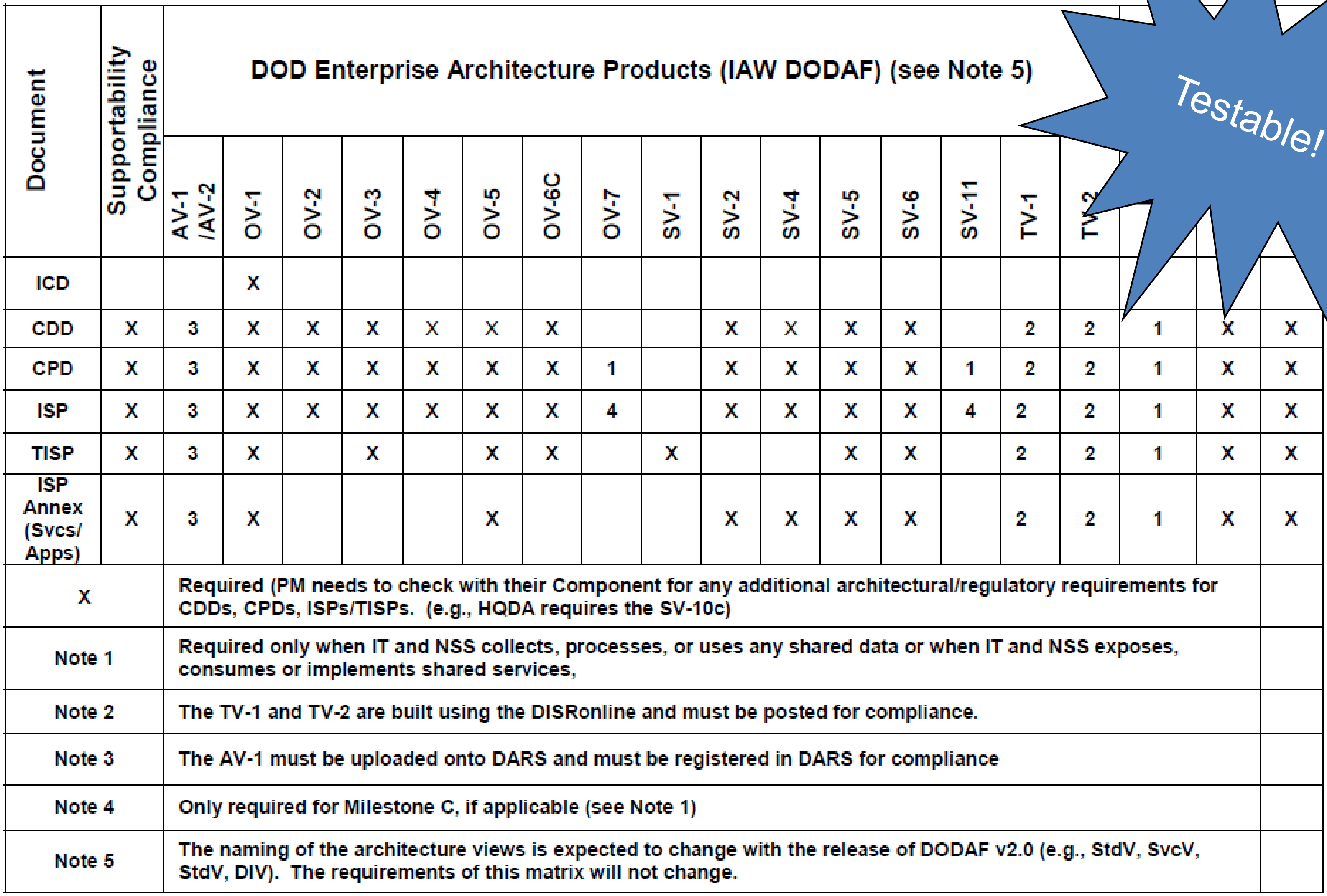
A Combat Support Agency

NR-KPP Statement

Testable?

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

NR-KPP Requirements Source



Document	Supportability Compliance	DOD Enterprise Architecture Products (IAW DODAF) (see Note 5)																		
		AV-1 /AV-2	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	OV-7	SV-1	SV-2	SV-4	SV-5	SV-6	SV-11	TV-1	TV-2			
ICD			X																	
CDD	X	3	X	X	X	X	X	X			X	X	X	X		2	2	1	X	X
CPD	X	3	X	X	X	X	X	X	1		X	X	X	X	1	2	2	1	X	X
ISP	X	3	X	X	X	X	X	X	4		X	X	X	X	4	2	2	1	X	X
TISP	X	3	X		X		X	X		X			X	X		2	2	1	X	X
ISP Annex (Svcs/ Apps)	X	3	X				X				X	X	X	X		2	2	1	X	X

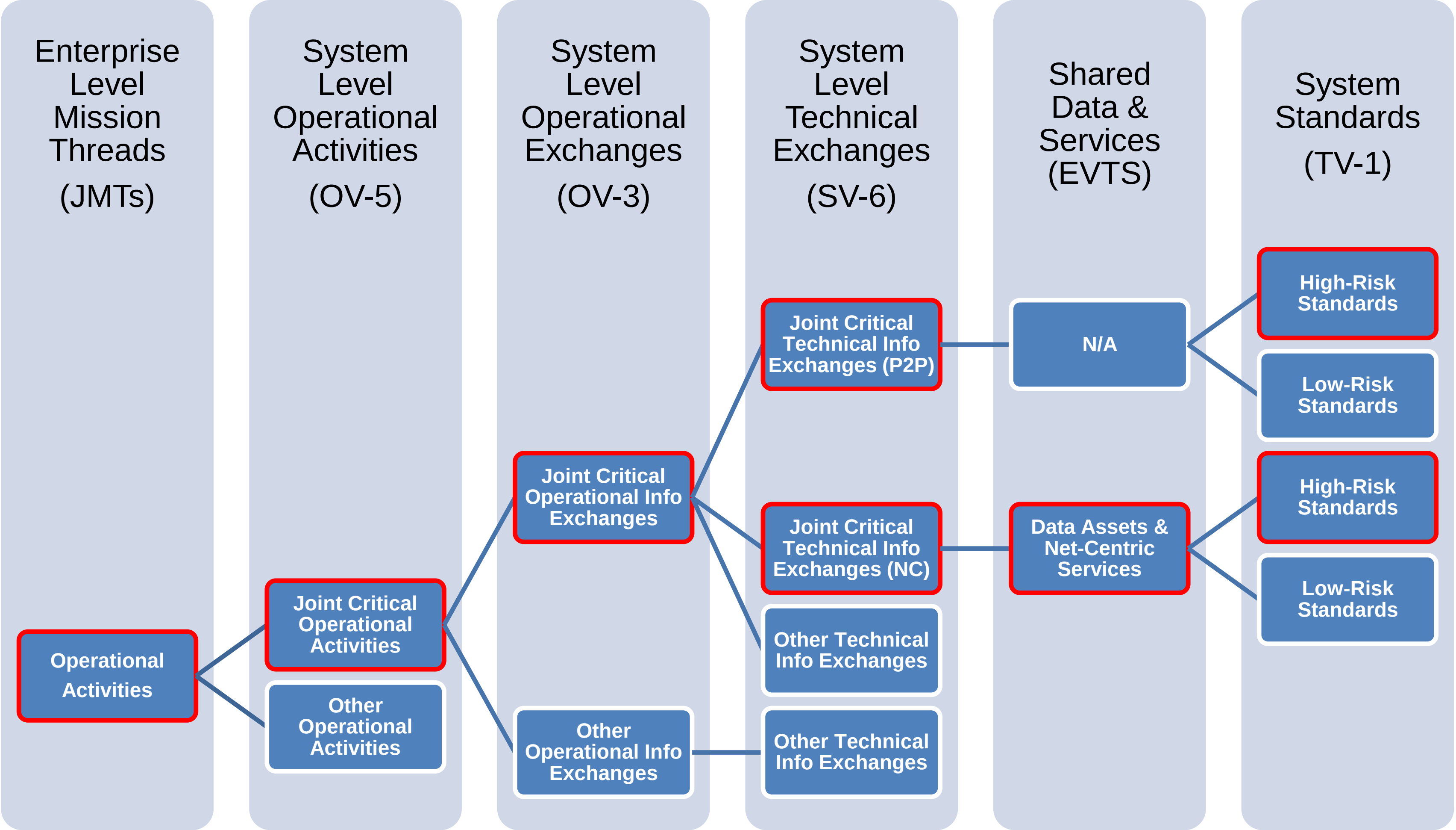
X	Required (PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs, ISPs/TISPs. (e.g., HQDA requires the SV-10c)
Note 1	Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements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

Testable!

DISA

A Combat Support Agency

Mapping NR-KPP to Operational Impact



Enterprise Level Mission Threads (JMTs)
System Level Operational Activities (OV-5)
System Level Operational Exchanges (OV-3)
System Level Technical Exchanges (SV-6)
Shared Data & Services (EVTS)
System Standards (TV-1)
Operational Activities
Joint Critical Operational Activities
Other Operational Activities
Joint Critical Operational Info Exchanges
Other Operational Info Exchanges
Joint Critical Technical Info Exchanges (P2P)
Joint Critical Technical Info Exchanges (NC)
Other Technical Info Exchanges
Other Technical Info Exchanges
N/A
Data Assets & Net-Centric Services
High-Risk Standards
Low-Risk Standards
High-Risk Standards
Low-Risk Standards

Universal Joint Task Metrics	Universal Joint & Service Task Metrics	Secure, Timely, Accurate, and Usable as Defined in OV-3	Secure, Timely, Accurate, and Usable as Defined in SV-6	Visible, Accessible, Understandable, Secure, Interoperable	No Conformance Issues Resulting in Critical Operational Impact

Operationally Effective Information Exchanges

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

Operationally Effective Information Exchanges

- Requirements Analysis
  - What missions and activities does the system support?
    - Joint Mission Threads
    - OV-6c
    - OV-5
  - What information exchanges are necessary to execute those missions and activities?
    - OV-3
    - SV-6

- Test Planning and Execution
  - Must be on production representative system in an operationally realistic environment

Did the system meet all *joint critical* information exchange requirements?

Data & Services Strategies

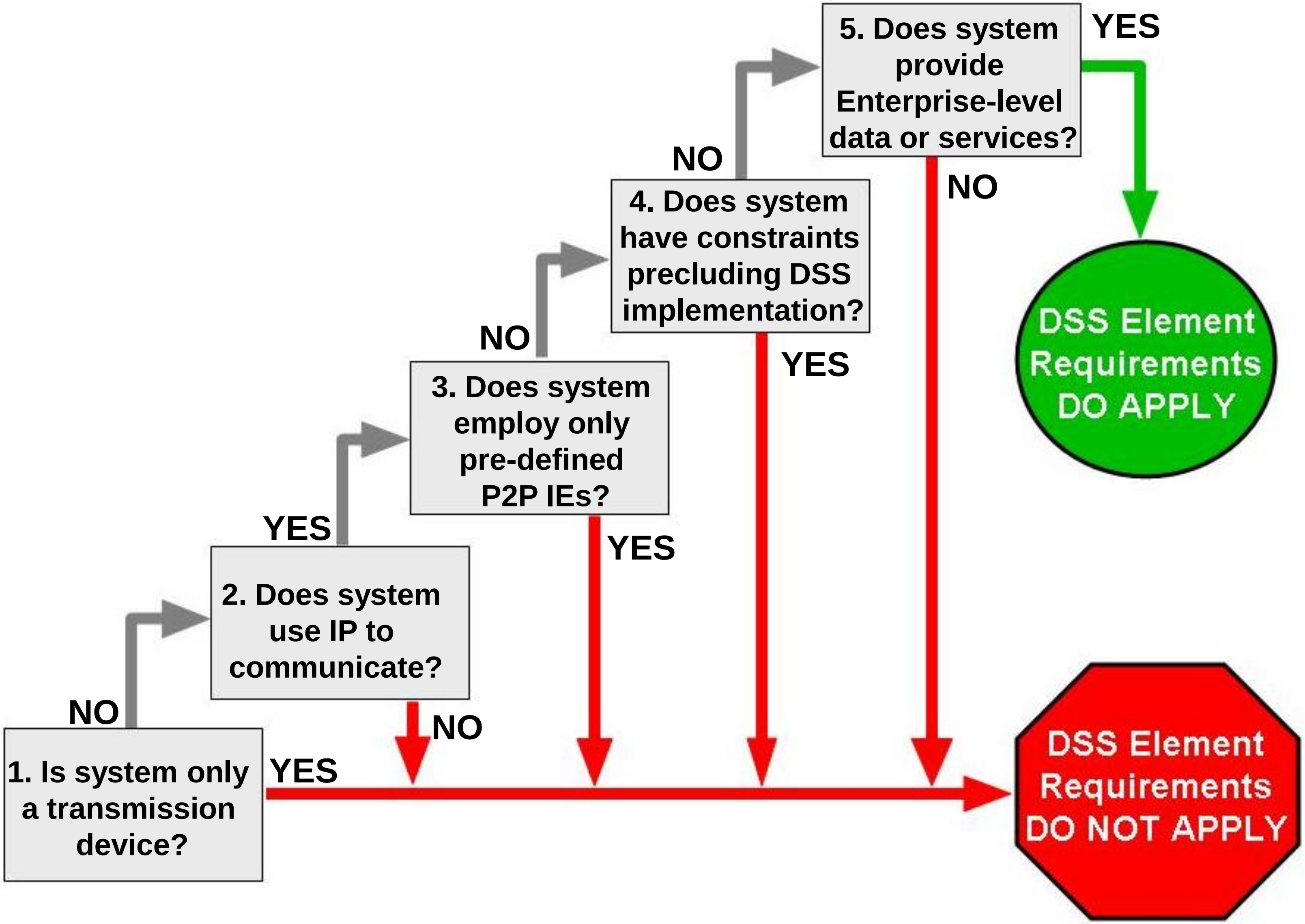
KPP	Threshold	Objective
Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system,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

DISA

A Combat Support Agency

Data & Services Strategies

Does it apply?



5. Does system provide Enterprise-level data or services?
YES
NO
4. Does system have constraints precluding DSS implementation?
NO
YES
3. Does system employ only pre-defined P2P IEs?
NO
YES
2. Does system use IP to communicate?
YES
NO
1. Is system only a transmission device?
NO
YES
DSS Element Requirements DO APPLY
DSS Element Requirements DO NOT APPLY

Data & Services Strategies

Requirements

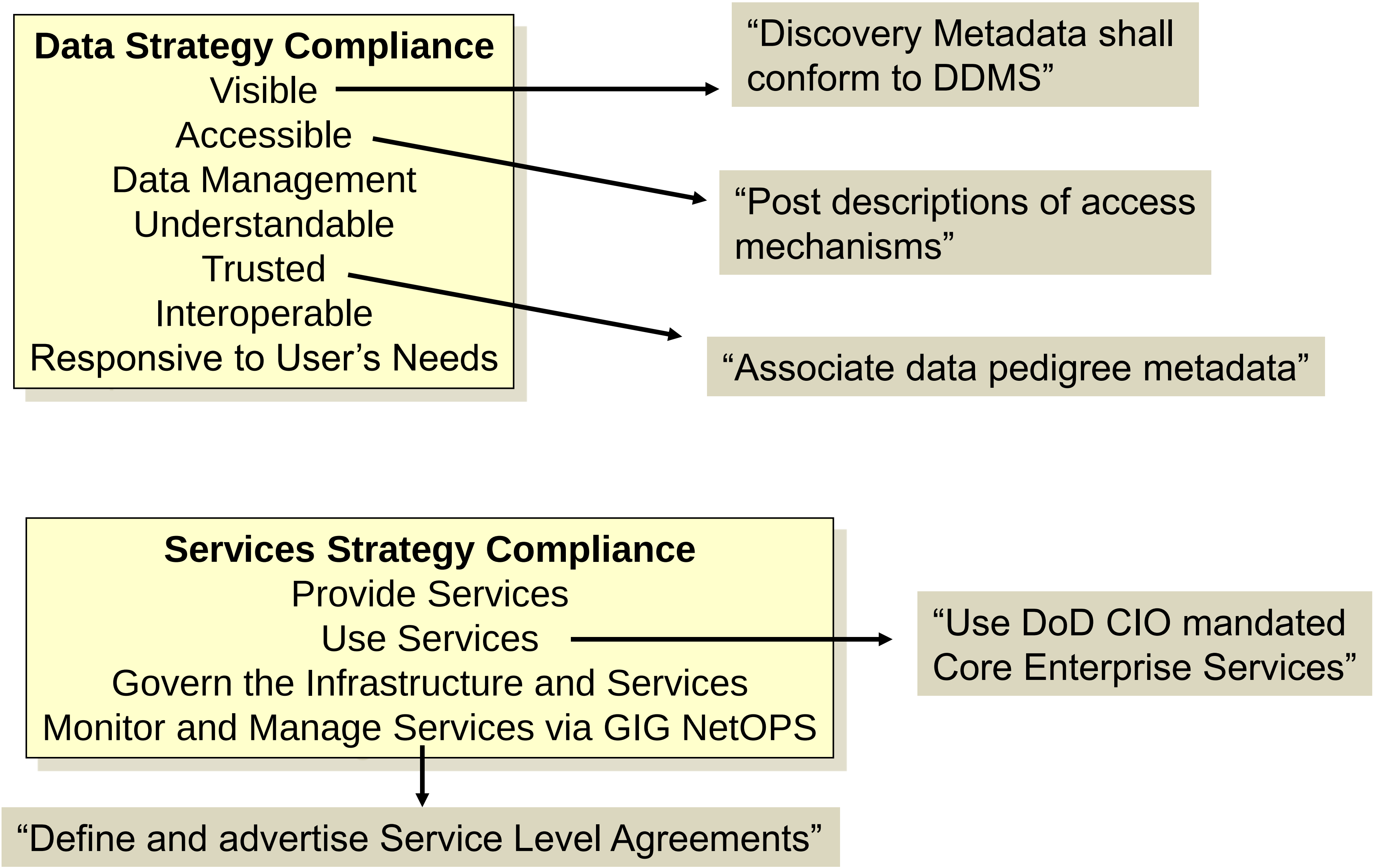
Data Strategy Compliance
Visible
Accessible
Data Management
Understandable
Trusted
Interoperable
Responsive to User's Needs

Services Strategy Compliance
Provide Services
Use Services
Govern the Infrastructure and Services
Monitor and Manage Services via GIG NetOPS

DoD Information Enterprise Architecture Compliance
Data and Services Deployment
Secured Availability
Shared Infrastructure Environment
Computing Infrastructure Readiness
NetOPS Agility

Data & Services Strategies

Requirements



Data Strategy Compliance

Visible

Accessible

Data Management

Understandable

Trusted

Interoperable

Responsive to User's Needs

"Discovery Metadata shall conform to DDMS"

"Post descriptions of access mechanisms"

"Associate data pedigree metadata"

Services Strategy Compliance

Provide Services

Use Services

Govern the Infrastructure and Services

Monitor and Manage Services via GIG NetOPS

"Use DoD CIO mandated Core Enterprise Services"

"Define and advertise Service Level Agreements"

A Combat Support Agency

Data & Services Strategies

Requirements

Net-Centric Data Requirement

Data is Visible

Post discovery metadata in an Enterprise Catalog: Department of Defense (DoD) Discovery Metadata Specification (DDMS)- conformant discovery metadata is posted in the Net-Centric Enterprise Services (NCES) Enterprise Catalog or other compatible/federated enterprise catalog that is visible to the Enterprise.

Use appropriate keywords for discovery: Discovery keywords should reflect common user terms, be appropriate for mission area or data type, be understandable, and conform with MDR requirements that map back to COI identified mission data.

Data is Accessible

Post data to shared space: Data asset is available in a shared space, i.e., a space that is accessible to multiple end users.

Provide access policy: If data is not accessible to all users, a written policy on how to gain access is available and accurate.

Provide serving (access) mechanism: Shared space provides serving (access) mechanisms for the data. I.e., a service provides users with access to the data.

Publish active link to data asset: The Enterprise Catalog DoD Discovery Metadata Specification (DDMS) entry contains an active link (e.g., Uniform Resource Identifier (URI)) to the data asset.

Data is Understandable

Publish semantic and structural metadata

- Semantic and structural metadata are published in the Enterprise Catalog.

Register data artifacts in DoD MDR

- XML schema definitions (XSD), eXtensible Markup Language (XML) instances, data models (such as entity relationship diagrams) and other appropriate artifacts are registered in the DoD Metadata Registry (MDR).

Data is Interoperable

Base vocabularies on Universal Core (UCore)

- Semantic vocabularies reuse elements of the Universal Core (Ucore) standard.

Comply with COI data-sharing agreements

- Semantic and structural metadata conform to interoperability agreements promoted through communities, e.g., Community of Interest (COI).

Conform to DDMS

- All metadata, including record-level database tagging and in-line document tagging, complies with DDMS.

Data is Trusted

Provide information assurance and security metadata

- All metadata, including record-level database tagging and in-line document tagging, includes data pedigree and security metadata, as well as an authoritative source for the data (when appropriate).

Net-Centric Services Requirement

Services are Visible

Publish a description of the service or access mechanism

- Descriptions (metadata) for the service or access mechanism are published in an enterprise service registry, e.g., the NCES Service Registry.

Comply with enterprise-specified minimum service discovery requirements

- The data access mechanism complies with enterprise-specified minimum service discovery requirements, e.g., a Universal Description, Discovery and Integration (UDDI) description to enable federated discovery.

Services are Accessible

Provide an active link to the service in the enterprise catalog

- Active link (e.g., Uniform Resource Identifier (URI)) to the specified service is included in the enterprise catalog metadata entry (i.e., metacard) for the specified service.

Provide an active link to the service in the NCES Service Registry

- URIs as the operational end points for services shall be registered in the NCES Service Registry by referencing the WSDL (that is in the MDR).

Services are Understandable

Publish a description of the service or access mechanism to the NCES Service Registry

- Metadata for the service or access mechanism are published in the NCES Service Registry.

Publish service artifacts to DoD MDR

- Web Service Description Language (WSDL) documents, and other appropriate artifacts are registered in the DoD Metadata Registry (MDR).

Provide service specification or Service Level Agreement (SLA)

- A service specification or Service Level Agreement (SLA) exists for services and data access mechanisms.

Services are Trusted

Operate services in accordance with SLA

- The service meets the performance standards in the SLA

Include security mechanisms or restrictions in the service specification

- The service specification describes security mechanisms or restrictions that apply to the service

Enable continuity of operations and disaster recovery for services

- The service has a defined and functional Continuity of Operations Plan

Provide NetOps Data (NetOps Agility)

- Services and data access mechanisms provide operational states, performance, availability, and security data/information to NetOps management services, e.g., Enterprise Management, Content Management, and Network Defense services

Use of Core Enterprise Services (CES)

- Core Enterprise Services (CES) are used in accordance with DoD CIO mandates

Data & Services Strategies

- **Requirements Analysis**
  - **Do the net-centric requirements apply?**
  - **What enterprise-level shared data and service assets are documented in the Exposure Verification Tracking Sheets?**
  - **What data and service assets support a joint critical operational activity?**

- **Test Planning and Execution**
  - **Static analysis (e.g., registration of assets)**
  - **Conformance/compliance testing (e.g., schema conformance)**
  - **Mission effectiveness (e.g., visibility, accessibility)**

Did the system meet all *joint critical* net-centric requirements?
(Visible, Accessible, Understandable, Trusted, Interoperable)

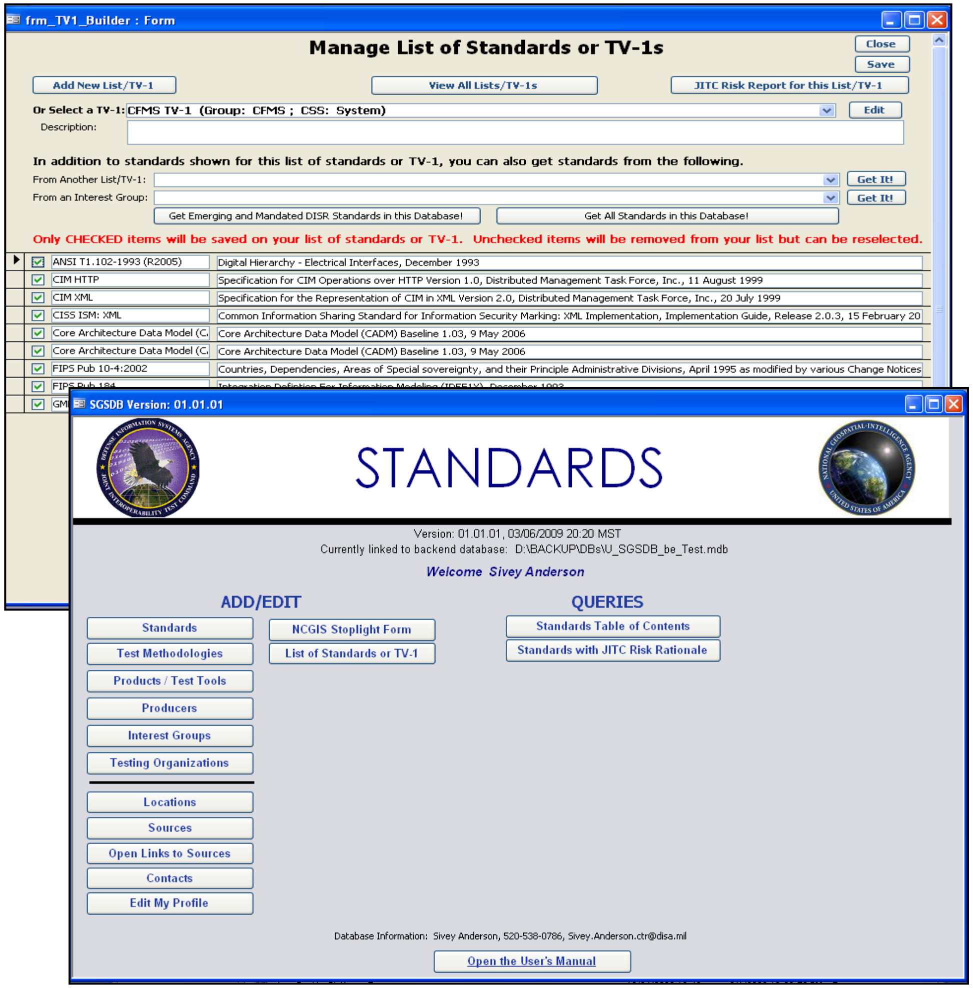
GIG Technical Guidance

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

GIG Technical Guidance

Standards Conformance

- **Requirements Analysis**
  - **Risk analysis on standards identified in system TV-1**
- **Test Planning and Execution**
  - **Leverage commercial and government test results, as appropriate**
  - **Execute standards conformance testing, as appropriate**



frm_TV1_Builder : Form

Manage List of Standards or TV-1s

Close
Save
Add New List/TV-1
View All Lists/TV-1s
JITC Risk Report for this List/TV-1
Edit
Get It!
Get It!
Get Emerging and Mandated DISR Standards in this Database!
Get All Standards in this Database!

Or Select a TV-1: CFMS TV-1 (Group: CFMS ; CSS: System)

Description:

In addition to standards shown for this list of standards or TV-1, you can also get standards from the following.

From Another List/TV-1:

From an Interest Group:

Only CHECKED items will be saved on your list of standards or TV-1. Unchecked items will be removed from your list but can be reselected.

☑	ANSI T1.102-1993 (R2005)	Digital Hierarchy - Electrical Interfaces, December 1993
☑	CIM HTTP	Specification for CIM Operations over HTTP Version 1.0, Distributed Management Task Force, Inc., 11 August 1999
☑	CIM XML	Specification for the Representation of CIM in XML Version 2.0, Distributed Management Task Force, Inc., 20 July 1999
☑	CISS ISM: XML	Common Information Sharing Standard for Information Security Marking: XML Implementation, Implementation Guide, Release 2.0.3, 15 February 20
☑	Core Architecture Data Model (C.	Core Architecture Data Model (CADM) Baseline 1.03, 9 May 2006
☑	Core Architecture Data Model (C.	Core Architecture Data Model (CADM) Baseline 1.03, 9 May 2006
☑	FIPS Pub 10-4:2002	Countries, Dependencies, Areas of Special sovereignty, and their Principle Administrative Divisions, April 1995 as modified by various Change Notices
☑	FIPS Pub 184	Integration Definition For Information Modeling (IDEF1X), December 1993
☑	GM	

SGSDB Version: 01.01.01

STANDARDS

Version: 01.01.01, 03/06/2009 20:20 MST
Currently linked to backend database: D:\BACKUP\DBs\U_SGSDB_be_Test.mdb

Welcome Sivey Anderson

Database Information: Sivey Anderson, 520-538-0786, Sivey.Anderson.ctr@disa.mil

Did the system have any conformance-issues that could result in a critical operational impact?

Information Assurance

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

Information Assurance

- **Requirements Analysis**
  - **What Certification and Accreditation (C&A) process (DIACAP, NISCAP, ICD 503) does the system fall under?**
- **Test Planning and Execution**
  - **Ensure the system is operating in the approved IA configuration during interoperability/operational testing**
  - **Verify IATO/ATO**
  - **Execute required additional IA testing**

Has the system received an Interim Authority to Operate (IATO)/Authority to Operate (ATO)?

Supportability

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

Supportability

- **Threshold = Objective**
  - **Spectrum Supportability**
    - **Verify the system has an approved (Stage 4) DD Form 1494 (for any spectrum dependent system) (DoDI 5000.02)**
    - **Verify completion of applicable requirements of DODD 3222.2, "DOD Electromagnetic Environmental Effects (E3)"**
  - **Selective Availability Anti-Spoofing Module (SAASM)**
    - **Verify any GPS receivers procured are SAASM compliant or that a waiver has been obtained from ASD(NII)**
  - **Joint Tactical Radio System (JTRS)**
    - **Verify a JTRS solution or waiver from ASD(NII) for any radio solution operating within the 2MHz to 2 GHz range***

Reference: (ASD(NII)/DOD CIO memorandum, 23 May 2005, "Temporary Suspension of the Joint Tactical Radio Systems (JTRS) Waiver Process" and ASD(NII)/DOD CIO memorandum, 12 January 2007 "Reinstatement of the Joint Tactical Radio, (JTRS) Waiver Process for Handheld Radio Procurements")

Interoperability Certification Products

Certification	Description	System can be fielded (Y/N)?
Standards Conformance Certification	System is certified for conformance to a standard/standards profile	No
Joint Interoperability Test Certification	Full system certification. System meets at least all critical interoperability requirements	Yes
Limited Joint Interoperability Test Certification	System meets subset of critical interoperability requirements	Yes, with ICTO
Interim Joint Interoperability Test Certification	Capability module has adequately demonstrated interoperability for at least all critical threshold requirements identified for the increment	Yes
Special Interoperability Test Certification	Certification is based on other J-6 approved requirements other than the NR-KPP, e.g., use of UCR for voice switches	Yes
Non-Certification	Critical operational impacts expected Provides a warning to the warfighter	No
Interoperability Assessment	PM would like to determine interoperability status. System may lack J-6 certified requirements	No

A Combat Support Agency

Contact Information & Resources

- **Hotline**
  - 24/7 C4I Technical Support
  - 1-800-538-JITC (5482)
  - hotline@disa.mil
  - http://jitc.fhu.disa.mil/support.html
- **Joint Interoperability Tool (JIT)**
  - http://jit.fhu.disa.mil
  - Lessons Learned reports
  - NATO Interface Guide
- **System Tracking Program (STP)**
  - https://stp.fhu.disa.mil
  - Test events
  - Test plans and reports
  - Certification results
- **NR-KPP Helpdesk**
  - NR-KPP_Helpdesk@disa.mil
- **NR-KPP Testing Guidebook**
  - https://www.us.army.mil/suite/doc/23429848
- **CJCSI 6212 Resource Page**
  - https://www.intelink.gov/wiki/Portal:CJCSI_6212_Resource_Page

Questions?

Danielle Mackenzie Koester
Chief, Engineering & Policy Branch
Joint Interoperability Test Command
March 15, 2011

DEFENSE INFORMATION SYSTEMS AGENCY