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

DOD 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)."

DODI 4630.8
"All IT and NSS ... must be tested for interoperability before fielding ... and certified 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."

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."

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

DOD 5101.41, JOINT TEST & EVALUATION (JT&E) PROGRAM
"JITC is OT&E that brings ... assess Service interoperability in joint operations."

DOD 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

DISA INSTRUCTION 640-19S-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."
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.
Joint Interoperability Certification Process

Joint Staff J-6
Interoperability & Supportability Certification Documents:
CDD, CPD, ISP, ISP Annex and TISP

Joint Interoperability Test Certification
Expires after 4 years, or upon changes affecting interoperability (system or environment)

Risk Analysis

Developmental and Operational Test & Evaluation

NOTE: Interoperability changes require reentering process at appropriate point:
- Requirements updates
- J-6 I&S Certification
- JITC Test & Certification
NR-KPP Statement

Net-Ready: 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.

Net-Ready - KPP Statement

<table>
<thead>
<tr>
<th>KPP</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net-Ready: 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:</td>
<td>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:</td>
<td></td>
</tr>
<tr>
<td>1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges</td>
<td>1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.</td>
<td>5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.</td>
<td></td>
</tr>
<tr>
<td>Document</td>
<td>Supportability Compliance</td>
<td>DOD Enterprise Architecture Products (IAW DODAF) (see Note 5)</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>ICD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDD</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>CPD</td>
<td>X 3 x x x x x x</td>
<td></td>
</tr>
<tr>
<td>ISP</td>
<td>X 3 x x x x x 1</td>
<td></td>
</tr>
<tr>
<td>TISP</td>
<td>X 3 x x x x</td>
<td></td>
</tr>
<tr>
<td>ISP Annex (SvcS/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apps)</td>
<td>X 3 x x x x</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>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)</td>
</tr>
</tbody>
</table>

**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.
# Mapping NR-KPP to Operational Impact

## Enterprise Level
- Mission Threads (JMTs)

## System Level
- Operational Activities (OV-5)
- Operational Exchanges (OV-3)
- Technical Exchanges (SV-6)

## Shared Data & Services (EVTS)
- Joint Critical Technical Info Exchanges (P2P)
- Joint Critical Technical Info Exchanges (NC)
- Data Assets & Net-Centric Services

## System Standards (TV-1)
- High-Risk Standards
- Low-Risk Standards

## Operational Activities
- Secure, Timely, Accurate, and Usable as Defined in OV-3
- Visible, Accessible, Understandable, Secure, Interoperable

## Other Technical Info Exchanges
- No Conformance Issues Resulting in Critical Operational Impact

## Universal Joint Task Metrics
- Universal Joint Task Metrics

## Universal Joint & Service Task Metrics
- Other Operational Activities
- Other Operational Info Exchanges

## Joint Critical Operational Activities
- Joint Critical Operational Info Exchanges

## Other Operational Activities
- Other Technical Info Exchanges
# Operationally Effective Information Exchanges

<table>
<thead>
<tr>
<th>KPP</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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?
### KPP

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.

---

### Threshold

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.

---

### Objective

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.
1. Is system only a transmission device?

2. Does system use IP to communicate?

3. Does system employ only pre-defined P2P IEs?

4. Does system have constraints precluding DSS implementation?

5. Does system provide Enterprise-level data or services?

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 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”
### Data & Services Strategies

#### Requirements

<table>
<thead>
<tr>
<th>Net-Centric Data Requirement</th>
<th>Net-Centric Services Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Net-Centric Data Requirement</strong></td>
<td><strong>Net-Centric Services Requirement</strong></td>
</tr>
<tr>
<td><strong>Data is Visible</strong></td>
<td><strong>Services are Visible</strong></td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Data is Accessible</strong></td>
<td><strong>Services are Accessible</strong></td>
</tr>
<tr>
<td>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.</td>
<td>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).</td>
</tr>
<tr>
<td><strong>Data is Understandable</strong></td>
<td><strong>Services are Understandable</strong></td>
</tr>
<tr>
<td>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).</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Data is Interoperable</strong></td>
<td><strong>Services are Trusted</strong></td>
</tr>
<tr>
<td>Base vocabularies on Universal Core (UCore) - Semantic vocabularies reuse elements of the Universal Core (Ucore) standard. Comply with UCore 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.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Data is Trusted</strong></td>
<td><strong>Use of Core Enterprise Services (CES)</strong></td>
</tr>
<tr>
<td>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).</td>
<td>- Core Enterprise Services (CES) are used in accordance with DoD CIO mandates.</td>
</tr>
</tbody>
</table>
• 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)
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.
• 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

Did the system have any conformance-issues that could result in a critical operational impact?
<table>
<thead>
<tr>
<th>KPP</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
• 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)?
<table>
<thead>
<tr>
<th>KPP</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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*

# Interoperability Certification Products

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

- **Hotline**
  - 24/7 C4I Technical Support
  - 1-800-538-JITC (5482)
  - hotline@disa.mil

- **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**

- **CJCSI 6212 Resource Page**
Questions?

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