



Defense Information Systems Agency

Joint Interoperability Test Command

**FY2010
NR-KPP GUIDEBOOK**



(This page intentionally left blank.)



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY
REFER TO: Joint Interoperability Test Command (JT)

MEMORANDUM FOR JOINT INTEROPERABILITY TEST COMMAND WORKFORCE

SUBJECT: Joint Interoperability Test Command (JITC) Net-Ready Key Performance Parameter (NR-KPP) Testing Guidebook

1. The JITC NR-KPP Testing Guidebook provides a consistent and repeatable test methodology in accordance with industry best practices, JITC procedures, and Department of Defense (DoD) policies.
2. The JITC NR-KPP Testing Guidebook will be updated on a quarterly basis to ensure test procedures are always kept up to date based on changes in policy, technology, and user feedback.
3. The current version of the JITC NR-KPP Testing Guidebook is available at <\\Cdxfhul\groups\PLANS & POLICIES TRAINING\NR-KPP\Guidebook>
4. Comments to the content of the Guidebook should be sent to the JITC NR-KPP Helpdesk: NR-KPP_Helpdesk@disa.mil
5. The point of contact for this action is Ms. Danielle Koester, Chief, Engineering & Policy Branch, (520) 538-5342, DSN, 879-5342, or e-mail Danielle.Koester@disa.mil.

A handwritten signature in black ink, appearing to read "Ronald C. Stephens", is positioned above the typed name.

RONALD C. STEPHENS
Colonel, USA
Commanding

(This page intentionally left blank.)

TABLE OF CONTENTS

	Page
Introduction.....	1
Chapter 1 – Solution Architecture.....	1-1
Chapter 2 – Net-Centric Data and Services Strategy.....	2-1
Chapter 3 – Global Information Grid Technical Guidance.....	3-1
Chapter 4 – Information Assurance	4-1
Chapter 5 – Supportability Element.....	5-1
Appendix A – Acronyms.....	A-1
Appendix B – Definitions.....	B-1
Appendix C – Integrated Architecture Traceability Matrix Methodology.....	C-1
Appendix D – Data and Services Strategy Test Procedures.....	D-1
Appendix E – References.....	E-1

(This page intentionally left blank.)

INTRODUCTION

NET-READY KEY PERFORMANCE PARAMETER OVERVIEW

The Net-Ready Key Performance Parameter (NR-KPP) compliance statement in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E states that, at a minimum, the capability, system, or service must fully support execution of operational activities and Information Exchanges (IEs) identified in the Department of Defense (DoD) Enterprise Architecture and solution architectures (based on integrated DoD Architecture Framework (DoDAF) content) must satisfy the technical requirements for transition to net-centric military operations. The following five elements summarize the minimum (threshold) requirements.

- **Solution Architecture.** Solution architecture products must comply with the current DoDAF version, guided by the regulations and policies of the DoD Information Enterprise Architecture (IEA), and demonstrate operationally effective IEs.
- **Net-Centric Data and Services Strategy Compliance.** The capability, system, or service must comply with the DoD Net-Centric Data Strategy, the DoD Net-Centric Services Strategy, and the principles and rules identified in the DoD IEA.
- **Global Information Grid Technical Guidance.** The capability, system, or service must comply with Global Information Grid (GIG) Technical Guidance (GTG) as necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views. The GTG includes Information Technology (IT) standards identified in the Technical View-1 and implementation guidance of GIG Enterprise Service Profiles.
- **Information Assurance.** The capability, system, or service must comply with Information Assurance (IA) requirements and must have an Authorization to Operate or Interim Authorization to Operate, issued by the Designated Accrediting Authority. The IA requirements include availability, integrity, authentication, confidentiality, and non-repudiation.
- **Supportability.** The capability, system, or service must comply with supportability requirements to include Selective Availability Anti-Spoofing Module, Spectrum, and Joint Tactical Radio System requirements.

THE JOINT INTEROPERABILITY TEST COMMAND'S ROLE

The Joint Interoperability Test Command's (JITC's) role is to evaluate a capability, system, or service's ability to meet the threshold and objective levels of each NR-KPP element when testing a system for joint interoperability certification. The threshold level requires that the capability, system, or service must fully support execution of joint critical operational activities and IEs. The objective level requires that

all of the capability, system, or service must fully support execution of all operational activities and IEs.

Definition of Joint Critical. The criticality of operational activities or IE reflects the impact on mission accomplishment of its failure. The system's Program Management Office provides the criticality of every operational activity or IE in the Operational View-5 and System View-6 in the Joint Staff (JS)-certified requirements documents. The IT systems or National Security Systems (NSS) receive one of several joint designations depending on their potential to exchange data or services with IT systems or NSS outside the sponsoring agency. For this guidebook, the term *joint critical* applies to any operational activity or IE designated as critical in JS-certified requirements documents for a program with joint-potential designation.

Joint Staff-Certified Requirements Documents. The JITC begins its requirements analysis when JS J-6, through the Defense Information Systems Agency, tasks JITC to review the capabilities documents. For the purposes of this guidebook, the capabilities documents include the Capability Design Document (CDD), Capability Production Document (CPD), and Information Support Plan (ISP) or Tailored ISP (TISP). According to CJCSI 6212.01E, the ISP (or TISP) is the "preferred reference for all technical artifacts mandated for Interoperability and Supportability certification compliance." Some executive agents may have other requirements documents outside the scope of CJCSI 6212.01E. If so, it may be necessary to confirm with JS J-6 that the requirements have been certified.

The DoD Directive 4630.05 provides the following capabilities document descriptions:

- **ISP.** The ISP documents the program's interoperability, information, and support requirements for the program. The ISP also documents Interoperability and Supportability shortfalls and proposed mitigation plans.
- **CPD.** The CPD provides the operational performance attributes necessary to support production, testing, and deployment of an increment. The CPD presents performance attributes, including Key Performance Parameters. The JS-certified NR-KPP is documented in the CPD.
- **CDD.** The CDD provides the operational performance attributes (e.g., Interoperability and Supportability) necessary for the acquisition community to design the proposed system. The CDD references the originating Initial Capability Document, identifies other CDDs and/or CPDs that are required for full realization of the capability(ies), and references additional overarching doctrine, organization, training, materiel, leadership, personnel, and facilities considerations necessary to develop an effective capability. The JS-certified NR-KPP is also documented in the CDD.

The cases below describe the conditions where JITC can deliver an interoperability certification for a system.

Case 1 – ISP/TISP or CPD. Policy states that a JS-certified ISP/TISP or CPD is needed for certification. If either the ISP/TISP or CPD has been JS-certified, then the JITC may conduct a joint interoperability certification evaluation and issue a Joint Interoperability Certification Memorandum.

Case 2 – CDD. If the system has only a JS-certified CDD and the ISP/TISP/CPD documents have not been JS-certified (or don't exist), then JITC may conduct a joint interoperability assessment and issue a Joint Interoperability Assessment Report. However, JITC has conducted certification evaluations on systems that had only a JS-certified CDD and a JS waiver for the CPD (no significant changes were made to the CDD). This has only occurred on a case-by-case basis.

Case 3 - Special Cases. Some executive agents may have specific documentation requirements that vary from the standard DoD requirements (e.g., the Business Transformation area). Their capability documents should provide the same information for evaluating IEs as the ISP/TISP/CPD. If these documents are JS certified, the JITC can use them for joint interoperability certification; otherwise, they will be considered on a case-by-case basis. This does not apply in cases where the program office is creating its own documentation formats to avoid the process.

GUIDEBOOK ORGANIZATION

This guidebook provides an overview of the test requirements specific, test methodology, and reporting methodology for each NR-KPP element. Appendix C provides instructions on how to use the Integrated Architecture Traceability Matrix to analyze the solution architectures. Appendix D contains instructions for evaluating the Data and Services Strategy.

(This page intentionally left blank.)

CHAPTER 1 – SOLUTION ARCHITECTURE

NET-READY KEY PERFORMANCE PARAMETER STATEMENT

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E defines the Solution Architecture element of the Net-Ready Key Performance Parameter (NR-KPP) as:

"...Compliant with DoD Enterprise Architecture based on integrated DoDAF content, including specified operationally effective information exchanges..."

CJCSI 6212.01E

The Solution Architecture element, also referred to as Compliant Solution Architectures, identifies the requirements for end-to-end, operationally effective Information Exchanges (IEs). During Solution Architecture assessment, testers perform end-to-end interoperability testing via data exchange and ensure the exchange of that data is operationally effective, based on requirements outlined in the Department of Defense (DoD) Architecture Framework (DoDAF) products.

To analyze requirements, the tester will need to analyze the DoDAF products to determine the missions, functions, and activities that the system is implementing and the exchanges that support those missions, functions, and activities. The Operational View (OV)-3 and Systems View (SV)-6 provide the aforementioned information for a particular IE and the performance criteria needed to be assessed during end-to-end interoperability testing.

Developers must ensure that the system's solution architecture 1) Is developed in accordance with the DoD Information Enterprise Architecture business rules and principles; 2) Is developed so that the combination of operational, systems, services, data, and technical views provide an integrated and accurate picture of the operational capability; and 3) Supports execution of joint critical operational activities.

Developers must ensure that the system's solution architecture products 1) Are developed in accordance with the DoDAF, 2) Describe the internal and external information flows in sufficient detail to enable the assessment of interoperability requirements, 3) Show linkage to parent enterprise architectures (where available), 4) Fit within Component and DoD Capability Portfolio Management architecture descriptions (if they exist), and 5) Are registered and maintained in the DoD Architecture Registry System and DISRonline (as appropriate).

Terminology used in this guidebook:

- The term *solution architecture* refers to the architecture of the system (i.e., the "solution").
- The term *solution architecture products* refers to the diagrams that describe the operational and technical requirements for the system to exchange data using its interfaces.

As part of interoperability testing, Joint Interoperability Test Command (JITC) testers must verify that the system's solution architecture meets all joint critical IE requirements contained in the Joint Staff (JS)-certified NR-KPP. All IE requirements should be represented in the system's solution architecture products as part of the JS-certified requirements documents.

REQUIREMENTS ANALYSIS

Architecture Products. The system's solution architecture products describe the operational and technical requirements for the system to exchange data using its interfaces.

The DoDAF defines how a system's solution architecture should be represented using graphical and textual models. The DoDAF provides a common language for comparing and integrating architectures across Service, joint, and multi-national boundaries. The DoDAF Version (V) 2.0 is the most current version as of 28 May 2009.

The DoDAF V1.5 and DoDAF V2.0 view/viewpoint requirements contain differences in terminology and focus. Consequently, the solution architecture views/viewpoints available to testers will vary depending on the DoDAF version in effect at the time of publication of the system's requirements documents (i.e., Capability Development Document (CDD), Capability Production Document (CPD), Information Support Plan (ISP), or Tailored Information Support Plan (TISP)).

DoDAF V2.0 Terminology:

- *Models* are the templates for organizing and displaying data.
- *Views* are models populated with system specific data.
- *Viewpoints* are models/views that would be in a system's ISP, CPD, or CDD.

DoDAF Versions. The DoDAF V1.5 architecture viewpoints are organized under four models and the DoDAF V2.0 architecture viewpoints are organized under eight models. The DoDAF V2.0 accommodates models created under DoDAF V1.5 and includes new models to meet user requirements.

Table 1-1 shows the models from each DoDAF version and their relationship.

Table 1-1. Comparison of DoDAF Models

DoDAF V1.5	DoDAF V2.0
Architecture View (AV)	All Viewpoint (AV) Overarching aspects of architectural context that relate to all models.
Operational View (OV)	Operational Viewpoint (OV) Conveys operational scenarios, processes, activities, and requirements.
Systems and Services View (SV)	Services Viewpoint (SvcV) Conveys the performers, activities, services, and their exchanges providing for, or supporting, DoD functions.
	Systems Viewpoint (SV) Conveys the legacy systems or independent systems, their composition, interconnectivity, and context providing for, or supporting, DoD functions.
Technical View (TV)	Standards Viewpoint (StdV) Conveys applicable operational, business, technical, and industry policy, standards, guidance, constraints, and forecast.
No DoDAF V1.5 relationship	Capability Viewpoint (CV) – New Conveys the capability requirement, delivery timing, and deployed capability.
No DoDAF V1.5 relationship	Data and Information Viewpoint (DIV) – New Conveys the data relationships and alignment structures in the architecture content.
No DoDAF V1.5 relationship	Project Viewpoint (PV) – New Describes the relationships between operational and capability requirements and the various projects being implemented; details dependencies between capability management and the Defense Acquisition System process.
LEGEND:	
DoDAF	DoD Architecture Framework
DoD	Department of Defense
	V
	Version

The DoDAF V2.0 shifts the emphasis from "required models" to "fit-for-purpose" or user-defined views. As per DoDAF V2.0, programs have the option to choose architectural models that suit their program needs ("fit for purpose").

The DoDAF V2.0 focuses on architectural data rather than products. Testers must identify the technical information needed for testing IEs, whether it appears in a DoDAF model or not. The CJCSI 6212.01E identifies the required DoDAF models for each requirements document.

Table 1-2 shows the DoDAF models that are typically used for displaying the required system requirements information.

Table 1-2. DoDAF Models and Descriptions

Model Name	Description	Purpose
Architectural View (AV)-1 Overview and Summary Information	This model depicts the scope, purpose, intended users, system environment, and analytical findings.	The AV-1 includes assumptions, constraints, and limitations that may affect high-level decisions relating to an architecture-based work program.
Operational View (OV)-1 High-Level Operational Concept Graphic	This model provides a high-level graphical/textual description of operational concept.	The OV-1 provides a graphical depiction of what the architecture is about and an idea of the players and operations involved.
OV-2 Operational Resource Flow (defined in DoDAF V1.5 as the "Operational Node Connectivity Description")	This model provides a description of the Resource Flows between operational activities.	The OV-2 can be used to show flows of funding, personnel, and materiel in addition to information.

Table 1-2. DoDAF Models and Descriptions (continued)

Model Name	Description	Purpose
OV-3 Operational Resource Flow Matrix (defined in DoDAF V1.5 as the Operational Information Exchange Matrix)	This model provides a description of the resources exchanged and the relevant attributes of the exchange.	This model is initially constructed from the information contained in the OV-2. JITC focus is on the information exchanged between nodes and the attributes of that exchange.
OV-5b Operational Activity Model (defined as OV-5 in DoDAF V1.5)	This model consists of model overlays that show capabilities, operational activities, and relationships among activities, inputs, and outputs.	This model describes the operational, business, and defense portion of the intelligence community activities. The OV-5 and OV-2 are complements of each other and should normally be developed together.
OV-6c Operational Event-Trace Description	This is one of three models used to describe the operational activity. It traces actions in a scenario or sequence of events.	The information content of messages in an OV-6c may be related with the Resource Flows in the OV-3 and OV-5b and information entities in the Data and Information Viewpoint (DIV)-2.
Services Viewpoint (SvcV)-1 Services Context Description	The identification of services, service items, and their interconnections.	The SvcV-1 links together the operational and services architecture viewpoints by depicting how resources are structured and interact to realize the logical architecture specified in an OV-2.
SvcV-2 Services Resource Flow Description	A description of Resource Flows exchanged between services.	This model can show which ports are connected, the producing services that the port belongs to, the services that the Service Resource Flows are consumed by, and the definition of the Service Resource Flow in terms of the physical/logical connectivity.
SvcV-3a Systems-Services Matrix	This model describes the relationships among or between systems and services in a given architectural description.	The SvcV-3a provides a tabular summary of the system and services interactions specified in the SvcV-1 for the Architectural Description. This model can be useful in support existing systems that are transitioning to provide services.
SvcV-4 Services Functionality Description (defined as SV-4b in DoDAF V1.5)	This model is a behavioral diagram showing the functions performed by services and the service data flows among service functions (activities).	The SvcV-4 is the behavioral counterpart to the SvcV-1.
SvcV-5 Operational Activity to Services Traceability Matrix (defined as SV-5c in DoDAF V1.5)	This model maps services (activities) back to operational activities (activities) in a matrix.	The SvcV-5 addresses the linkage between service functions described in SvcV-4 and Operational Activities specified in OV-5a or OV-5b.
SvcV-6 Services Resource Flow Matrix	This model provides details of service Resource Flow elements being exchanged between services and the attributes of that exchange.	This model is useful in support of net-centric implementation of services. The SvcV-6 is the physical equivalent of the logical OV-3. Each Service Resource Flow exchange listed in the SvcV-6 table should be traceable to at least one Operational Resource Flow exchanged listed in the corresponding OV-3 and these, in turn, trace to OV-2.
Standards Viewpoint (StdV)-1 Standards Profile (defined as Technical View (TV)-1 in DoDAF V1.5)	This model provides a listing of standards that may also apply to other systems viewpoint elements in a given architecture.	The protocols referred to Resource Flow descriptions (Systems View (SV)-2 or SvcV-2) are examples of standards and should be included in the StdV-1 listing.

Table 1-2. DoDAF Models and Descriptions (continued)

Model Name	Description	Purpose
StdV-2 Standards Forecast (defined as TV-2 in DoDAF V1.5)	This model is a description of emerging standards and the potential impact on other system viewpoint elements, within a set of time frames.	The StdV-2 is a detailed description of emerging standards relevant to the systems, operational, and business activities covered by the Architectural Description. The forecast for evolutionary changes in the standards need to be correlated against the time periods mentioned in the SV-8 Systems Evolution Description, SvcV-8 Services Evolution Description, SV-9 Systems Technology & Skills Forecast, and SvcV-9 Services Technology and Skills Forecast viewpoints.
SV-1 Systems Interface Description	This model shows identification of system nodes, systems, and system items and their interconnections, within and between nodes.	The SV-1 links together the operational and systems architecture models by depicting how resources are structured and interact to realize the logical architecture specified in an OV-2. Note that Resource Flows between systems may be further specified in detail in SV-2 Systems Resource Flow Description and SV-6 Systems Resource Flow Matrix.
SV-2 Systems Resource Flow Description (defined as a Communications Description in DoDAF V1.5)	This model shows Resource Flows exchanged between systems depicted by system nodes, systems, and system item and their related communications lay-downs.	The SV-2 viewpoint shows which ports are connected, the systems that the ports belong to and the definition of the System Resource Flow in terms of the physical connectivity. Any protocol referred to in a SV-2 diagram needs to be defined in the StdV-1.
SV-4 Systems Functionality Description	This model shows functions performed by systems and the system data flows among system functions.	This model is used to describe task workflow, identify functional system requirements, functionally decompose systems, and relate human and system functions. SV-4 is the behavioral counterpart to SV-1. Functions are related to operational activities of OV-5a.
SV-5a Operational Activity to Systems Function Traceability Matrix (defined as SV-5 in DoDAF 1.5)	This model maps system functions to capabilities or system functions to operational functions.	This model is used to trace functional system requirements to user requirements, trace solution options to requirements and identify overlaps and gaps. SV-5a ties together the logical specification in the OV-5a with the physical specification of the SV-4.
SV-6 Systems Resource Flow Matrix (defined as the Data Exchange Matrix in DoDAF V1.5)	This model provides the Resource Flow criteria and technical attributes for each information exchange. These include the physical characteristics of the Resource Flows depicted in the OV-3.	Each system Resource Flow exchange listed in the SV-6 table should be traceable to at least one operational Resource Flow exchanged listed in the corresponding OV-3. These, in turn, trace to operation Resource Flows in the OV-2.
DIV-1 Conceptual data Model	This model provides required high-level data concepts and their relationships.	The DIV-1 describes information or data of importance to the business whereas the DIV-3 describes data relevant at the system-level. A DIV-1 may be necessary for interoperability when shared information syntax and semantics form the basis for information systems interoperability or when an information repository is the basis for integration and interoperability among business activities and between capabilities.

Table 1-2. DoDAF Models and Descriptions (continued)

Model Name	Description	Purpose
DIV-2 Logical Data Model (defined as OV-7 in DoDAF V1.5)	This model provides the documentation of the data requirements and structural business process (activity) rules.	The DIV-2 provides a common dictionary of data definitions to consistently express models wherever logical-level data elements are included in the description. The DIV-2 is a generalized formal structure in computer science. It directly reflects the paradigm or theory-oriented mapping from DIV-1 to the DIV-2.
DIV-3 Physical Data Model (defined as SV-11 in DoDAF V1.5)	This model provides the physical implementation format of the Logical Data Model entities; e.g., message formats, file structures, physical schema.	The DIV-3 is an implementation-oriented viewpoint that is used in the Systems Viewpoint and Services Viewpoint to describe how the information requirements represented in DIV-2 Logical Data Viewpoint are actually implemented.
Capability View (CV)-6 Capability to Operational Activities Mapping	This model provides a mapping between the capabilities and the operational activities that those capabilities support.	The CV-6 shows which elements of a capability may be used in support of specific operational activities by means of a mapping matrix. It provides the interface between Capability and Operational Models.
CV-7 Capability to Services Mapping	This model provides a mapping between the capabilities and the services that these capabilities enable.	The CV-7 provides a bridge between capability analyzed using CVs and services analyzed using SvcVs. Specifically, it identifies how services can be performed using various available capability elements. It is similar in function to the SV-5a, which maps system functions to operational activities.
LEGEND: DoDAF Department of Defense Architecture Framework V Version JITC Joint Interoperability Test Command		

Determine Requirements. The system's solution architecture products describe the technical parameters and system design details for the system interfaces and corresponding IEs. The mission requirements, capabilities, functionality, and operational activities (as they relate to the interfaces and corresponding IEs) should be traceable throughout the system viewpoints. The JITC Joint Capabilities Integration and Development System Document Review Checklist outlines the traceability relationships between system architecture viewpoints to be examined. The JITC is promoting the Integrated Architecture Traceability Matrix (IATM) methodology as the recommended standardized approach to identify the threshold and objective interoperability requirements for a system's solution architecture. The IATM methodology, explained in detail in Appendix C, supports NR-KPP requirements analysis, risk analysis, and Test and Evaluation strategy development.

Verify System Capabilities and Interfaces Support Mission Activities. The JITC reviewers must determine that the system capabilities shown in the SV-4s and the interfaces shown in the SV-6s support the mission activities shown in the OV-5 (Appendix C provides the methodology for IATM development). For example, the system may have a capability, "Provide Blue Force (BF) Location Auto Track Feed," with corresponding interfaces "Force XXI Battle Command-Brigade and Below (FBCB2)" and "Blue Force Tracking (BFT) Satellite Communications (SATCOM),"

shown in the program's SV-6. These all support the mission activity, "Understand BF Resource States," shown in the program's OV-5.

Identify the Joint Critical Interfaces and Corresponding IE Requirements. The next step in requirements analysis is to identify the joint critical interfaces and corresponding IE requirements. Joint critical interfaces are in the viewpoints listed in Table 1-2; testers may also determine joint critical interfaces from the narrative sections of the CPD, ISP, or TISP. Testers must identify all of the IE requirements (technical criteria) for the joint critical interfaces. The interoperability criteria include metrics for performance attributes such as timeliness, accuracy, completeness, and usability. The tester needs to extrapolate additional technical criteria and parameters needed to test the IEs. For example, the OV-5, OV-6c, and SV-4 identify how mission requirements, system capabilities, functionality, and operational activities relate to the interfaces and corresponding IEs defined in the SV-6. The OV-3 and SV-6 define relevant attributes and interoperability criteria for the interfaces and IEs.

Compliance with the threshold value of the NR-KPP Compliance Statement requires that all joint critical interfaces are operationally effective. The JITC must, therefore, assess all joint critical interfaces. However, the NR-KPP Compliance Statement states that, objectively, JITC should assess all IEs as resources and time permit.

TEST PLANNING AND EXECUTION

The JITC leverages all program lifecycle testing for data collection. The tester can accept relevant Developmental Test, Operational Assessment, and Operational Test procedures and data for Interoperability Test Certification. For example, the sample in Table 1-6 combines operational assessment data and interoperability test data samples for the total number of data transfers for each IE.

Interoperability testing of IEs must be conducted on a production-representative system in an operationally realistic environment. This means that the network configuration, loading conditions, Information Assurance posture, and interfacing systems must represent, accurately and completely, the environment in which the system will be fielded. If the test environment does not provide a close approximation of the operational environment, then the test may not reveal all interoperability issues.

The tester must perform end-to-end testing of the paths the IEs take through all interfaces. The tester may develop Measures of Effectiveness (MOEs) and Measures of Performance (MOPs) for each interface that are based on performance criteria as defined in the solution architecture viewpoints. The MOPs for each IE are usually in terms of accuracy, completeness, timeliness, and usability. The MOE is an accumulation of the associated MOPs for each interface. The MOEs can be based on each interface or on data transmission type. Not all programs formalize their test methodologies and measures of success with MOEs and MOPs; the interface and IE requirements are addressed directly in an IE requirements table.

For example, consider an interface that exchanges situational awareness data between FBCB2 and the system being assessed. The FBCB2 interface’s IEs might have the following MOE and MOPs.

MOE 1. FBCB2 Interface:

- **MOP 1.** Percentage of IEs with FBCB2 that are accurate (Criterion: 95 percent)
- **MOP 2.** Percentage of IEs with FBCB2 that are complete (Criterion: 95 percent)
- **MOP 3.** Percentage of IEs with FBCB2 that are within the time requirement (Criterion: 95 percent within 60 seconds)
- **MOP 4.** Percentage of IEs with FBCB2 for which the user rated the data usable (support mission requirements) (Criterion: No user ratings of mission failure due to IE failure)

Table 1-3 shows how a test plan might present the performance criteria for each IE in a structure that relates the performance criteria to the IEs and corresponding interfaces.

Table 1-3. Sample IE Requirements Derived from JS-Certified Solution Architecture Viewpoints

Interface	Information Exchanges	Performance Criteria (IE Requirements)			
		Accuracy	Completeness	Timeliness	Usability
FBCB2	Sends request for situational awareness data.	95%	95%	95% within 60 sec	100%
	Receives situational awareness data.	95%	95%	95% within 60 sec	100%
	Sends situational awareness resource state data.	95%	95%	95% within 60 sec	100%
BFT SATCOM	Sends request for resource data.	95%	95%	95% within 60 sec	100%
	Receives resource data.	95%	95%	95% within 60 sec	100%
LEGEND:					
BFT	Blue Force Tracking	JS	Joint Staff		
FBCB2	Force XXI Battle Command-Brigade and Below	SATCOM	Satellite Communications		
IE	Information Exchange	sec	second(s)		

Testers must collect enough samples of each IE to verify the performance criteria at the confidence level provided in the requirements documents (a methodology for determining sample sizes and confidence levels is currently in development). If any collected data does not meet the criteria for accuracy, completeness, timeliness, or usefulness, the tester must interview the operational users to determine whether the failure had a critical impact on the mission. An interface is operationally effective when each of the IEs satisfies performance criteria and has no performance failures with a user-assigned critical operational impact.

Testers must collect, at a minimum, the following data elements for each of the IEs:

- Name and version number of the sending system and the receiving system.
- Number of samples exchanged for each IE for the specified time period of testing.
- Usability ratings provided by system users.
- User impact assignment and statement for any failures.

The following are additional data elements that may apply to a system:

- Time received and sent for each sample, and whether time in transit met or did not meet the program requirement threshold.
- Accuracy and completeness results of each comparison of transmitted and received data. Pass or fail result for each data comparison.
- If applicable, the relationship between this IE and any standards conformance testing and/or Global Information Grid (GIG) Technical Profile requirements.

The data collection forms should have formats that allow for recording the individual data elements during testing. For example, the form will have entry spaces for recording transaction time sent and time received. This is used to determine the time-in-transit data element and successful completion of the test activity. The test incident report forms will have entries to log the specific test event and the failure details.

Tables 1-4 and 1-5 show samples of how the interfaces and corresponding IEs and data collection information can be presented. The presentation needs will vary by system complexity.

Table 1-4. Information Exchange Matrix

Data Exchange Name and Process	Process Description	Producer/ Sender ID	Consumer/ Recipient ID	Protocol or Format or Media Type	Frequency Timeliness	Accuracy & Completeness
IE 1 Load Orders Shipment Planning Information	Information about orders provided to DPMS by DSS.	DSS Pre-Optimization Processing	DPMS (Manugistics Networks Transport) Load Information.	Digital ASCII data – MQ Series over TCP/IP Flat file, fixed length fields.	Every 2 hours or prior to optimization run.	95%

Table 1-4. Information Exchange Matrix (continued)

Data Exchange Name/Process	Process Description	Producer/ Sender ID	Consumer/ Recipient ID	Protocol or Format or Media Type	Frequency Timeliness	Accuracy & Completeness
IE 2 Load Location Shipment Planning Information	Address/Location information, including but not limited to, shippers, consignees, depots, military bases, and warehousing facilities.	DSS Pre-Optimization Processing	DPMS (Manugistics Networks Transport) Load Information.	Digital ASCII data – MQ Series over TCP/IP Flat file, fixed length fields.	As needed, event-driven basis.	95%
IE 3 Update to Tendered Shipment Planning Information	This is the manual entry by DDC personnel indicating that a vendor has accepted the transportation plan and will be tendered (offered) as planned.	DSS Send Intent to Tender to DPMS	DPMS (Manugistics Networks Transport) Change Status to Tendered.	Digital ASCII data – MQ Series over TCP/IP Flat file, fixed length fields.	As needed, event-driven basis.	95%
LEGEND:						
ASCII	American Standard Code for Information Interchange	IE	Information Exchange			
DDC	Destination Distribution Center	MQ	Message Queue			
DPMS	Defense Property Management System	TCP/IP	Transmission Control protocol/Internet Protocol			
DSS	Defense Shipping Service					

Table 1-5. Information Exchange Test Conditions and Data

Information Exchange	Interface	Operational Mission Area/IE Description	Test Conditions and Data Collection Details
IE 1 Load Orders	DSS-DPMS	Shipment Transportation Planning capability. Second Destination Distribution Center Order data provided to DPMS (Manugistics Networks Transport) by DSS.	Orders will be optimized for distribution centers and optimized shipment transportation plans produced for the orders. Minimum Sample Size: Verify accurate order information on 32 customer orders within optimized shipment plans for three distribution centers.
IE 2 Load Locations	DSS-DPMS	Shipment Transportation Planning Capability. Address and location information for Second Destination Distribution Center Orders from DSS provided to DPMS (Manugistics Networks Transport).	Address and location information is included on individual orders within the shipment plan and includes, but is not limited to, shippers, consignees, distribution centers, military bases, and warehousing facilities. Minimum Sample Size: Verify accurate address and location information is sent and received on 32 orders from shipment plans generated during optimization process for second destination orders.
IE 3 Update DPMS to Tendered	DSS-DPMS	Shipment Transportation Planning Capability. Manual process by DDC personnel in DSS that sends updated tendered status for Second Destination Distribution Center Order to DPMS (Manugistics Networks Transport).	This is mostly a manual input process by DDC personnel in DSS, indicating that a vendor has accepted the transportation plan and that it is now alright to tender the shipment to the carrier. The DSS changes status and updates DPMS that the shipment is acceptable to vendor and will be tendered as planned. Notification from DSS updates status to "Tendered" within DPMS. Minimum Sample Size: Verify accurate tendered status updates on 32 vendor orders in DPMS and DSS.
LEGEND:			
DPMS	Defense Property Management System	IE	Information Exchange
DSS	Defense Shipping Service		

REPORTING

During test planning, the testers should consider how the report will present the test results. According to the "JITC Guide to Test Documentation," June 2008, JITC requires that the test report provide the following for each interface and IE requirement:

- Performance criteria (including threshold levels) for timeliness, accuracy, completeness, and usability
- IE identification information and associated format (e.g., Link 16, Hypertext Markup Language (HTML), Joint Photographic Experts Group (JPEG))
- Incident report for each failure with user assigned impact rating

Tables 1-6 and 1-7 show sample results tables for reports.

Table 1-6. Information Exchange Interoperability Data Sample

IE #	Number of Data Transfer Samples		Data Sample Transfer Results			Percent of Accurate Samples Successfully Transferred	Problem Report
	Operational Assessment Data Samples	Interoperability Test Data Samples	# of Successful Data Transfers	# of Samples with Accurate Data	# of Samples with Timely Data Transfers		
1	118	61	179	179	179	100%	None
2	118	61	179	179	179	100%	None
3	118	61	179	179	179	100%	None
LEGEND:							
IE Information Exchange							

Table 1-7. Information Exchange Data Summary

IE #	Name and Description	Producer/Sender ID	Consumer/Recipient ID	Samples Collected	Percent Successful	Status and Remarks
1	Load Order Information. Shipment Transportation Planning capability. Second Destination Distribution Center Order data provided to DPMS (Manugistics Networks Transport) by DSS.	DSS	DPMS	179	100% compliance	Met
2	Load Locations. Shipment Transportation Planning Capability. Address and location information for Second Destination Distribution Center Orders from DSS provided to DPMS (Manugistics Networks Transport).	DSS	DPMS	179	100% compliance	Met

Table 1-7. Information Exchange Data Summary (continued)

IE #	Name and Description	Producer/Sender ID	Consumer/Recipient ID	Samples Collected	Percent Successful	Status and Remarks
3	Update to Tender. Shipment Transportation Planning Capability. Manual process by DDC personnel in DSS that sends updated tendered status for Second Destination Distribution Center Order to DPMS (Manugistics Networks Transport).	DSS	DPMS	179	100% compliance	Met
LEGEND:						
DDC	Destination Distribution Center		ID	Identification		
DPMS	Defense Property Management System		IE	Information Exchange		
DSS	Defense Shipping Service					

Table 1-8 shows the criteria for the requirements being Met or Not Met. When determining whether the system passed or failed, the testers should use the following threshold and objective level definitions to show the status in the Joint Interoperability Certification Memorandum.

Table 1-8. Solution Architecture Criteria Table

Status	Threshold	Objective
Met	Met all critical Information Exchange (IE) requirements (for a given interface, between two given systems, or IEs (data)).	Met all IE requirements (for a given interface, between two given systems, or IEs (data)).
Partially Met	Met some but not all critical IE requirements with no discrepancies identified with a critical operational impact (for a given interface, between two given systems, or IEs (data)).	Met some but not all IE requirements and/or all net-centric requirements with no discrepancies identified with a critical operational impact (for a given interface, between two given systems, or IEs (data)).
Not Met	Tested and failed to meet a critical IE requirement or other IE requirement resulting in a critical operational impact (for a given interface, between two given systems, or IEs (data)).	Tested and failed to meet any IE requirement or other IE requirement resulting in a critical operational impact (for a given interface, between two given systems, or IEs (data)).
Not Tested	No critical IEs were tested.	No IEs were tested.

The Engineering and Policy Branch of the Strategic Planning and Engineering Division provides specific reporting formats in the JITC Instruction 380-50-02, "Interoperability and Standards Conformance Test and Evaluation and Certification;" JITC Instruction 210-85-01, "Documentation of Test and Evaluation Activities;" and the JITC Guide to Test Documentation. The Joint Interoperability Certification Memorandum reports the results of the interfaces IE evaluation. The following tables are from the Joint Interoperability Certification Memorandum and show the IE status and interface status, providing the overall IE testing results.

Table 1-9 is an example of the IE status included in the Certification Testing Summary of the Joint Interoperability Certification Memorandum. Table 1-10 shows the appropriate status for different interface requirement success or failure conditions.

Table 1-9. Information Exchange Requirements and Status

IE #	Name	Producer/ Sender ID	Consumer/ Recipient ID	Critical	I#	Rqmts	Status	Remarks
IE1	Load orders	DSS	DPMS	Yes	1	Accurate Complete Timely Usable	Met	100% compliance
IE2	Load locations	DSS	DPMS	Yes	1	Accurate Complete Timely Usable	Met	100% compliance
IE3	Update to tenders	DSS	DPMS	Yes	1	Accurate Complete Timely Usable	Met	100% compliance
LEGEND:								
DPMS	Defense Property Management System			ID	Identification			
DSS	Defense Shipping Service			IE	Information Exchange			
I	Interface			Rqmts	Requirements			

The IEs identified in Table 1-9 for each interface are combined into an overall status for each interface as shown in Table 1-10. The overall status for the DoD Shipping Services interface is Met because all 3 applicable IEs are Met with 100-percent compliance.

After testing is completed, testers will analyze the system performance data and assess the impact that the overall system performance could have on mission accomplishment. Factors to consider when analyzing the impact of failures include:

- Frequency of failures versus volume of traffic across the interface
- Severity of the failure/time to repair
- Importance of the affected data to the mission
- User satisfaction with the system versus alternatives

Table 1-10 is an example of the interface requirements and status included in the Joint Interoperability Certification Memorandum and/or test report.

Table 1-10. Example of the Interface Requirements and Status Table

Interface #	Name	Version	Critical	KIP/GESP	Requirements	Status	Remarks
1	DSS	1.3	Yes	N/A	ISP	Met	100% compliance
LEGEND:							
DSS	Defense Shipping Service			KIP	Key Interface Profile		
GESP	Global Information Grid Enterprise Services Profile			N/A	Not Applicable		
ISP	Information Support Plan						

Table 1-11 is the NR-KPP status table in the Joint Interoperability Certification Memorandum and/or test report and provides the overall status of the Solution Architecture requirements. The Solution Architecture status row in this table is the overall compliance status of the interfaces. If all interfaces successfully met the IE requirements, then the overall status is Met. A failure with a user-assigned critical impact would result in the interface being identified as Not Met, resulting in the Solution Architecture element being Not Met. The applicable items for the Solution Architecture element are highlighted in the table.

Table 1-11. NR-KPP Status – Solution Architecture

INTEROPERABILITY REQUIREMENT	STATUS		REMARKS
	Threshold	Objective	
1. Solution Architectures; i.e., operationally effective information exchanges	<i>Status (i.e., Met)</i>	<i>Status (i.e., Not Tested)</i>	Degree of compliance with the requirements and expected operational impact. (i.e., Tested to the Threshold: All joint critical interfaces, not all of the interfaces for this system. There were no failures with a major or critical impact to the users. Two minor failures occurred and evaluated by the users having no impact to their mission accomplishment.)
2. Net-Centric Data and Services Strategy	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
a. Data Sharing Requirements	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
b. Service Sharing Requirements	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
3. GTG	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
DISR	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
GESP/KIP	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
4. IA	<i>Status</i>	<i>Status</i>	Statement that testing was performed in the approved IA configuration. Statement that the DAA issued an IATO/ATO, including date of issue and termination date.
5. Supportability			
a. Spectrum certification	<i>Status</i>	<i>Status</i>	DD1494 Status and date.
b. E3 Program	<i>Status</i>	<i>Status</i>	E3 Test Report, EMI Test Report, or something similar and date.
c. SAASM	<i>Status</i>	<i>Status</i>	If SAASM compliant-N/A. If not SAASM compliant, waiver and date.
d. JTRS	<i>Status</i>	<i>Status</i>	If JTRS compliant-N/A. If not JTRS compliant, waiver and date.
6. Other (as required)	<i>Status</i>	<i>Status</i>	
LEGEND:			
ATO	Authorization to Operate	GTG	GIG Technical Guidance
DAA	Designated Accrediting Authority	IA	Information Assurance
DISR	Department of Defense Information Technology Standards Registry	IATO	Interim Authorization to Operate
E3	Electromagnetic Environmental Effects	JTRS	Joint Tactical Radio System
EMI	Electromagnetic Interference	KIP	Key Interface Profile
GESP	GIG Enterprise Services Profile	N/A	Not Applicable
GIG	Global Information Grid	NR-KPP	Net-Ready Key Performance Parameter
		SAASM	Selective Availability Anti-Spoofing Module

CHAPTER 2 – NET-CENTRIC DATA AND SERVICES STRATEGY

NET-READY KEY PERFORMANCE PARAMETER STATEMENT

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E defines the Data and Services Strategy (DSS) element of the Net-Ready Key Performance Parameter (NR-KPP) as:

"...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..."

CJCSI 6212.01E

Programs delivering Information Technology (IT) systems and National Security Systems (NSS) must meet the DSS requirements, Department of Defense (DoD) Directive 8320.02, and the DoD Information Enterprise Architecture Version 1.1. The policies in these documents comprise the DoD net-centric policy and form the basis for the DSS element.

Each net-centric capability, system, or service seeking Joint interoperability Test Command (JITC) interoperability certification must meet applicable net-centric data and service sharing requirements.

DSS REQUIREMENTS

The DSS requirements fall into two categories, net-centric data sharing and net-centric service sharing. Tables 2-1 and 2-2 list the net-centric data sharing and net-centric service sharing requirements based on DoD net-centric policy.

Table 2-1. Data Sharing Requirements

Requirement	Source of Requirement
Data is Visible	
<u>Post discovery metadata in an Enterprise Catalog</u> - 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.	Chairman of the Joint Chiefs of Staff (CJCSI) 6212.01E, Enclosure (Encl) E, paragraph (para) 3.b.(2)(b) <u>4.a.(1)</u> , page (p.) E-7 DoD Net-Centric Data Strategy, para 3.1.2, p. 11 DoD Directive (DoDD) 8320.02, para 4.3, p. 2
<u>Use appropriate keywords for discovery</u> - Discovery keywords should reflect common user terms, be appropriate for mission area or data type, be understandable, and conform with Metadata Registry (MDR) requirements that map back to Community of Interest (COI)-identified mission data.	CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.c.(1)

Table 2-1. Data Sharing Requirements (continued)

Requirement	Source of Requirement
Data is Accessible	
<u>Post data to shared space</u> - Data asset is available in a shared space, i.e., a space that is accessible to multiple end users.	CJCSI 6212.01E, Encl E, para 3.b.(2)(b) <u>4.b.(1)</u> DoDD 8320.02, para 4.3, p. 2
<u>Provide access policy</u> - If data is not accessible to all users, a written policy on how to gain access is available and accurate.	CJCSI 6212.01E, Encl E, para 3.b.(2)(b) <u>4.b.(2)</u>
<u>Provide serving (access) mechanism</u> - Shared space provides serving (access) mechanisms for the data, i.e., a service provides users with access to the data.	DoD Net-Centric Data Strategy 3.1.1, p. 11
<u>Publish active link to data asset</u> - The Enterprise Catalog DDMS entry contains an active link (e.g., Uniform Resource Identifier (URI)) to the data asset.	CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.b.(3)
Data is Understandable	
<u>Publish semantic and structural metadata</u> - Semantic and structural metadata are published in the Enterprise Catalog.	CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.c.(1)
<u>Register data artifacts in DoD MDR</u> - eXtensible Markup Language (XML) Schema Definitions (XSDs), XML instances, data models (e.g., entity relationship diagrams) and other appropriate artifacts are registered in the DoD MDR.	CJCSI 6212.01E, Encl E, para 3.b.(2)(b) <u>4.a.(3)</u> , p. E-7 DoD Net-Centric Data Strategy, para 3.1.4, p. 13
Data is Interoperable	
<u>Base vocabularies on Universal Core (UCore)</u> - Semantic vocabularies reuse elements of the Ucore standard.	CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.e.(1) DoD Information Enterprise Architecture (IEA) 1.1, Data and Services Deployment (DSD) Business Rules, p. 11
<u>Comply with COI data-sharing agreements</u> - Semantic and structural metadata conform to interoperability agreements promoted through communities; e.g., COI.	DoDD 8320.02, para 4.7, p. 3
<u>Conform to DDMS</u> - All metadata, including record-level database tagging and in-line document tagging, complies with DDMS.	DoD Net-Centric Data Strategy 3.6.4, p. 17
Data is Trusted	
<u>Provide information assurance and security metadata</u> - 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).	DoDD 8320.02, para 4.5, p. 2 DoD Net-Centric Data Strategy 3.5.1, p. 16

Table 2-2. Service Sharing Requirements

Requirement	Source of Requirement
Services are Visible	
<p><u>Publish a description of the service or access mechanism</u> - Descriptions (metadata) for the service or access mechanism are published in an enterprise service registry, e.g., the NCES Service Registry.</p>	<p>DoD IEA 1.1, Data and Services DSD Business Rules, p.11 DoD Net-Centric Services Strategy, para 3.1, p. 6 DoD 8320.02-G, para C4.3.2.4, p. 28</p>
<p><u>Comply with enterprise-specified minimum service discovery requirements</u> - 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.</p>	<p>DoD 8320.02-G, para C4.2.2.5.2, p. 25</p>
Services are Accessible	
<p><u>Provide an active link to the service in the enterprise catalog</u> - Active link (e.g., URI) to the specified service is included in the enterprise catalog metadata entry (i.e., metacard) for the specified service.</p>	<p>CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.b.(3), p. E-8</p>
<p><u>Provide an active link to the service in the NCES Service Registry</u> - URIs as the operational end points for services shall be registered in the NCES Service Registry by referencing the Web Service Description Language (WSDL) (that is in the MDR).</p>	<p>CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.a.(4), p. E-7</p>
Services are Understandable	
<p><u>Publish a description of the service or access mechanism to the NCES Service Registry</u> - Metadata for the service or access mechanism are published in the NCES Service Registry.</p>	<p>CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.c.(2), p. E-8 DoD Net-Centric Services Strategy, para 3.1, p. 6 DoD 8320.02-G, para C4.3.2.4, p. 28</p>
<p><u>Publish service artifacts to DoD MDR</u> - WSDL documents and other appropriate artifacts are registered in the DoD MDR.</p>	<p>CJCSI 6212.01E, Encl E, para 3.b.(2)(b) 4.a.(3), p. E-7</p>
<p><u>Provide service specification or Service Level Agreement (SLA)</u> - A service specification or SLA exists for services and data access mechanisms.</p>	<p>DoD Net-Centric Services Strategy 3.1, p. 7 DoD IEA 1.1 Global Principles, p.5</p>
Services are Trusted	
<p><u>Operate services in accordance with SLA</u> - The service meets the performance standards in the SLA.</p>	<p>DoD IEA 1.1 Global Principles, p.5</p>
<p><u>Include security mechanisms or restrictions in the service specification</u> - The service specification describes security mechanisms or restrictions that apply to the service.</p>	<p>DoD Net-Centric Services Strategy 3.1, p. 7</p>
<p><u>Enable continuity of operations and disaster recovery for services</u> - The service has a defined and functional Continuity of Operations Plan.</p>	<p>DoD IEA SI Business Rules, p. 16</p>
<p><u>Provide Network Operations (NetOps) Data (NetOps Agility)</u> - 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.</p>	<p>DoD IEA 1.1, NetOps Agility (NOA) Principles and Business Rules, p. 25 DoD IEA 1.1, NetOps Agility Business Rules: Situational Awareness (NOAR) 06, p. A-6</p>
Use of Core Enterprise Services (CES)	
<p>- CES are used in accordance with DoD Chief Information Officer mandates.</p>	<p>DoD Net-Centric Services Strategy para 3.2, p. 8</p>

REQUIREMENTS ANALYSIS

Because not all of the DSS requirements will apply, the JITC testers must analyze the Joint Staff (JS)-certified and DSS requirements to develop an NR-KPP assessment plan. During this requirements analysis, JITC testers must review documentation, identify enterprise-level shared data and services, and determine the applicability of net-centric requirements.

Review Documentation. The JITC begins its requirements analysis when JS J-6, through Defense Information Systems Agency (DISA), tasks JITC to review the capabilities documents. This package should contain DoD Architecture Framework (DoDAF) viewpoints and Exposure Verification Tracking Sheets (EVTSSs). If these are not included with the JS-certified requirements documents, the tester must request that the Program Manager (PM) or Point of Contact (POC) provide supporting DoDAF products (e.g., an Operational Activity Model) and other architecture descriptions. For programs with limited documentation, testers should request System Design Requirements, Standards Support Documents, segment specifications, Final Requirements Document, etc., from the POCs.

To assess the DSS element, the JITC testers will also require all documents that explain or clarify the data or service sharing methods. A complete package must include the following artifacts, as appropriate:

- Data structures and models (e.g., entity relationship diagrams)
- Data dictionaries and/or vocabularies
- Data schemas (i.e., eXtensible Markup Language schema definitions)
- Documentation for data access mechanisms (to include link(s) to content data)
- Web Service Descriptor Language files
- Web Application Description Language files
- eXtensible Stylesheet Language Transformations files
- Community of Interest (COI)-approved or capability-specific vocabulary lists
- Taxonomy/ontology descriptions
- User guides and readme files as appropriate
- Specific version information for all artifacts

The JITC testers do not currently receive any of these artifacts. Nevertheless, they are necessary for DSS assessment. Testers should request these items from the program office as well as a manifest listing of the items and their explicit versions and revision dates. The JITC testers should compare received artifacts against the architecture product viewpoints to identify missing artifacts. Discrepancies should be reported to the PM or POC. The JITC cannot complete testing without all appropriate artifacts.

Before testing, the PM must declare that the current release version of the system is the baseline that will be tested. After the baseline version has been set, no modification can be made before or during the test event.

Identify Shared Services and Data Assets. Testers must confirm that the Program Management Office has identified all the data assets and services that are intended to be shared. Testers should use the JS-certified requirements documents as the primary source for determining what services and data assets are intended to be shared.

Information Exchange (IE) and system requirements are shown in the System View-6, "Systems Resource Flow Matrix," and the Operational View-5, "Operational Activities." The tester must analyze the system requirements to determine which capabilities, IEs, system functions, etc., provide enterprise data and/or services.

The EVTSS (if available and accurate) identify shared services and data assets according to Joint Capabilities Area (JCA). Viewpoints define IE requirements for services and data assets and the JCA can cross-reference them to the shared services and data assets in the EVTSS.

The JITC testers must perform a thorough review of architecture documents to ensure a complete assessment. The Service Level Agreement can also provide valuable information regarding the availability, timeliness, and security measures for specific interfaces that may vary from its basic performance requirements.

Determine Applicability of Net-Centric Requirements. Some IT systems and NSS are not net-centric and, consequently, do not require evaluation for compliance with the DSS element (e.g., systems that are tactical or use non-Internet Protocol communications).

Figure 2-1 illustrates the process to determine applicability of the DSS element.

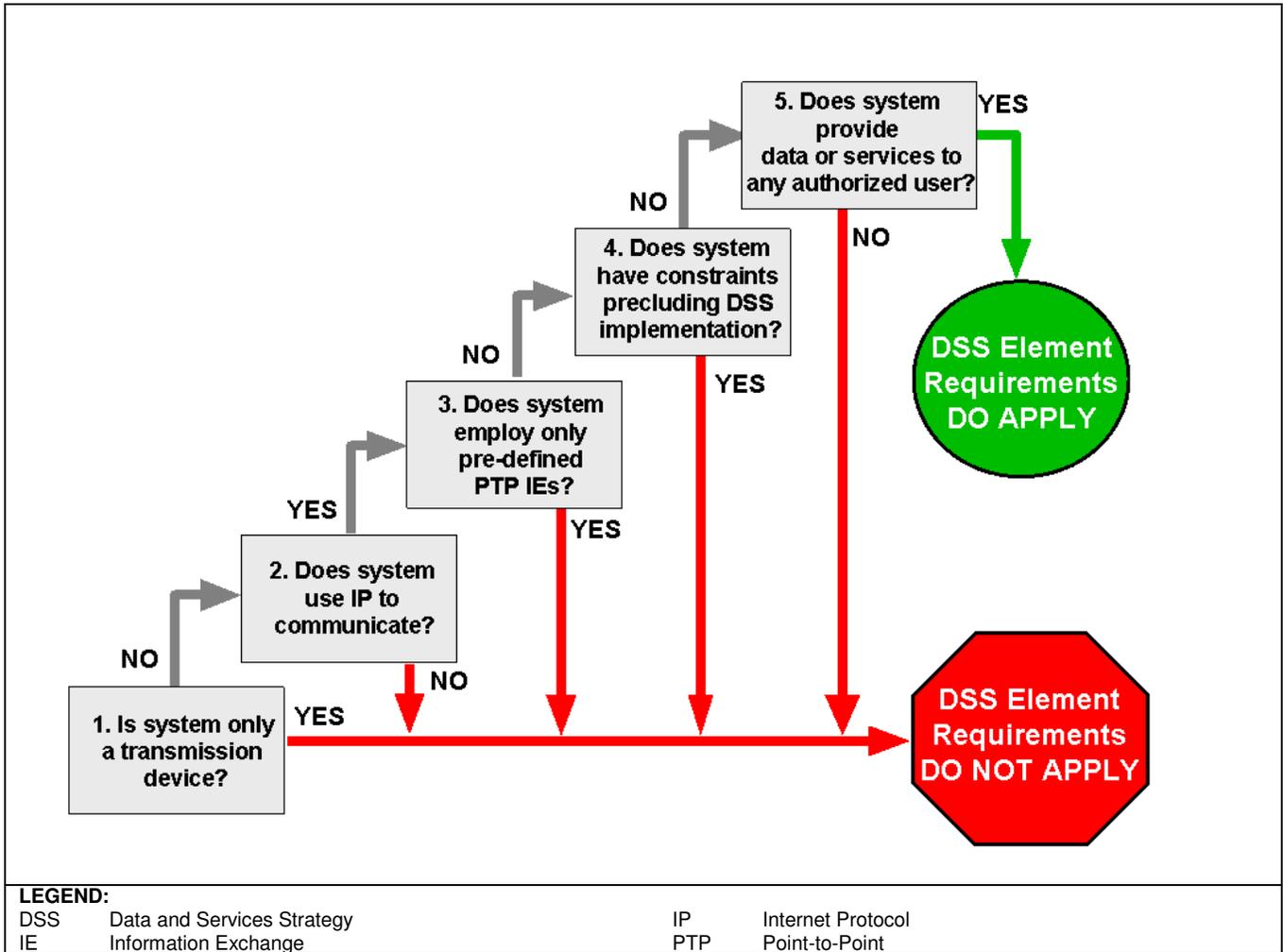


Figure 2-1. Net-Centric Decision Tree

The following questions from the Net-Centric Decision Tree help determine whether or not the DSS applies to a system:

1. Is the system only a transmission device such as a radio, satellite, or network equipment?

Transmission Devices are communications devices which provide connectivity, but do not handle data except in encapsulated form.

If the answer is YES, then the net-centric DSS element does not apply.

2. Does the system employ Internet Protocol (IP) to communicate?

IP is a protocol used for communicating data across a packet-switched network.

If the answer is NO, then the net-centric DSS element does not apply.

3. Does the system employ only pre-defined, Point-to-Point information exchanges?

Point-to-Point information exchanges are pre-defined, engineered information exchanges on a closed network. Points or nodes require physical connection or system administrator intervention (creating an address) to establish connectivity.

If the answer is YES, then the net-centric DSS element does not apply.

4. Does the system have infrastructure or timeliness constraints that preclude implementation of the Net-Centric Data or Services Strategy?

Do any of the following apply:

- System is designed for network connectivity at less than 85 percent of operational time
- System resides on a network infrastructure with less than 100 Kilobits per second bandwidth
- Latency constraints are equal to or less than 1 second (data must be delivered in one second or less)

If the answer is YES, then the net-centric DSS element does not apply.

5. Is the system's data or service intended to be available to any authorized users?

Net-centric data and services are designed for use across Command, Component, Service, or Agency boundaries and are available to be used by both anticipated and unanticipated users.

If the answer is NO, then the net-centric DSS element does not apply.

Applicability of DSS requirements also depends on the program's architecture products, requirements documents, and shared data and services. Some policy requirements may not be applicable due to the system's architecture or process implementation method.

For example, consider an authoritative source data asset that is shared via an externally available service such as a publishing service. The system does not provide its own data access mechanism. In this case, the data access mechanism is outside of the responsibility and control of the PM. The system does not provide a service; consequently, the service sharing requirements do not apply. However, the system does provide a data asset, so the data sharing requirements apply.

RISK ASSESSMENT

To determine which requirements must be tested, testers must assess risk levels for each of the applicable DSS requirements. Requirements with critical risk must be tested. Requirements with contributory risk may or may not be tested, depending on resources and customer requests. For example, the PM could request that JITC test to determine if the system meets the contributory level for the system. The risk levels are as follows:

- **Joint Critical.** The system provides enterprise or COI data or services as part of its joint critical IE requirements.
- **Contributory.** The system provides enterprise or COI data or services that are not part of joint critical IE requirements.

TEST PLANNING AND EXECUTION

The JITC has developed test methodology and high-level test procedures for evaluating the DSS requirements. Appendix D presents detailed test procedures for evaluating DSS compliance; the procedures are organized according to specific objects that the testers must examine rather than by requirement. Text blocks in the right-hand margins in Appendix D relate the test procedures to one or more DSS requirement(s).

If possible, the DSS test procedures must be augmented with specific measures obtained from the JS-certified requirements documents. For example, consider the following fictitious requirement:

- 85 percent (threshold) of data produced daily (in megabytes (MB)) must be available to authorized users within 10 minutes of being created.

Rather than verifying that content data is accessible to authorized end users, testers should time all data produced in a day, from creation to availability, and calculate the percent of data (in MB) that became available within 10 minutes of creation.

REPORTING

The threshold criterion for the DSS element requires the system meets *all joint critical* net-centric requirements contained in the JS-certified NR-KPP. Objectively, the system should meet *all net-centric* requirements contained in the JS-certified NR-KPP.

Table 2-3 contains Met/Not Met criteria for DSS requirements. Specific instructions for their application will be provided in a future update.

Table 2-3. Definitions (Criteria) for Data and Services Strategy Compliance

Decision	Criteria
Met	Meets all joint critical net-centric requirements.
Partially Met	Meets some joint critical net-centric requirements. None of the discrepancies have a critical operational impact.
Not Met	Failed to meet certain joint critical net-centric requirements. Discrepancies with critical operational impact exist.
Not Tested	Critical net-centric requirements were not tested.
Not Applicable	Net-centric requirements are not applicable to the capability.

The Engineering and Policy Branch of the Strategic Planning and Engineering Division will provide reporting formats for the test report and the Joint Interoperability Certification Memorandum.

Tables 2-4 and 2-5 are examples of status tables for the Joint Interoperability Certification Memorandum and/or test report. These tables present status of compliance with data and service sharing requirements.

Table 2-4. Net-Centric Data Compliance

REQUIREMENT	CRITERIA	STATUS	REMARKS
Data is Visible	Post discovery metadata in an Enterprise Catalog.	Met	
	Use appropriate keywords for discovery.	Not Met	
Data is Accessible	Post data to shared space.		
	Provide access policy.		
	Provide serving (access) mechanism.		
	Publish active link to data asset.		
Data is Understandable	Publish semantic and structural metadata.		
	Register data artifacts in DoD MDR.		
Data is Interoperable	Base vocabularies on UCore.		
	Comply with COI data-sharing agreements.		
	Conform to DDMS.		
Data is Trusted	Provide information assurance and security metadata.		
LEGEND:			
COI	Community of Interest	MDR	Metadata Registry
DDMS	DoD Discovery Metadata Specifications	UCORE	Universal Core
DoD	Department of Defense		

Table 2-5. Net-Centric Service Compliance

REQUIREMENT	CRITERIA	STATUS	REMARKS
Services are Visible	Publish a description of the service or access mechanism.	Met	
	Comply with enterprise-specified minimum service discovery requirements.	Not Met	
Services are Accessible	Provide an active link to the service in the enterprise catalog.		
	Provide an active link to the service in the Net-Centric Enterprise Services (NCEs) Service Registry.		
Services are Understandable	Publish a description of the service or access mechanism to the NCEs Service Registry.		
	Publish service artifacts to Department of Defense (DoD) Metadata Registry.		
	Provide service specification or Service Level Agreement (SLA).		
Services are Trusted	Operate services in accordance with SLA.		
	Include security mechanisms or restrictions in the service specification.		
	Enable continuity of operations and disaster recovery for services.		
	Provide Network Operations (NetOps) Data (NetOps Agility).		
Use of Core Enterprise Services (CES)	CES are used in accordance with DoD Chief Information Officer mandates.		

Table 2-6 is the NR-KPP status table in the Joint Interoperability Certification Memorandum and/or test report and provides the overall status of the DSS requirements. The applicable items for the DSS element are highlighted in the table.

Table 2-6. NR-KPP Status – Net-Centric Data and Services Strategy

INTEROPERABILITY REQUIREMENT	STATUS		REMARKS
	Threshold	Objective	
1. Solution Architectures; i.e. operationally effective information exchanges	<i>Status (i.e., Met)</i>	<i>Status (i.e., Not Tested)</i>	Degree of compliance with the requirements and expected operational impact. (i.e., Tested to the Threshold: All joint critical interfaces, not all of the interfaces for this system. There were no failures with a major or critical impact to the users. Two minor failures occurred and evaluated by the users having no impact to their mission accomplishment.)
2. Net-Centric Data and Services Strategy	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
a. Net-Centric Data	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
b. Net-Centric Services	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
3. GTG	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
DISR	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
GESP/KIP	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
4. IA	<i>Status</i>	<i>Status</i>	Statement that testing was performed in the approved IA configuration. Statement that the DAA issued an IATO/ATO, including date of issue and termination date.
5. Supportability			
a. Spectrum certification	<i>Status</i>	<i>Status</i>	DD1494 Status and date.
b. E3 Program	<i>Status</i>	<i>Status</i>	E3 Test Report, EMI Test Report, or something similar and date.
c. SAASM	<i>Status</i>	<i>Status</i>	If SAASM compliant-N/A. If not SAASM compliant, waiver and date.
d. JTRS	<i>Status</i>	<i>Status</i>	If JTRS compliant-N/A. If not JTRS compliant, waiver and date.
6. Other (as required)	<i>Status</i>	<i>Status</i>	
LEGEND:			
ATO	Authorization to Operate	GTG	GIG Technical Guidance
DAA	Designated Accrediting Authority	IA	Information Assurance
DISR	Department of Defense Information Technology Standards Registry	IATO	Interim Authorization to Operate
E3	Electromagnetic Environmental Effects	JTRS	Joint Tactical Radio System
EMI	Electromagnetic Interference	KIP	Key Interface Profile
GESP	GIG Enterprise Services Profile	N/A	Not Applicable
GIG	Global Information Grid	NR-KPP	Net-Ready Key Performance Parameter
		SAASM	Selective Availability Anti-Spoofing Module

(This page intentionally left blank.)

CHAPTER 3 – GLOBAL INFORMATION GRID TECHNICAL GUIDANCE

NET-READY KEY PERFORMANCE PARAMETER STATEMENT

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E defines the Global Information Grid (GIG) Technical Guidance (GTG) element of the Net-Ready Key Performance Parameter (NR-KPP) as:

"...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..."

CJCSI 6212.01E

According to CJCSI 6212.01E, programs must be compliant with Information Technology (IT) standards and implementation guidance from GIG Enterprise Service Profiles (recently renamed as GIG Technical Profiles (GTPs)). This version of the instruction removes references to Key Interface Profiles (KIPs). However, KIPs remain valid until GTPs are mandated. Therefore, requirements documents will continue to identify KIPs relevant for the system.

The GTG element is evolving. The GTG will provide the resources for a Program Management Office (PMO) to determine where its IT system or National Security System fits into the GIG and what it must do to ensure interoperability with the GIG. The GTG provides a grace period for PMOs publishing system documentation. Program documents published up to six months after the release of a new GTG version can use the previous GTG version guidance.

The GTG Portal on Intellipedia offers the latest GTG information. It is available at: https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance. There is also a GTG Federation Web site being developed for the purpose of assessing GTPs and developing Information Support Plans (ISPs). Users can sign up for an account and try out the demonstration at the GTG Federation homepage: <https://216.181.9.90/gtg/homepage.do>.

There are two areas that must be evaluated to determine GTG element compliance, Implementation of GTPs/KIPs and Compliance with Department of Defense (DoD) Information Technology Standards Registry (DISR)-approved standards.

GTP/KIP Implementation. The GTPs/KIPs provide a combination of technical guidance and solutions for accessing the GIG infrastructure, accessing data and services, and ensuring interoperability with other GIG users.

GTPs. The GTPs are aligned with the DoD Information Enterprise Architecture priority areas: Communications, Data and Services, Secured Availability, Network Operations, and Computing Infrastructure. They provide the minimal core set of technical functions and standards required to implement a needed capability, described in terms of DISR-mandated IT standards, supporting IT standards, associated profiles, reference implementations, and tests. At the present time, there are no mandated or approved GTPs. The first set of GTPs has been sent to the GTG Configuration Management Board (CMB) for approval. The CMB will forward approved GTPs to the appropriate communities of interest for formal review and comment. Any GTPs that become mandated for use will be posted to the GTG Federation Web site.

The GTPs use a template to ensure they address the required issues. The template has these sections:

- **Interoperability Reference Architecture and Service Description.** This section includes a description and graphic of where the GTP architecture fits in the GIG Reference Topology and a description of services provided under the GTP.
- **Interoperability Requirements Description.** This section describes the interoperability requirements necessary to fulfill the Interoperability Reference Architecture, best practices for implementation, and requirements for Secured Availability.
- **Technical Implementation Profile.** This section links requirement or guidance statements with DISR standards and verification methods.
- **Maturing guidance.** This section has guidance on potential changes in the scope of the GTP or technologies for programs to consider in their mid- and far-term planning and implementation. It is outside the scope of assessment.
- **Compliance Testing.** This section should contain the test concepts, responsible agencies, and documentation for demonstrating conformance to a standard. Most of the current drafts have descriptions of the five verification methods.
- **Key Programs Implementing GTP.** This section lists any DoD programs that have implemented the GTP so a PMO can compare the implementations.
- **Data.** This section contains data formats, techniques, or exchange requirements necessary to ensure GTP capability functionality.
- **References.** This section contains all the references used in developing the GTP.

KIPs. The KIPs are organized into three families: Transport, Computing Infrastructure, and Application Enterprise Services. However, only the Transport KIPs are approved. Information related to KIPs can be found at:

<https://www.us.army.mil/suite/page/477323>.

DISR Standards Compliance. The DISR is the authoritative source for all IT standards. The DISR categorizes standards as Emerging, Mandated, or Retired.

The Joint Staff (JS)-certified Technical View (TV)-1 lists standards in the current development effort. The TV-2 lists standards for future development efforts. These viewpoints are referenced or included in the Capability Development Document (CDD), Capability Production Document (CPD), ISP, and/or Tailored information Support Plan (TISP). If the PMO includes non-DISR standards in the TV-1, the PMO must submit a Change Request to DISR requesting approval to use those standards. If the TV-1 contains non-DISR or retired DISR standards, the PMO must request and receive a JS waiver to use these standards.

REQUIREMENTS ANALYSIS

GTP/KIP Implementation. The JITC testers will review the GTP/KIP declaration to verify the correct profiles are identified and that the standards, standards profiles, and implemented options comply with the profile specifications.

DISR Compliance. The JITC testers will review the system's TV-1 and TV-2 for the selection and use of mandated standards, emerging standards, non-mandated DISR standards, and non-DISR standards. The tester will verify that appropriate change requests and waivers have been approved. If the TV-1 or TV-2 contains any standards that are not mandated in DISR, the JITC tester should review the ISP for a discussion of risk for these standards.

RISK ASSESSMENT

The GTP/KIP-associated standards require a risk assessment. A risk assessment, in this case, is the analysis and determination of the level of risk any one standard poses to the functionality and interoperability of the system. The level of risk will determine if and what type of evaluation methods is required.

KIP/GTP. Since KIPs and GTPs, and their related standards, are proven and pre-approved for use in the GIG environment, the risk for all approved KIPs and GTPs is considered low. However, interoperability certification may still require conformance testing if the KIP/GTP-related Information Exchanges (IEs) are considered critical or implementation or system functionality is unique.

DISR Standards. The JITC evaluates a standard's risk by using the JITC Risk Assessment Database (J-RAD). The J-RAD contains IT standards related to the NR-KPP from the DISR and some non-DISR standards. Each standard has a corresponding JITC-developed risk evaluation and rationale, associated testing methodologies, and information on JITC testing facilities. The J-RAD also has links to Web sites of organizations concerned with the development, approval, and implementation of IT standards.

The JITC J-RAD team develops risk evaluations based on the following criteria:

- **General.** Is the standard listed in DISR or the ASSIST database? Are there published Abstract or Executable Test Suites for the standard? Are conformance test services available?
- **Maturity.** Is technical maturity and stability information in the DISR profile? Is the standard widely deployed in the DoD or Intelligence Community enterprise or commercially?
- **Interoperability.** Does DISR list DoD or commercial systems or products using the standard? Has JITC tested the standard with similar systems or products?
- **Implementation.** Are implementation profiles published in DISR? Is the release dependent on new hardware or software technology? Is the system using new standards or protocols? Does the implementation of the standard present unusual challenges?

The JITC J-RAD team will also identify standards in the TV-1 that are known to be incompatible with each other.

The JITC tester can assign a different risk rating than the J-RAD-recommended risk as needed. In some cases, the JITC-recommended risk may not be appropriate for a specific implementation. In such cases, the JITC tester will provide the program manager a justification for the different risk level and recommendation for additional conformance testing when appropriate.

For example, the recommended risk for the Joint Photographic Experts Group (JPEG) imagery standard is low for most applications, because it is widely deployed and has few reported problems. However, if JPEG is used to pass time-sensitive or critical intelligence overlays, the risk may be high.

TEST EXECUTION

Testing the GTG element involves standards conformance testing and interoperability testing. The risk assessment, previously discussed, will be used to determine the level and type of testing required to determine GTG compliance.

Standards conformance to all high-risk IT standards must be verified unless costs, lack of capabilities, or lack of established methodologies prevents verification. It may also be desirable to test low-risk standards that support critical IEs. The JITC tester will take advantage of all developmental and operational testing to collect interoperability test data. The JITC tester will work with the system PMO to identify what standards will be tested, where they will be tested, and how they will be tested.

Evaluation Methods. The following paragraphs describe GTG evaluation methods.

Analysis. Analysis involves the static analysis of the technical profiles, operational views, and system views or data collected from several test events. Analysis can include comparing software text with the requirements from the standard or verifying the system components are connected as described in the KIP or GTP. The tester can also compile data from a number of activities (e.g., developmental and operational tests, exercises, or operational missions) to assess system interoperability.

Demonstrations. These are scripted tests conducted during developmental testing. The testers use scripted material to stimulate the system and produce responses. The conditions are controlled and the tests can be structured to exercise all the system functions; however, there are no monitoring tools to capture the performance and structural details. The demonstration should not rely on a few scripted samples; it should include additional inputs following the script models.

Vendor Declarations. Vendor declarations are statements from the developer, signed by responsible officials, that the system is in compliance with various standards. These should contain a description of the system configuration tested, tools and methodologies used for testing, and whether conformance was demonstrated to government representatives. These declarations are key data elements for evaluating many systems, because the JITC or other testing organizations may not have the standards or test tools to conduct conformance tests.

Interoperability Tests. These tests do not provide a detailed assessment of the standard implementation, but they show the degree information is exchanged. They are described in more detail below.

Conformance Tests. These formal laboratory tests confirm that an implementation meets the requirements of an IT standard. They are described in more detail below.

Interoperability Testing. Interoperability testing involves multiple systems exchanging information and is required for an IT system's fielding decision. It is generally done in conjunction with relevant developmental or operational testing. The interoperability test is the final proof that the IT standards have been implemented correctly. If the interoperability test is the only way to evaluate the implementation of a standard, the tester must develop test procedures that focus on the system functionality, capability, or components using the standard. Interoperability testing verifies that the system's implementation of the GTP/KIP standards result in successful IEs with other systems.

Standards Conformance Testing. Standards conformance testing is done on an isolated system in a controlled or semi-controlled environment to establish that technical specifications have been met. The JITC has several laboratories available for conformance testing. Testing can also be done at other federal government facilities or commercial facilities. If these tests are part of the developer's testing, representatives from the PMO, operational test agency, or JITC should witness them to provide independent evaluation of the tests' thoroughness. The scope of standards conformance testing is affected by several variables, including the number of standards involved, the complexity of the tests, availability of test methodologies and tools, the program schedule, and costs. Not all standards implementations can be tested; there may not be an accepted methodology, an available test facility, or test facility with the necessary tools for that implementation. Military-unique implementations of even low-risk standards should be considered for conformance testing. The J-RAD team can provide information on which standards must be tested, which can be evaluated with other methods, and what facilities can do the tests.

GTP/KIP Compliance. The JITC tester will verify the CDD/CPD/ISP/TISP-described implementations are consistent with the tested system and that implementations are compliant with the applicable profiles. Standards conformance assessments will verify the system has implemented the profiles and related standards properly at all critical IEs.

DISR Standards Compliance. The J-RAD will identify the appropriate test laboratory at JITC and other facilities that should be contacted to arrange testing. The following are examples of test facilities and what standards can be tested at those facilities:

- The JITC Ultra High Frequency (UHF) Satellite Communications Test Facility is the only test facility authorized to certify systems for conformance to the Military Standard 188-181, 188-182, and 188-183 series.
- The JITC Joint Tactical Data Link Laboratory tests systems using tactical data links (e.g., Link-16).
- The National Imagery Transmission Format Standards Laboratory tests commercial products to confirm that they meet various imagery standards.
- The Motion Imagery Standards Laboratory can perform standards conformance tests for an organization to benchmark a product against a standard.
- The Joint Terminal Engineering Office tests satellite communications terminals for use outside the UHF spectrum for conformance to military standards.
- The Federal Aviation Administration tests and certifies aircraft-to-control tower communications systems.

REPORTING

The Engineering and Policy Branch of JITC's Strategic Planning and Engineering Division has provided reporting formats for the Joint Interoperability Certification Memorandum and test report.

Table 3-1 shows the criteria for determining whether the system meets the GTG compliance requirements.

Table 3-1. GTG Compliance Criteria

Decision	Threshold	Objective
Met	No critical standards conformance-based deficiencies were identified in DT or OT by a combination of government and/or commercial verifications or JITC standards testing or conformance certifications that included all high-risk standards in the TV-1 that support a critical information exchange and/or all high-risk net-centric standards. Met all critical IE requirements for a given interface, between two given systems, or information (data) exchanges.	No critical standards conformance-based deficiencies were identified in DT or OT by a combination of government and/or commercial verifications or JITC conformance certification for any high-risk standards in the TV-1.
Partially Met	Met some but not all applicable GTG requirements.	Met some but not all applicable GTG requirements.
Not Met	Tested and failed to meet GTG requirements that result in a critical (operational impact) failure.	Tested and failed to meet GTG requirements that result in a critical (operational impact) failure.
Not Tested	No critical IEs were tested.	No IEs were tested.
LEGEND:		
DT	Developmental Testing	JITC Joint Interoperability Test Command
GIG	Global Information Grid	OT Operational Testing
GTG	GIG Technical Guidance	TV Technical View
IE	Information Exchange	

DISR Compliance. Table 3-2 is an example of the DISR compliance results table; it is located in the Joint Interoperability Certification Memorandum and/or test report.

Table 3-2. DISR Compliance

System: XYZ		TV-1 last updated on: DD MMM YYYY				
SERVICE AREA	STANDARD IDENTIFIER	TITLE OF STANDARD	DISR STATUS	RISK/RATIONALE	EVALUATION METHOD	RESULTS
Document Interchange	CISS ISM:XML	Common Information Sharing Standard for Information Security Marking: XML Implementation Guide, release 2.0.3, 15 February 2006	Mandated	High – Standard mandated within the last three years, standard is critical to interoperability/net-centricity based on the Intelligence Community security marking standards from the CAPCO Standard.	Conformance testing with the test tool XML Spy in the "N" laboratory.	Passed

Table 3-2. DISR Compliance (continued)

SERVICE AREA	STANDARD IDENTIFIER	TITLE OF STANDARD	DISR STATUS	RISK/RATIONALE	EVALUATION METHOD	RESULTS
Application-specific Data Interchange and Document Interchange	Department of Defense Discovery Metadata Specification (DDMS) 1.3 (CISS RM 1.3)	DDMS Version 1.3, 20 July 2005; aka Common Information Sharing Standard for Resources Metadata: Application Profile Data	Mandated	High – Standard mandated within the last three years, DDMS is a mature DoD- specific standard; W3C is the international body responsible for standard. Standard is critical to interoperability/net-centricity. Supports DoD Net-Centric Data Strategy which identifies approaches that will improve flexibility in data exchange, supporting interoperability between systems without requiring predefined, pair-wise interfaces between them. This flexibility is essential in the many-to-many exchanges of a net-centric environment. Standard is available to all federal, state, local, and tribal agencies. Widely supported by commercial vendors in the format of database, XML document, and Word document.	Performed a manual Fed Search Procedure to verify that tagged data is searchable and definable by fed Search. Used DDMS tagged source data to compare DDMS Schemas to the published schema provided by the developer. Developer used DIFF Dog application during DT to verify DDMS conformance and Markup Language (XML) instances to ensure that DDMS tags and namespaces are used.	Passed
Document Interchange and Web Services	Document Object Model (DOM) level 3 W3C	DOM Level 3 Core Specification Version 1.0, W3C Recommendation, 07 April 2004	Mandated	High – Application programming interface for HTML and XML documents. DOM interfaces for XML internal and external subsets have not been specified. It is publicly available: http://www.w3c.org/TR/2004/REC-DOM-Level-3-Core-20040407 . DOM3 is a final W3C Recommendation, finalized on 07 April 2004.	System Program Management Office (PMO) obtained a vendor letter of compliance testing during software acceptance testing and DT events.	Passed
Electronic Data Interchange (EDI)	EDI	XML Schema Part 2: Datatypes, Second Edition, W3C Recommendation, 28 October 2004	Mandated	Low – It is mature, stable, and supported by thousands of products. Support for it is widespread.	Not tested	Not tested
Document Interchange	Web Services Description Language (WSDL) 1.1	WSDL 1.1, W3C Note, 15 March 2001	Mandated	High – Defines the XML grammar needed for network services for distributed systems and provides the methods for automating the details involved in applications communication. Enables net-centric interoperability by allowing the formal standardized description of web services. This makes it possible to perform publishing and discovery using Universal Description, Discovery, and Integration (UDDI) for the services described using WSDL 1.1. WSDL 1.1 is a W3C Note, which does not carry official standing in W3C. It is publicly available, mature, stable, widely implemented, and commonly supported in commercial products and services.	WSDL conformance test procedures used in the "N" Lab with test tools ITKO LISA and XML Spy. Captured WSDL and verified through ITKO LISA.	Passed

(Legend is on the next page.)

LEGEND:			
CAPCO	Controlled Access Program Coordination Office	HTML	Hypertext Markup Language
CISS	Common Information Sharing Standard	ISM	Information Security marking
DIFF	Differential	RM	Reference Model
DISR	DoD Information Technology Standards Registry	TV	Technical View
DoD	Department of Defense	W3C	Worldwide Web consortium
DT	Developmental Testing	XML	eXtensible Markup Language
Fed	Federated		

KIP/GTP Compliance. The Technical Profiles are addressed through the identification of KIPs or GTPs and the implementation of the KIP/GTP-associated standards and guidance. Table 3-3 shows the overall GTP/KIP status; it is located in the Joint Interoperability Certification Memorandum and/or test report. The Status column should reflect the lowest results of the applicable sub-elements.

Table 3-3. GTP/KIP Compliance

REF #	NAME	VERSION/ DATE	IMPLEMENT- ATION PHASE	INTERFACE REF #	STATUS	REMARKS (INCLUDING CONSUMER/PROVIDER)
K1	UHF-Band SATCOM	DISR Baseline Release 07-2.0 2007-06-27	T	I1	Not Met	Provider. This software version not certified for UHF SATCOM DAMA. MIL-STD-188-181A not conformant. Critical operational impact.
GESP 0006.0003	UHF-Band Satellite Communications	0.3 15 January 2010	T	I1	Not tested	UHF-Band GTP not yet mandated.
K2	Ku-Band SATCOM	DISR Baseline Release 06-1.0 2006-02-21	O	I2	Met	Provider/Consumer. SATCOM Certification: PanAmSat US-7744. Interoperability testing did not identify any instances of significant non-conformance to standards. All information exchange requirements met.
GESP 0003.0006	Ku-Band Satellite Communications	0.6 15 January 2010	O	I2	Not tested	Ku-Band GTP not yet mandated.
K3	Global Positioning System (GPS)	DISR Baseline Release 06-1.0 2006-02-21	O	I4	Not tested	Not tested. GPS has not been identified for GTP development.

LEGEND:			
DAMA	Demand Assigned Multiple Access	MIL-STD	Military Standard
DISR	Department of Defense Information Technology Standards Registry	O	Objective
GESP	GIG Enterprise Services Profile	REF	Reference
GIG	Global Information Grid	SATCOM	Satellite Communications
GTP	GIG Technical Profile	T	Threshold
I	Interface	UHF	Ultra High Frequency
K	Key Interface Profile		

Summary. Table 3-4 is the NR-KPP status table in the Joint Interoperability Certification Memorandum and/or test report and provides the overall status of the GTG requirements. The applicable items for the GTG element are highlighted in the table.

Table 3-4. NR-KPP Status – GTG Compliance

INTEROPERABILITY REQUIREMENT	STATUS		REMARKS
	Threshold	Objective	
1. Solution Architectures; i.e., operationally effective information exchanges	Status (e.g., Met)	Status (e.g., Not Tested)	Degree of compliance with the requirements and expected operational impact. (e.g., Tested to the threshold: All joint critical interfaces, not all of the interfaces for this system. There were no failures with a major or critical impact to the users. Two minor failures occurred and evaluated by the users having no impact to their mission accomplishment.
2. Net-centric Data and Services Strategies	Roll-up status	Roll-up status	
a. Data Sharing Requirements	Status	Status	Degree of compliance with the requirements and expected operational impact.
b. Services Sharing Requirements	Status	Status	Degree of compliance with the requirements and expected operational impact.
3. GTG	Roll-up status	Roll-up status	
a. DISR	Status	Status	Degree of compliance with the requirements and expected operational impact.
b. GESP/KIP	Status	Status	Degree of compliance with the requirements and expected operational impact.
4. IA	Status	Status	Statement that testing was performed in the approved IA configuration. Statement that the DAA issued an IATO/ATO, including date of issue and termination date.
5. Supportability			
a. Spectrum certification	Status	Status	DD1494 Status and date.
b. E3 Program	Status	Status	E3 Test Report, EMI Test Report, or something similar, and date.
c. SAASM	Status	Status	If SAASM compliant-N/A. If not SAASSM compliant, waiver and date.
d. JTRS	Status	Status	If JTRS compliant-N/A. If not JTRS compliant, waiver and date.
6. Other (as required)	Status	Status	
LEGEND:			
ATO	Authorization to Operate	GTG	GIG Technical Guidance
DAA	Designated Accrediting Authority	IA	Information Assurance
DISR	Department of Defense Information Technology Standards Registry	IATO	Interim Authorization to Operate
E3	Electromagnetic Environmental Effects	JTRS	Joint Tactical Radio System
EMI	Electromagnetic Interference	KIP	Key Interface Profile
GESP	GIG Enterprise Services Profile	N/A	Not Applicable
GIG	Global Information Grid	NR-KPP	Net-Ready Key Performance Parameter
		SAASM	Selective Availability Anti-Spoofing Module

CHAPTER 4 – INFORMATION ASSURANCE

NET-READY KEY PERFORMANCE PARAMETER STATEMENT

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E defines the Information Assurance (IA) element of the Net-Ready Key Performance Parameter (NR-KPP) as:

"...Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization To Operate (ATO) by the Designated Accrediting Authority (DAA)..."

CJCSI 6212.01E

The IA element requires that the capability, system, or service complies with the IA requirements in Department of Defense (DoD) 8500 series (overarching policy guidance for the IA element) and the CJCSI 6510 series directives, instructions, and manuals.

The DoD employs a defense-in-depth strategy to establish and maintain acceptable IA across the Global Information Grid (GIG). Protection mechanisms minimize system and information vulnerabilities, ensuring information and information systems maintain the appropriate level of availability, integrity, authentication, and non-repudiation based on mission assurance category and confidentiality level while maintaining the level of interoperability essential to the GIG.

Each capability, system, or service seeking Joint Interoperability Test Command (JITC) interoperability certification must obtain an Interim Authorization to Operate (IATO) or an Authorization to Operate (ATO) from the Designated Accrediting Authority (DAA). Any testing involving an operational network requires at least an Interim Authorization to Test (IATT) from the DAA.

TEST EXECUTION

The JITC will verify that the system has an IATO or ATO and that the system was tested in an approved IA configuration. At the program manager's discretion, the JITC may also perform IA testing.

There is no approved policy/guidance for JITC's IA testing at this time. The "JITC Policies and Procedures for the Verification of IA in Support of Joint Interoperability Certification" is not yet approved.

The JITC IA Branch provides guidance and oversight for all IA test support efforts within the JITC. The JITC's IA focus during interoperability testing is to determine if a system's accredited IA solution facilitates interoperability.

According to CJCSI 6212.01E, IA compliance may be verified through:

- **DoD Information Assurance Certification and Accreditation Process (DIACAP) Compliance.** The DIACAP verification determines whether Certification and Accreditation (C&A) has been accomplished and, if so, what final C&A determination was made (e.g., ATO, IATO, IATT, or Denial of Authorization to Operate).
- **C&A.** The C&A verification determines compliance with Intelligence Community Directive Number 503 under either the National Security Agency/Central Security Service Information System Certification and Accreditation Process or the C&A procedures defined by the Defense Intelligence Agency for the DoD Intelligence Information System. For capabilities evaluated with these processes, the JITC shall verify, determine, and report the status accorded.
- **Exemption Memorandum.** For systems granted an exemption from DIACAP (processed/granted through DAA), the program or proponent office will provide a copy of the exemption memorandum to the JITC. The IA requirements for these systems will be incorporated as part of normal design and test processes.
- **Configuration Compliance.** For all systems, determination shall be made regarding whether the IA configuration of the capability as tested corresponds to the IA configuration requirements asserted for the capability.
- **IA Scans.** For systems connecting to an enterprise network (e.g., Unclassified-But-Sensitive Internet Protocol Router Network, Secret Internet Protocol Router Network, Joint Worldwide Intelligence Communication System, Defense Switched Network, Defense Red System Network), appropriate IA configuration and security scan testing dictated by the network manager for approval to connect shall be performed and the status reported.

REPORTING

The JITC will report whether the system has an IATO or ATO and whether the system was tested in an approved IA configuration. The JITC will also report the results of additional IA testing (e.g., gold disk scans and retina scans). A thorough description of a system's or program's IA compliance with each applicable policy and regulation/instruction must be included in the test report to meet the IA element requirements. Program managers/sponsors must provide a memorandum to Defense Information Systems Agency/JITC, signed by the proponent DAA, when claiming exemption from any IA requirements (e.g., weapon systems without platform IT interconnections).

Table 4-1 shows the proposed criteria for Met and Not Met for system requirements. Specific instructions will be provided in a guidebook update.

Table 4-1. IA Compliance Criteria

Decision	Criteria	Remarks	
Verified	IATO/ATO and no critical discrepancies.	N/A	
Met	Only used if JITC performed the IA assessment.	N/A	
Partially Met	Program is following the DIACAP process steps, but has not been granted an IATO/ATO.	N/A	
Not Met	Failed to obtain an IATO (T) and/or ATO (O) or discrepancies identified with critical operational impacts.	Not Met – Failed to meet a constituent interface, interfacing system and ultimately individual information exchange requirements resulting in a critical (operational impact) failure. Any not met status for any critical information exchange requirement must result in issuance of a non-certification memorandum.	
Not Tested	Program is not following required IA processes or failed to obtain an IATO/ATO due to critical discrepancies.	N/A	
LEGEND:			
ATO	Authorization to Operate	IATO	Interim Authorization to Operate
DIACAP	Defense Information Assurance Certification and Accreditation Process	JITC	Joint Interoperability Test Command
IA	Information Assurance	O	Objective
		T	Threshold

Table 4-2 is required for reporting the IA compliance in the Joint Interoperability Certification Memorandum.

Table 4-2. Information Assurance Compliance Status

Requirements	Status		Remarks
	Threshold	Objective	
IA Configurations Used in Test Environment			
DIACAP Accreditation			
IA Compliance (JITC assessments)			
LEGEND:			
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process	JITC	Joint Interoperability Test Command
IA	Information Assurance		

Table 4-3 is the NR-KPP status table in the Joint Interoperability Certification Memorandum and/or test report and provides the overall status of the IA requirements. The applicable items for the IA element are highlighted in the table.

Table 4-3. NR-KPP Status – IA Compliance

INTEROPERABILITY REQUIREMENT	STATUS		REMARKS
	Threshold	Objective	
1. Solution Architectures; i.e., operationally effective information exchanges	<i>Status (i.e., Met)</i>	<i>Status (i.e., Not Tested)</i>	Degree of compliance with the requirements and expected operational impact. (i.e., Tested to the Threshold: All joint critical interfaces, not all of the interfaces for this system. There were no failures with a major or critical impact to the users. Two minor failures occurred and evaluated by the users having no impact to their mission accomplishment.
2. Net-Centric Data and Services Strategy	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
a. Data Sharing Requirements	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
b. Service Sharing Requirements	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
3. GTG	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
DISR	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
GESP/KIP	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
4. IA	<i>Status</i>	<i>Status</i>	Statement that testing was performed in the approved IA configuration. Statement that the DAA issued an IATO/ATO, including date of issue and termination date.
5. Supportability			
a. Spectrum certification	<i>Status</i>	<i>Status</i>	DD1494 Status and date.
b. E3 Program	<i>Status</i>	<i>Status</i>	E3 Test Report, EMI Test Report, or something similar and date.
c. SAASM	<i>Status</i>	<i>Status</i>	If SAASM compliant-N/A. If not SAASM compliant, waiver and date.
d. JTRS	<i>Status</i>	<i>Status</i>	If JTRS compliant-N/A. If not JTRS compliant, waiver and date.
6. Other (as required)	<i>Status</i>	<i>Status</i>	
LEGEND:			
ATO	Authorization to Operate	GTG	GIG Technical Guidance
DAA	Designated Accrediting Authority	IA	Information Assurance
DISR	Department of Defense Information Technology Standards Registry	IATO	Interim Authorization to Operate
E3	Electromagnetic Environmental Effects	JTRS	Joint Tactical Radio System
EMI	Electromagnetic Interference	KIP	Key Interface Profile
GESP	GIG Enterprise Services Profile	N/A	Not Applicable
GIG	Global Information Grid	NR-KPP	Net-Ready Key Performance Parameter
		SAASM	Selective Availability Anti-Spoofing Module

CHAPTER 5 – SUPPORTABILITY

NET-READY KEY PERFORMANCE PARAMETER STATEMENT

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E defines the Supportability element of the Net-Ready Key Performance Parameter (NR-KPP) as:

"...Supportability requirements to include SAASM, Spectrum, and JTRS requirements."

CJCSI 6212.01E

Supportability refers to the ability of systems and infrastructure components, external to specific Information Technology (IT) systems or National Security Systems (NSS), to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT systems or NSS to achieve its required operational and functional capability(ies). The Joint Interoperability Test Command's (JITC's) involvement must not drive any additional costs beyond what is necessary to review and report the status in certification documentation. This element requires compliance with spectrum certification requirements, Electromagnetic Environmental Effects (E3) Program Control and Spectrum Supportability Policy, Joint Tactical Radio System (JTRS), Selective Availability Anti-Spoofing Module (SAASM), Tactical Data Link (TDL) Implementations, and Bandwidth Analysis as defined in the capability, system, or service's Joint Staff (JS)-certified requirements documents. The JITC will verify Program Management Office (PMO) efforts comply with the requirements in these areas.

REQUIREMENTS ANALYSIS

The JITC testers will verify that the PMO has completed the necessary documentation and obtained the necessary certifications or waivers from responsible agencies.

E3 Control and Spectrum Supportability Policy. This policy requires systems to comply with E3 requirements and obtain spectrum certification.

E3 Requirements. The Department of Defense (DoD) Directive 3222.3, "DoD Electromagnetic Environmental Effects Program," establishes the electromagnetic compatibility, interference, and vulnerability requirements systems must address. System testing for these issues is usually completed during the developmental testing phase. The JITC will verify that the Test and Evaluation Master Plan (TEMP) identifies developmental testing of E3 requirements, where applicable.

Spectrum Certification. The Frequency Allocation-to-Equipment Process supports the DoD spectrum management goal. Certification is achieved through

submission and approval of a DD Form 1494, "Application For Equipment Frequency Allocation," and the approval of a DD Form 1494 (Stage 4) through the United States Military Communications-Electronics Board (MCEB). The DoD acquisition policy states that the funds for the acquisition, research, development, production, purchase, lease, or use of weapons systems, information management systems, electronic warfare systems, or other systems that require use of the electromagnetic spectrum will not be released by the obligating authority until an application for frequency allocation has been approved.

The DD Form 1494 will address the transmission, reception, antenna characteristics, general information, and foreign coordination information of the system. The DD 1494 applies to four stages of frequency allocation:

- **Stage 1 – Conceptual.** During this stage, initial system planning is completed, frequency bands and other characteristics are proposed, and funding is needed for studies or proof-of-concept testbeds.
- **Stage 2 – Experimental.** In this stage, preliminary system design is completed and the program needs working test models or assignment of frequencies for experimental use.
- **Stage 3 – Developmental.** In this stage, the major design has been completed and the program is ready for engineering development models.
- **Stage 4 – Operational.** In this stage, development has been completed and measured data for technical characteristics is available.

The Stage 4 application must include the measured technical data and identifies the final operating constraints or restrictions. Approval of the Stage 4 application by the MCEB Equipment Spectrum Guidance Permanent Working Group (ESG PWG) constitutes the authorization to radiate/operate in support of operational deployment. The JITC will verify that the DD Form 1494 has been approved (Stage 3 for Milestone (MS) B, Stage 4 for MS C) by the ESG PWG, and the Capability Development Document/Capability Production Document (CPD) states that the system has received approval of its applicable frequency application.

JTRS Policy. The JTRS covers all radio-based communications equipment in the 2-megahertz to 2-gigahertz frequency range. The DD Form 1494 addresses the system's frequency requirements. The system must acquire any radio-based communications components operating in that range from a JTRS-based capability source. Only the Assistant Secretary of Defense (ASD) (Networks and Information Integration (NII))/DoD Chief Information Officer (CIO) may grant waivers to this policy. If the system is to operate in this frequency range, the JITC will verify that only a JTRS-based capability source was used or an ASD (NII)/DoD CIO waiver was granted.

SAASM Requirements. These requirements apply to any systems incorporating Global Positioning Systems (GPSs). Any GPS receivers procured after 1 October 2006 must be SAASM or M-code GPS User Equipment (MGUE) compliant. These requirements also apply to legacy systems integrating GPS receivers and any

modifications to GPS subsystems. The JITC tester will verify that the requirements document states the system will use SAASM-compliant equipment if applicable.

TDL Implementation. Policy within the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Joint Tactical Data Enterprise Services Migration Plan requires all systems and platforms employing tactical information exchanges (e.g., fixed or variable format message TDLs) shall use joint certified software programmed to the specific suite of Military Standards. CJCSI 6212.01 requires programs to fully describe their TDL implementation in the JS-certified requirements documents.

The JITC TDL Branch tests all inter-Service data link uses (by definition almost all TDLs) and reviews and approves Service/Agency tests. The JITC requires the detailed implementation data in order to conduct the standards conformance tests and the joint mission area interoperability/information exchange evaluations. Because of the potential size of the implementation data it is not reasonable to include all the details implied by CJCSI 6212, but the TDL Branch would expect at least a reference to a database or other document. If the Program Office doesn't provide all the required data for the testing, JITC will not be able to issue a standards conformance certification. Data shortfalls could also prevent the NR-KPP certification.

Bandwidth Analysis. The MS C submission packet (CPD and/or Information Support Plan (ISP)) shall include bandwidth and quality of service requirements. The submission must address the information sharing requirements and their potential impact to the Global Information Grid (GIG). The PMO must discuss the program's current and future bandwidth requirements for all transport methods (Terrestrial, Satellite, etc) and data types (e.g., voice, video, Internet Protocol, etc). The JITC tester will verify that system bandwidth and quality of service requirements for transmitting and receiving information is documented in the CPD and/or ISP and that current and future bandwidth requirements and potential GIG impacts are addressed

RISK ASSESSMENT

Risk assessment, in this case, is the evaluation that the information availability is sufficient to determine the capability, system, or service's compliance to Supportability requirements. The tester reviews the program requirements documentation to determine if any of the Supportability areas apply to the capability, system, or service. The tester also verifies that the program has obtained the required certifications before the JITC interoperability certification. If the capability, system, or service has SAASM requirements, compliance only requires a report of the compliance status of SAASM and MGUE receivers. Any interoperability issues with the actual function of GPS receivers are captured under the corresponding information exchange requirements identified in the solution architecture. The PMO should provide evidence of any documents received from other agencies, such as MCEB or United States Army Electronic Proving Ground, regarding document submissions or specialized testing. The TEMP should describe developmental and operational testing with sufficient detail for the testers to determine appropriate data collection events.

TEST EXECUTION

E3 Control and Spectrum Supportability Policy. The PMO will provide JITC any test documentation used to support E3 control and spectrum supportability compliance. Developmental and operational testing should reveal any problems with the actual implementation of TDL and GPS equipment and errors in estimating the requirements for bandwidth.

JTRS. The JITC Radio Frequency Test Facility was built for testing JTRS equipment. This laboratory can determine if a system needs testing. The High Frequency and Ultra High Frequency test facilities can also test radio systems in the JTRS range.

SAASM. The PMO will provide JITC any SAASM documentation and related test reports. Information on SAASM-compliant GPS receivers can be obtained from the Service GPS program offices. The SAASM testing is currently limited to developmental or laboratory tests. If applicable, the JITC will request documentation (test and/or certification) that verifies the system has met SAASM or MGUE requirements and that the GPS component is capable of using cryptographic keys. Developmental and operational testing should reveal any problems with the actual implementation of GPS equipment.

TDL. The PMO is responsible for ensuring TDL standards compliance and will provide the JITC tester with all TDL compliance test data and reports. The JITC can conduct standards conformance testing of TDL systems in their Common Data Link, Joint Tactical Data Link, and Situational Awareness Data Link laboratories.

Bandwidth Analysis. The JITC will use developmental and operational test data to confirm that documented bandwidth requirements are reliable estimations.

REPORTING

The JITC reporting of the Supportability element serves three primary purposes: 1) Report to the PMO whether a system meets or does not meet specific supportability requirements, 2) Identify to the PMO and warfighter the operational risks associated with non-compliant criteria, 3) Results provide a summary to support the interoperability certification decision.

Table 5-1 shows the criteria for Met and Not Met for system Supportability requirements.

Table 5-1. Supportability Requirement Criteria

Element	Met	Not Met	Remarks
E3 Program Compliance	Completion of applicable requirements of DoDD 3222.3.	DoDD 3222.3 requirements have not been satisfactorily completed.	N/A
Spectrum Certification	System has an approved DD Form 1494 (Stage 4).	System's DD Form 1494 (Stage 4) was disapproved or was not obtained for any reason.	System does not radiate in the electromagnetic spectrum.
JTRS Policy Compliance	System has radio-based communications operating in the 2-MHz to 2-GHz frequency range and is fielding/fielded a JTRS solution.	System has radio-based communications operating in the 2-MHz to 2-GHz frequency range, does not have a waiver for JTRS requirements and is fielding/ fielded a non-JTRS solution.	System does not have radio-based communications operating in the 2-MHz to 2-GHz frequency range subject to JTRS or JTRS requirements have been waived.
GPS SAASM Compliance	System procured SAASM or MGUE-compliant GPS receivers.	System failed to procure SAASM or MGUE-compliant GPS receivers.	System does not include any integrated GPS receivers or employs legacy GPS receivers procured prior to 10/1/2006
TDL Implementation	Platform TDL implementation information was included in an I&S certified requirements document.	Platform TDL implementation information was not included in an I&S certified requirements document.	System does not include TDL implementation.
Bandwidth Analysis	Expected bandwidth and quality of service requirements for information transmission and reception are included in the MS C submission documents.	Expected bandwidth and quality of service requirements for information transmission and reception are not included in the MS C submission documents.	This applies to any net-enabled system.
LEGEND:			
DoDD	Department of Defense Directive	MGUE	M-code GPS User Equipment
E3	Electromagnetic Environmental Effects	MHz	Megahertz
GHz	Gigahertz	MS	Milestone
GPS	Global Positioning System	N/A	Not Applicable
I&S	Interoperability and Supportability	SAASM	Selective Availability Anti-Spoofing Module
JTRS	Joint Tactical Radio System	TDL	Tactical Data Link

Table 5-2 shows Supportability status; it is located in the Joint Interoperability Certification Memorandum and/or test report.

Table 5-2. Supportability

ELEMENT	CRITERIA	STATUS																
E3 Program Compliance	Completion of applicable requirements of DoD Directive 3222.3, "DOD Electromagnetic Environmental Effects (E3) Program," including verification of Electromagnetic Compatibility (EMC), Electromagnetic Interference (EMI), and Electromagnetic Vulnerability (EMV), and other aspects as dictated by the capability and its operational environment.																	
Spectrum Certification	The program must have a completed Stage 4 (Operational) spectrum supportability determination (DD Form 1494).																	
JTRS Compliance	Verification that any radio-based communications requirement to be satisfied as part of the capability under evaluation and operating in the JTRS spectrum, 2 MHz to 2 GHz, is acquired as a component capability from a JTRS-based program source. Exceptions to this policy may only be made by ASD (NII)/DoD CIO.																	
GPS SAASM Compliance	Verification that any GPS receiver equipment acquired for use as part of the capability conforms to the requirements of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6130.01 for incorporation of a SAASM.																	
TDL Implementation Details	Platform TDL implementation information was included in an I&S certified requirements document; i.e., ISP, TISP, CPD.																	
Bandwidth Analysis	Systems that receive or transmit information provided an estimate of the expected bandwidth and quality of service requirements for support of the system(s) in the MS C submission; i.e., TISP, ISP, CPD.																	
<p>LEGEND:</p> <table border="0"> <tr> <td>ASD (NII) Assistant Secretary of Defense (Networks and Information Integration)</td> <td>I&S Interoperability and Supportability</td> </tr> <tr> <td>CIO Chief Information Officer</td> <td>ISP Information Support plan</td> </tr> <tr> <td>CPD Capability Production Document</td> <td>JTRS Joint Tactical Radio System</td> </tr> <tr> <td>DoD Department of Defense</td> <td>MHZ Megahertz</td> </tr> <tr> <td>E3 Electromagnetic Environmental Effects</td> <td>MS Milestone</td> </tr> <tr> <td>GHz Gigahertz</td> <td>SAASM Selective Availability Anti-Spoofing Module</td> </tr> <tr> <td>GPS Global Positioning System</td> <td>TDL Tactical Data Link</td> </tr> <tr> <td></td> <td>TISP Tailored Information Support Plan</td> </tr> </table>			ASD (NII) Assistant Secretary of Defense (Networks and Information Integration)	I&S Interoperability and Supportability	CIO Chief Information Officer	ISP Information Support plan	CPD Capability Production Document	JTRS Joint Tactical Radio System	DoD Department of Defense	MHZ Megahertz	E3 Electromagnetic Environmental Effects	MS Milestone	GHz Gigahertz	SAASM Selective Availability Anti-Spoofing Module	GPS Global Positioning System	TDL Tactical Data Link		TISP Tailored Information Support Plan
ASD (NII) Assistant Secretary of Defense (Networks and Information Integration)	I&S Interoperability and Supportability																	
CIO Chief Information Officer	ISP Information Support plan																	
CPD Capability Production Document	JTRS Joint Tactical Radio System																	
DoD Department of Defense	MHZ Megahertz																	
E3 Electromagnetic Environmental Effects	MS Milestone																	
GHz Gigahertz	SAASM Selective Availability Anti-Spoofing Module																	
GPS Global Positioning System	TDL Tactical Data Link																	
	TISP Tailored Information Support Plan																	

Table 5-3 is the NR-KPP status table in the Joint Interoperability Certification Memorandum and/or test report and provides the overall status of the Supportability requirements. The applicable items for the Supportability element are highlighted in the table.

Table 5-3. NR-KPP Status

INTEROPERABILITY REQUIREMENT	STATUS		REMARKS
	Threshold	Objective	
1. Solution Architectures; i.e., operationally effective information exchanges	<i>Status (i.e., Met)</i>	<i>Status (i.e., Not Tested)</i>	Degree of compliance with the requirements and expected operational impact. (i.e., Tested to the Threshold: All joint critical interfaces, not all of the interfaces for this system. There were no failures with a major or critical impact to the users. To minor failures occurred and evaluated by the users having no impact to their mission accomplishment.
2. Net-Centric Data and Service Strategy	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
a. Data Sharing Requirements	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
b. Service Sharing Requirements	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
3. GTG	<i>Roll-up Status</i>	<i>Roll-up Status</i>	
DISR	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
GESP/KIP	<i>Status</i>	<i>Status</i>	Degree of compliance with the requirements and expected operational impact.
4. IA	<i>Status</i>	<i>Status</i>	Statement that testing was performed in the approved IA configuration. Statement that the DAA issued an IATO/ATO, including date of issue and termination date.
5. Supportability			
a. E3 Program	<i>Status</i>	<i>Status</i>	E3 Test Report, EMI Test Report, or something similar and date.
b. Spectrum certification	<i>Status</i>	<i>Status</i>	DD1494 Status and date.
c. JTRS	<i>Status</i>	<i>Status</i>	If JTRS compliant-Met. If not JTRS compliant, waiver and date, or else Not Met.
d. GPS/SAASM	<i>Status</i>	<i>Status</i>	If SAASM compliant-Met. If not SAASM compliant, waiver and date, or else Not Met.
LEGEND:			
ATO	Authorization to Operate	GTG	GIG Technical Guidance
DAA	Designated Accrediting Authority	IA	Information Assurance
DISR	Department of Defense Information Technology Standards Registry	IATO	Interim Authorization to Operate
E3	Electromagnetic Environmental Effects	JTRS	Joint Tactical Radio System
EMI	Electromagnetic Interference	KIP	Key Interface Profile
GESP	GIG Enterprise Services Profile	N/A	Not Applicable
GIG	Global Information Grid	NR-KPP	Net-Ready Key Performance Parameter
		SAASM	Selective Availability Anti-Spoofing Module

(This page intentionally left blank.)

APPENDIX A – ACRONYMS

ADS	Authoritative Data Source
ASA	Additional System Attributes
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
ATO	Authorization to Operate
AV	All Viewpoint, All Views, Architecture View
BF	Blue Force
BFT	Blue Force Tracking
C&A	Certification and Accreditation
C4I	Command, Control, Communications, Computer, and Intelligence
CDD	Capability Development Document
CES	Core Enterprise Services
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMB	Configuration Management Board
COI	Community of Interest
CPD	Capability Production Document
DAA	Designated Accrediting Authority
DDMS	DoD Discovery Metadata Specification
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DoDIEA	DoD Information Enterprise Architecture
DSD	Data and Service Deployment
DSS	Data and Services Strategy
DT	Developmental Testing
E3	Electromagnetic Environmental Effects
ESG PWG	Equipment Spectrum Guidance Permanent Working Group
EVTS	Exposure Verification Tracking Sheets
FBCB2	Force XXI Battle Command Brigade and Below
GESP	GIG Enterprise Services Profile
GIG	Global Information Grid

GPS	Global Positioning System
GTG	GIG Technical Guidance
GTP	GIG Technical Profile
IATM	Integrated Architecture Traceability Matrix
IA	Information Assurance
IATO	Interim Authorization to Operate
IATT	Interim Authorization to Test
IAW	In Accordance With
IE	Information Exchange
IEA	Information Enterprise Architecture
IP	Internet Protocol
ISP	Information Support Plan
IT	Information Technology
JCA	Joint Capabilities Area
JCIDS	Joint Capabilities Integration and Development System
JCPAT-E	Joint C4I Program Assessment Tool-Empowered
JITC	Joint Interoperability Test Command
JPEG	Joint Photograph Experts Group
J-RAD	JITC Risk Assessment Database
JROC	Joint Requirements Oversight Council
JS	Joint Staff
JTRS	Joint Tactical Radio System
KIP	Key Interface Profile
KPP	Key Performance Parameter
M&S	Modeling and Simulation
MB	Megabyte
MCEB	Military Communications-Electronics Board
MDR	Metadata Registry
MGUE	M-code GPS User Equipment
MIL-STD	Military Standard
MOE	Measure of Effectiveness
MOP	Measure of Performance
N/A	Not Applicable
NCES	Net-Centric Enterprises Services
NR-KPP	Net-Ready Key Performance Parameter
NSS	National Security Systems
OT	Operational Test/Testing
OT&E	Operational Test and Evaluation
OV	Operational View/Operation Viewpoint

PM	Program Manager
PMO	Program Management Office
POC	Point of Contact
REST	Representational State Transfer
SAASM	Selective Availability Anti-Spoofing Module
SATCOM	Satellite Communications
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SST	Service Specification Template
SV	System View/Systems Viewpoint
TDL	Tactical Data Link
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TISP	Tailored Information Support Plan
TV	Technical View
UHF	Ultra High Frequency
US	United States
V	Version
VV&A	Verification, Validation, and Accreditation
WADL	Web Application Description Language
WSDL	Web Services Description Language
XML	eXtensible Markup Language
XSD	XML Schema Definition
XSLT	XML Style Language Translation

(This page intentionally left blank.)

APPENDIX B – DEFINITIONS

Accessible: An authorized user is able to discover and use data or services, subject to applicable laws, regulations, and policy restrictions. The provider offers instructions about the access request policy or active links to the data or service.

Authoritative: Recognized by appropriate governing authorities to be valid or trusted (e.g., the United States (U.S.) Postal Service is the authoritative source for U.S. mailing ZIP codes).

Authoritative data:

- Data that is provided or produced by an Authoritative Data Source (ADS)
- An ADS is a single, official, recognized producer/source of specific information
- (https://www.intelink.gov/wiki/C2_Authoritative_Data_Source_Working_Group/AuthoritativeDataSource)

Content data (i.e., data): Conveys information needed by the end-user to support a business or mission function. Content data is information that a user might need for the mission. It could be a text document, a spreadsheet, an image.

Core Enterprise Services: That small set of services, whose use is mandated by the Chief Information Officer, to provide awareness of, access to, and delivery of information on the Global Information Grid. (Department of Defense (DoD) Information Enterprise Architecture (DoDIEA))

Data asset: 1. Any entity that is composed of data, such as system or application output files, documents, databases, or web pages. For example, a database is a data asset that comprises data records.
2. Services that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a Web site that returns data in response to specific queries (e.g., weather.com) would be a data asset. (Data and Service Deployment (DSD))

Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. (DoDIEA)

Interoperability: The ability of systems, units or forces to provide data, information, materiel, and services to and accept the same from other systems, units or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. The Information Technology (IT) systems and National Security Systems (NSS) interoperability includes both the technical exchange of information and the operational effectiveness of that exchanged information as required for mission accomplishment. Interoperability is more than just information exchange. It

includes systems, processes, procedures, organizations, and missions over the lifecycle and must be balanced with Information Assurance (IA). Interoperability non-exclusively references data formats, signal levels, physical interface characteristics, logical or relational alignments, and transmission methods or media types. (Chairman of the Joint Chiefs of Staff Instructions (CJCSI) 6212.01E and DoDIEA)

Interoperable: 1. Many-to-many exchanges of data occurring between systems, through interfaces that are predefined or unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed. (DSD)

2. Data can be easily combined or compared with other information through shared formats and semantics. Semantics are the vocabularies, naming conventions, and translation tables needed for data or services to be compatible.

Metadata: 1. Descriptive information about the meaning of content data. Metadata can be provided in many forms, including eXtensible Markup Language (XML) information describing the characteristics of data; data or information about data; or descriptive information about an entity's data, data activities, systems and holdings. Metadata includes data type, source/origin, authority, structure, age/date, etc. (CJCSI 6212.01E)

2. Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata serves the same functions in resource discovery as good cataloging does by allowing resources to be found by relevant criteria and identifying resources. For example, discovery metadata is a type of metadata that allows data assets to be found using enterprise search capabilities.

Metadata Catalog: A system that contains the instances of metadata associated with individual data assets. Typically, a metadata catalog is a software application that uses a database to store and search records that describe such items as documents, images, and videos. Search portals and applications can use metadata catalogs to locate the data assets that are relevant to their queries. (DSD)

Metadata Registry: A system that contains information that describes the structure, format, and definitions of data. Typically, a registry is a software application that uses a database to store and search data, document formats, definitions of data, and relationships among data. System developers and applications are the predominant users of a metadata registry. (DSD)

Service: A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description. (DoDIEA)

Service Level Agreement: An agreement between service provider and consumer, specifying levels of performance, availability, operation, or other attributes of the service. Testers might receive it with the requirements package.

Service Specification: 1. A pivotal Service Oriented Architecture (SOA) deliverable that enables both Service Provider and Consumer to share a common view of a Service's behavior. "However, despite the importance of Service Specification there is no widely adopted standard." (SOA Process Blogspot, March 24, 2009)

2. A service specification is now required by policy (the DoD Service Strategies document and the DoDIEA document). Although there is no firm information on this, the Service Specification may be similar to the Service Level Agreement (SLA), but contains more details.

Service Specification Template: A common model for providing service description information (e.g., functionality, access methods, security mechanisms/restrictions, points of contact, performance information); it is still in development.

Trusted: Users and applications can determine and assess the authority and suitability of the source because the pedigree, security level, and access control level of each data asset or service is known and available. The user must be able to trust the data they access – by knowing who created it or provided it, where it came from, when it was created or if and when it was modified, who modified it and perhaps the reason, the classification level, and access control requirements. The user must also have information that the data or service provided is compliant with IA requirements. (DSD and DoDIEA)

Understandable: 1. Users and applications can comprehend the data and readily determine how the data may be used for their specific needs. Data attributes such as structure (subject and content), relationships, and semantics (vocabularies and taxonomies) are well-defined.

2. Service artifacts including the SLA describe the service and are available to unanticipated users/developers.

Universal Core: The small set of concepts which are universally understandable and thus can be defined across the enterprise. (DoDIEA)

Visible: Users and applications can discover the existence of data assets and services through catalogs, registries, and search services using common user terms. All data assets (intelligence, non-intelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset. (DSD)

(This page intentionally left blank.)

APPENDIX C – INTEGRATED ARCHITECTURE TRACEABILITY MATRIX METHODOLOGY

OVERVIEW

The Integrated Architecture Traceability Matrix (IATM) methodology is a standardized approach to Solution Architecture requirements analysis that facilitates test planning and risk reduction to the Program Manager (PM) and Joint Interoperability Test Command (JITC).

Solution Architecture compliance is one of five elements of the Net-Ready Key Performance Parameter (NR-KPP) that must be evaluated to certify a system for interoperability. The solution architecture is the fundamental mechanism across the Department of Defense (DoD) for building and integrating capabilities, identifying strategic requirement shortfalls, and developing test and evaluation strategies. A system's solution architecture is detailed in its requirements documents, architecture views, and Information Support Plans (ISPs)/Tailored Information Support Plans (TISPs) in textual, tabular, and graphical formats.

Although the IATM is developed during the requirements analysis phase, the information it provides feeds all stages of the test and evaluation process, as illustrated in Figure C-1.

A compartmented, top down approach is frequently used to build architecture views, resulting in a higher rate of disconnects between compartments. This architectural design approach is used when systems are built to known operational requirements. The operational requirements are documented in operational views first, followed by the systems views and then technical views. Each sequential view within a compartment (i.e., Operational View (OV), System View (SV), or Technical View (TV)) contributes to the next within that compartment. Therefore, it is common for each series of views within a compartment (operational, systems, technical) to be built in sequential order after determining which products are needed. Time constraints (or lack of training) may prevent architects from performing a "crosswalk analysis" of requirements across compartments to confirm detail accuracy and completeness. The IATM provides that crosswalk between operational, systems, and technical views and provides a tool to identify disconnects and high-risk areas.

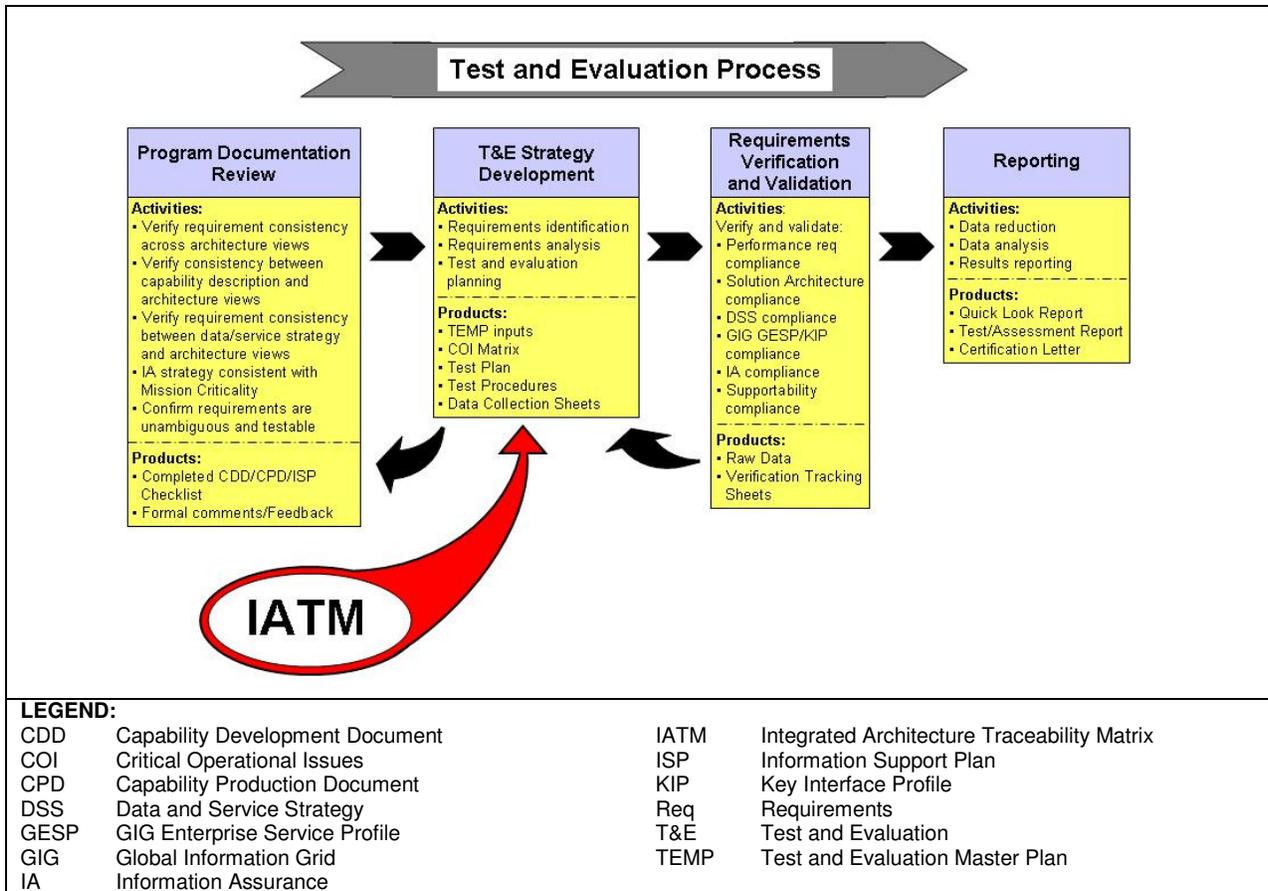


Figure C-1. Integrated Architecture Traceability Matrix Application

SCOPE

This paper provides the process used to develop the IATM, its functionality, and how to use it to identify testing requirements, develop the Test and Evaluation (T&E) strategy, support solution architecture documentation reviews, and determine Solution Architecture compliance.

DESCRIPTION

The IATM provides a comprehensive picture of the threshold and objective Solution Architecture requirements for a given system and a tool for requirements analysis. The IATM is initially developed at the onset of T&E Strategy development and refined as the capability matures and testing occurs. The IATM is created by mapping the operational, systems, and technical requirements identified in the architectural products to key information (e.g., Key Performance Parameters (KPPs), Additional System Attributes (ASAs), and Data and Service Strategy (DSS) element) identified in the requirements documents (e.g.; Capability Development Document (CDD), Capability Production Document (CPD), ISP).

From left to right, Figure C-2 indicates that the KPPs identified in the CDD and CPD can be associated with the operational activities in the OV-5. The SV-5 correlates the operational activities in the OV-5 to the system functions. This makes it possible to associate Information Exchanges (IEs) in the SV-6, transport structure in the SV-2, and the applicable standards in the TV-1 to the operational activities and, by earlier association, the KPPs. The results provide a baseline map (shown in the bottom half of Figure C-2).

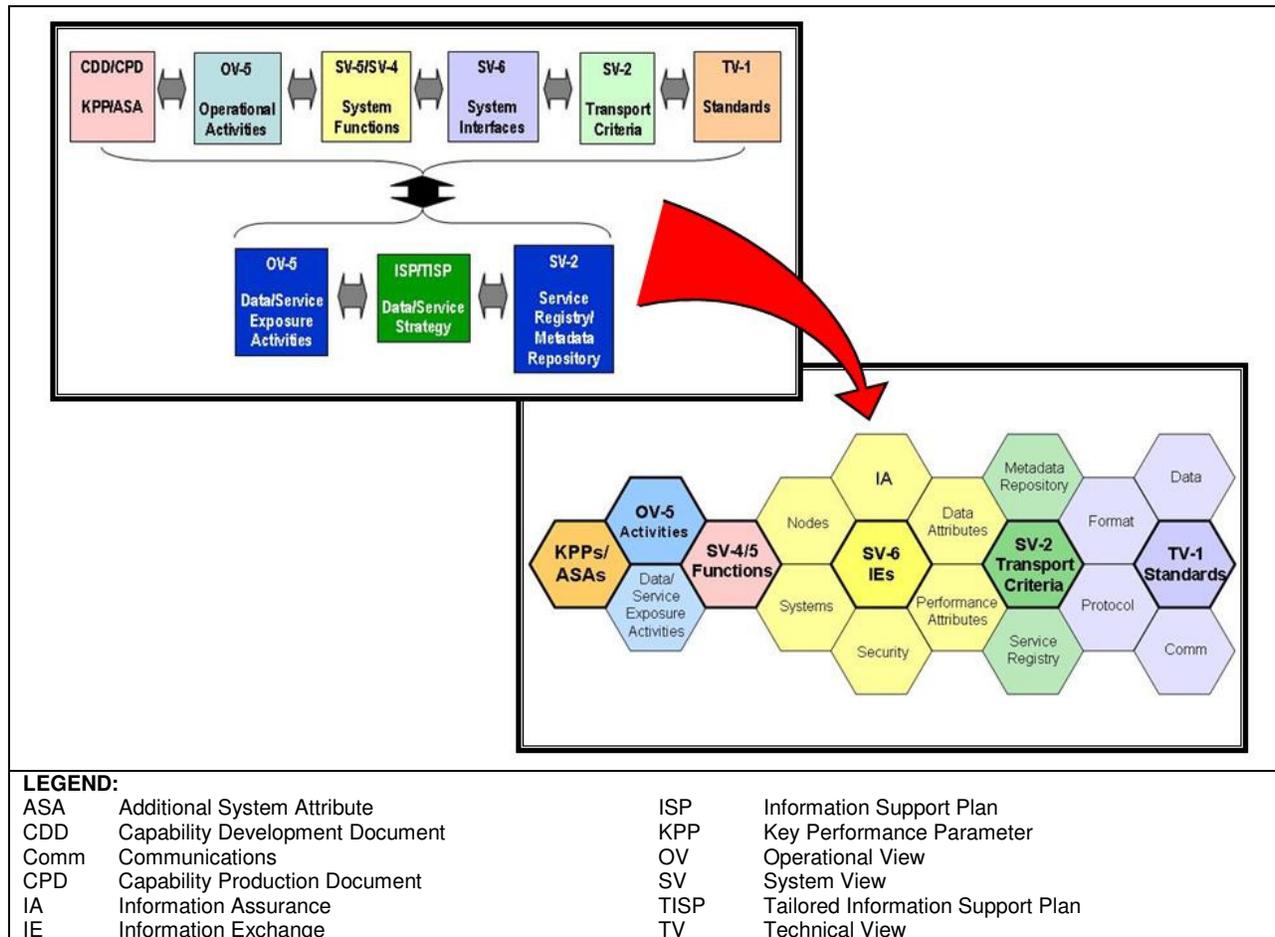


Figure C-2. Mapping the Integrated Architecture Traceability Matrix

The DSS requirements may also be linked to the baseline map to highlight key IEs and their associated operational activities that support the DSS. After the transport structure is identified, the Global Information Grid (GIG) Enterprise Service Profile (GESP)/Key Interface Profile (KIP) requirements (identified in the CDD, CPD, or ISP) can then be associated with their applicable IE and operational activity. The resulting map:

- Identifies the threshold and objective solution architecture for the system.
- Shows relationships between system requirements and operational requirements in one picture.

- Identifies critical IEs.
- Identifies relationships between IEs and operational activities, facilitating the mapping of IEs to mission threads.
- Identifies standards that support critical IEs and operational activities.
- Identifies IEs that support the system's DSS, their associated standards, operational activities, and KPPs.
- Identifies those interfaces and associated activities that have GESP/KIP requirements.
- Simplifies the identification of potential disconnects; e.g., missing IEs, DSS dependencies that might have problems, and non-critical IEs that should be critical.

METHODOLOGY

The IATM methodology consists of building the IATM, applying the IATM, and updating the IATM.

Building the IATM

STEP 1. Ensure you have the tools and minimum data required to build the IATM. These include a spreadsheet application, the system's CDD, CPD, or ISP and the associated architecture views. At a minimum, the views should include the OV-5, SV-2, SV-4, SV-5, SV-6, and TV-1. Having Joint Staff J-6-certified documents provides additional benefits, but is not required to create this product.

Completion of steps 2 through 9 will result in a baseline IATM product with the core elements as shown in Figure C-3.

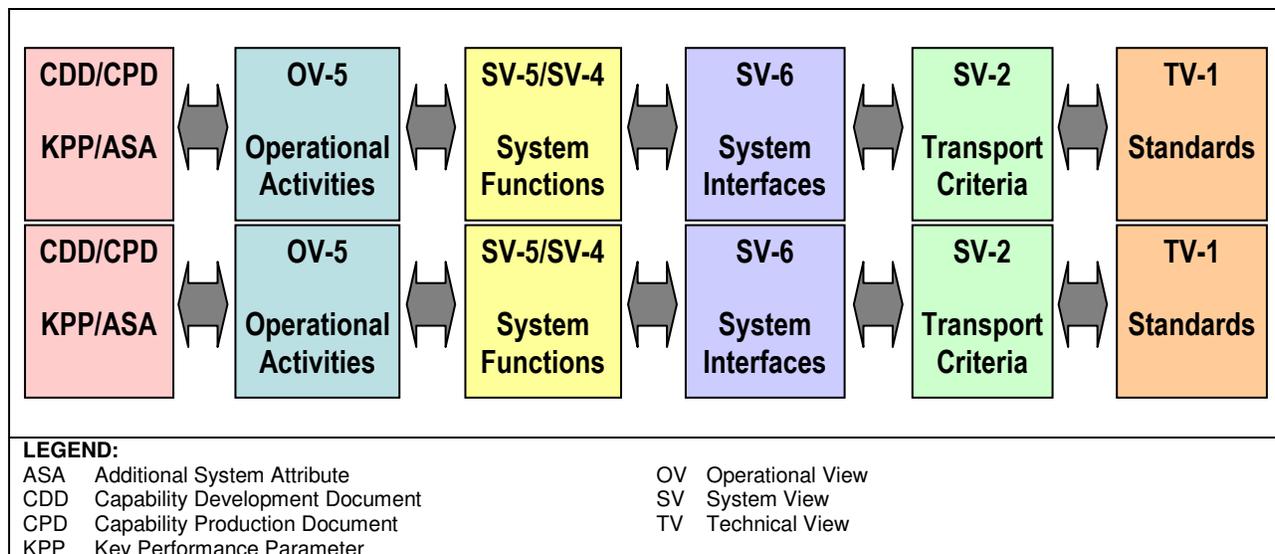


Figure C-3. The IATM Baseline

STEP 4. Using the SV-4, map the appropriate system function to each IE. The SV-4 identifies the system functions. A well created SV-4 will define each of the system functions, making it easier to map the function to the IE. In some cases, it may be easier to determine the operational activity (by examining the IE shown in the OV-5) than try to identify the system function. If the name of the data exchanged matches the name of the activity, as shown in Table C-1, it is recommended that the operational activity be identified first. The SV-5 can then be used to identify the applicable system function, as shown in Table C-2.

Table C-1. Information from Operational View-5

<u>Activity</u>	<u>Data exchanged</u>
Manage sensor plan	sensor plan

Table C-2. Information from System View-5

<u>Activity</u>	<u>System function</u>
Manage sensor plan	sensor plan manager

STEP 5. Populate the OV-5 Activity column with the applicable operational activity. The OV-5 describes each operational activity and subordinate activities. The SV-5 should correlate the functions with their applicable operational activity. If the SV-5 is missing, use the activity definitions in the OV-5 to guess or leave blank. Upon completion of the matrix, request a PMO architecture team review through your Government Action Officer, unless directed otherwise. It is recommended that a guess be identified using a different color font for the activity. This will highlight those areas of the matrix requiring more PMO focus.

STEP 6. After analyzing the KPP and ASA definitions in the CDD, CPD, or ISP/TISP, identify the KPP or ASA associated with each operational activity. The IEs that implement information assurance requirements should be mapped to the NR-KPP. If the correlation is not obvious, a PMO architecture team review should be requested upon completion of the matrix.

Steps 7 and 8 can be completed as early as Step 4 without an impact to the process or completion time.

STEP 7. Using the SV-2, identify the communications media (e.g.; Secret Internet Protocol Router Network, Asynchronous Transfer Mode) used for the IE. Some programs will incorporate the communications information into the SV-6.

STEP 8. Identify the applicable standards listed in the TV-1 for each IE. Standards should be identified for the communications used, message format, and any applicable protocols or data.

KPP/Attribute	OV-5 Activity	SV-4 Function	System Data Exchange	Content Exchange	Interface Name	Sending System	Sending Node	Receiving System
Net-Ready KPP	A.1 Post & Disseminate Information A.1.2 Post Information to the Enterprise	Product Distribution	Product Request	PMSlip Request	SFTS-MSS	SFTS	PS	MSS
Net-Ready KPP	A.1 Post & Disseminate Information A.1.2 Post Information to the Enterprise	Product Distribution	Product	PMSlip	MSS-SFTS	MSS	MOC	SFTS
Health & Status Tracking KPP	A.3 Monitor H&S A.3.1 Request H&S	Attnr Reporting	Health Status Report	Health Data	KOM-FHS	KOM	CH2	FHS
Health & Status Tracking KPP	A.3 Monitor H&S A.3.2 Collect H&S	Temp Monitor	KTamp	Temperature	TMS-FHS	TMS	KBB	FHS

Receiving Node	SV-2 Comm	Technical Criteria						TV-1 Standards
		Criticality	Classification	Timeliness	Accuracy	Reliability	Usability	
MOC	Internet	High	Unclass	NRT	.95	.95		IP, MDS
PS	Internet	High	Unclass	NRT	.95	.95		IP, MDS
MOC	FHNet	Low	Unclass	1/day	.65	.50		IP, MDS
MOC	FHNet	High	Unclass	Real Time	.99	.99		IP, MDS

NOTE:
The figure above is a fictitious example of IEs and their applicable functions, and activities that would be found in an SV-6 mapped to the applicable KPP found in the CDD/CPD.

LEGEND:

Attnr	Attendance	KTamp	Kids Temperature
CDD	Capability Development Document	MDS	Moms Data Standard
CH2	Child #2	MOC	Moms Operation Center
Comm	Communications	MSS	Moms Support System
CPD	Capability Production Document	NRT	Near Real Time
FHNet	Family Home Network	OV	Operational View
FHS	Family Health System	PMSlip	Permission Slip
H&S	Health and Status	PS	Private School
IATM	Integrated Architecture Traceability Matrix	SFTS	School Field Trip System
IE	Information Exchange	SV	System View
IP	Internet Protocol	Temp	Temperature
KBB	Kids Bunk Bed	TMS	Temperature Measuring System
KOM	Kids Own Mouth	TV	Technical View
KPP	Key Performance Parameter		

Figure C-5. Example Baseline IATM

Step 8 completes the baseline IATM. At this point, all external interfaces should be mapped to a system function, operational activity and KPP or ASA. The baseline IATM provides the threshold and objective solution architecture for the system and supports constructive requirements documentation review. Figure C-5 above shows an example baseline IATM.

To expand the IATM's functionality, requirements for DSS and GIG Technical Guidance (GTG) compliance can now be mapped to identify relevant IE's, system functions and operational activities as reflected in Figure C-6.

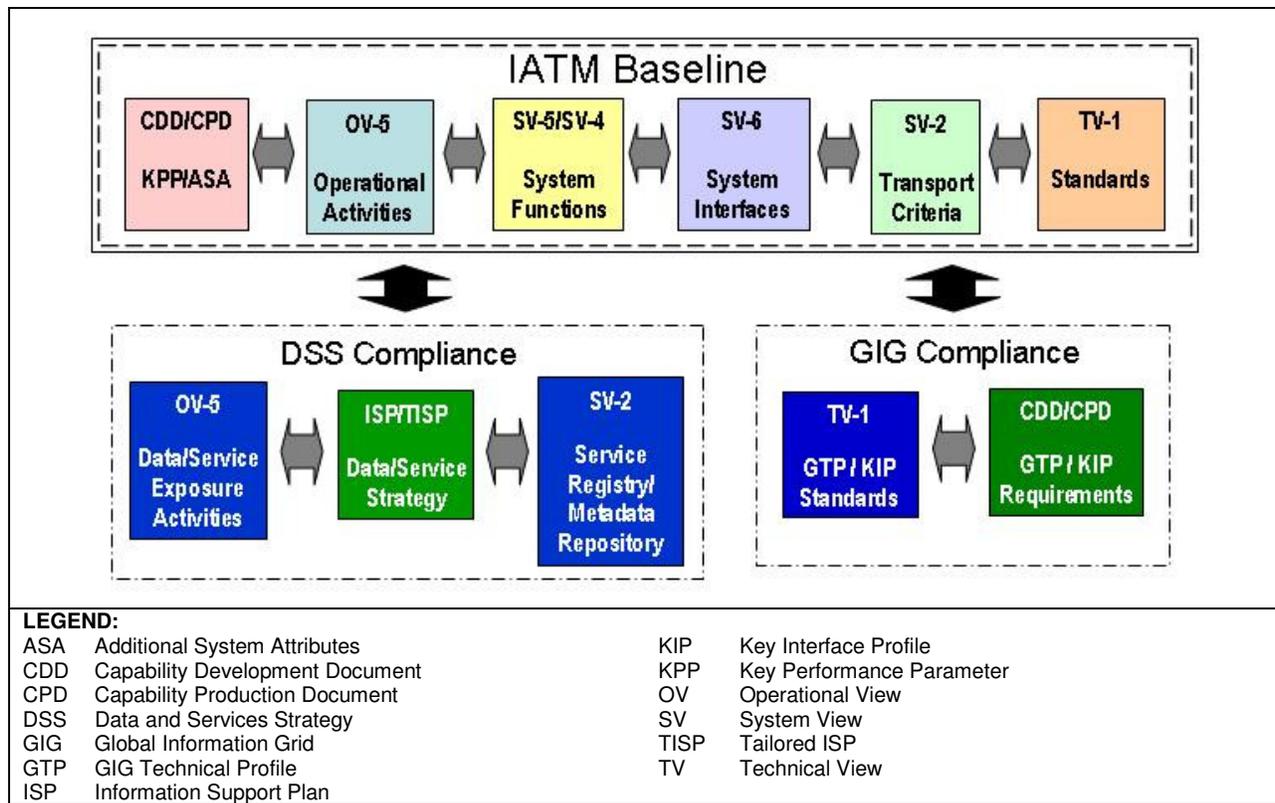


Figure C-6. Expanded IATM

STEP 9. Identify the IEs that support the DSS of the system using a combination of the OV-5, SV-2 and the ISP/TISP. Options include highlighting the row or adding an additional column and placing an "x" in the cell to mark the applicable IEs.

STEP 10. Add a GTG requirements column to the baseline IATM. Use this column to identify the applicable GESPs, recently renamed GIG Technical Profiles (GTPs). List the applicable KIPs, the precursor to GESPs, if the system documentation identifies them. The GTPs will replace related KIPs as they are mandated. Add the GESP or KIP standards to the standards column. The GTG requirements column can be sorted to group IEs that may need testing to support GTP compliance assessment. As there are few KIPs approved and currently no GESPs developed, the application of this step may provide limited benefits.

STEP 11. Apply an auto filter to the following columns: KPP/ASA, OV-5 Activities, SV-4 Functions, Sending/Receiving Systems and Nodes. This is accomplished by using the cursor to highlight the appropriate columns and the filter tool under the Tools menu. This allows a tester to group IEs according to KPPs, operational activities, nodes or systems (sending or receiving) providing added benefit to requirements analysis and test planning processes.

Step 11 allows a tester to quickly analyze the requirements and identify inconsistencies and discrepancies. For example, sorting by Activities will provide a smaller set of IEs for each activity. These IE sets can then be easily sequenced to identify if any IEs are missing. Upon analysis completion, it is advisable to request the PMO architecture team review the IATM for accuracy, resolve any inconsistencies and discrepancies, and assist in identifying any missing information.

Apply the IATM to Test and Evaluation Strategy Development. Architecture documentation sometimes falls short of providing the requirement details, non-ambiguity, and relationships needed for meaningful analysis, constructive feedback, and cost-effective T&E strategy development. Problems are frequently not discovered until testing occurs, resulting in an opportunity lost or time wasted. The following applications of the IATM will benefit the tester, PMO, developer, and user.

Threshold and Objective Solution Architecture Identification. Using a sort feature or automatic filter, sort the IATM by KPPs and ASAs. The combination of all KPP interfaces and all critical interfaces that map to an ASA defines the threshold solution architecture for the system. The resulting IATM provides a picture of the objective solution architecture, including the threshold solution architecture and all non-critical interfaces.

Critical IE Identification. The criticality of an IE is sometimes missing from the SV-6. Without knowing the criticality, test scope is difficult to determine. The IATM can be used to provide an idea of the criticality of IEs. Sort the IATM by KPPs and ASAs. According to CJCSI 6212.01E, a KPP is a capability or characteristic considered essential for successful mission accomplishment. Failure to meet a system or program's KPP threshold can be cause for the system to be re-evaluated or program reassessed or terminated. Therefore, by definition, IEs that map to a KPP should be identified as critical unless sufficient justification exists to be non-critical. Coordination with the PMO architecture developers will clarify and validate IE criticality.

Architecture Documentation Reviews. The IATM facilitates a comprehensive review of program solution architecture documentation. The following are examples of how the IATM matrix can be used to support the identification of inconsistencies and discrepancies within a requirements document.

- Identify inconsistencies between architecture views.
- Identify inconsistencies between different SV-6s of a system. Add an additional column for each SV-6 analyzed (e.g.; CDD, CPD, ISP, TISP) using the document title (e.g.; CDD, ISP, CPD) and document date as the column title. Number each row of the SV-6 being reviewed and identify the row number for each IE in the applicable IATM column. By adding a column for each document/SV-6 reviewed, the requirement differences between products will be highlighted and allow for additional scrutiny. Clarification should be requested from the PMO architecture team where differences between a previously J-6 approved SV-6 for a CDD and a non-approved SV-6 for a CPD are not explained in the requirements document.

- Identify missing IEs. Sort the IATM by KPPs and ASAs, and then by activities. This will identify all IEs involved to accomplish each activity for any given KPP or ASA. The IEs for each activity can then be visually sequenced. This process will identify IEs that may be missing. For example: An activity that has a data response without a corresponding data request is a potential deficiency.

Mapping IEs to Mission Threads. Using the sort feature or automatic filter, sort the IATM by Operational Activities. A mission thread is made up of a series of operational activities. As mission threads are created for testing, the IATM will quickly identify the IEs that will support each activity being exercised, providing a basis for test planning.

Standards Risk Analysis Support. The IATM identifies the standards used to support KPPs and thus critical IEs in one picture. The application of standards that support critical IEs and KPPs should bear closer scrutiny to reduce the risk of a KPP failure due to the application of standards.

Data and Service Strategy Support. Upon completion of step 9 (above), the IATM will identify the IEs that support the data and service strategies and their associated system functions and operational activities. If a DSS column is added, the IATM can be sorted to group those relevant IEs. These rows can then be printed and used as a quick reference during test planning meetings (provided the IATM is unclassified). As Developmental Testing (DT) and operational testing events are scheduled, and system functions and activities are identified for the test events, a tester will have the advantage of knowing which test events will provide the optimum data for data and service strategy assessment. This knowledge also provides leverage during test planning meetings. It is not uncommon for developers to change the content of a DT prior to the event to satisfy their specific needs. The JITC observer will have a more informed idea of the impacts these changes have on their ability to collect DSS data and, through negotiation, may be able to influence the testing to accommodate their needs.

GIG Compliance Assessment Support. The GIG compliance is primarily met by a system's correct application of GESPs and/or KIPs and their applicable standards. Adding a column in the IATM to identify those IEs and functions that have GIG requirements (as indicated in Step 10, above) allows a tester to capture a snapshot of the portion of the threshold solution architecture that has GIG requirements. This snapshot can then be used to address the GIG requirements in the Test Plan and Test Report.

Test Planning. The threshold solution architecture is the minimum testing required to adequately assess Solution Architecture compliance. The IATM defines the threshold solution architecture and provides a basis for test planning and cost estimates. Any testing beyond the threshold should be at the PM's specific request.

The system's Test and Evaluation Master Plan (TEMP) will sometimes identify the functions that will be tested during Developmental Test and Evaluation. If this is the case, the relationships between the IEs and functions in the IATM can be used in conjunction with the TEMP to identify which IEs will be tested during which DT events. Through analysis, the IATM will distinguish those IEs, and thus functions, that are most at risk. This will provide a means to identify early which DT events should be observed to best support the system assessment.

Adding additional columns for test events (e.g.; Scheduled Events, Date Tested) will provide a place to identify and track when an IE will be tested or was tested. This can be used for future test planning.

Risk Reduction. The IATM maps testable system requirements to operational requirements (operational activities) providing traceability back to user requirements and the Universal Joint Task List. This visible linkage is useful to facilitate PM buy-in to the scope and methodology of testing. Both are high risk areas for PMs. The scope (i.e., location, duration, and cost) of any given test is dependent on the mission threads (i.e., operational activities) being tested and the minimum data collections needed to adequately assess requirements compliance for those mission threads. By sorting the IATM data by operational activities, a test planner can identify the minimum data collection needed for a given mission thread, and thus identify testing locations, duration, and costs. Additionally, since the IATM is based on the PMO-developed solution architecture, the PM feels empowered that he dictated the scope of the test, minimizing PM resistance. This reduces risk to JITC. The benefits gained by requirements analysis and documentation review of the IATM, mentioned above, reduces inconsistencies in program requirements, reducing the PM's system development risk.

Updating the IATM. As new program documents are released for review, the IATM should be updated to reflect the new information. It's important to track those changes that are due to system maturity and those that result from missed information or mistakes. Working closely with the PMO architecture team will resolve most, if not all, of the uncertainties. Add a new row in the IATM for each new IE added to the system. If an IE test criteria has changed from a Joint Staff-approved requirement, add the IE to a new row immediately below the approved IE and highlight the row to track the change. Once the new IE has been approved by the Joint Staff, delete the previously approved IE.

CONCLUSION

The IATM methodology is a Solution Architecture requirements analysis tool. The methodology was created to provide a consistently reliable and trustworthy process to identify the threshold and objective Solution Architecture requirements and thus identify the T&E scope for the Solution Architecture element. The methodology includes building the IATM, application of the IATM, and updating the IATM.

The IATM provides a crosswalk between operational, systems, and technical views built from solution architecture products and other requirements documents. The IATM provides a sound basis for T&E strategy decisions while reducing risk to the PM and JITC. Although developed during the requirements analysis phase, the information gleaned from the IATM feeds all stages of the T&E process. Key benefits of the IATM include:

- Maps KPPs to the operational activities, system functions, joint interfaces, transport and associated standards
- Enables PMO support with sound advice for resolving program documentation conflicts
- Identifies Joint interfaces and standards that are critical for each KPP
- Identifies critical gaps and disconnects in the architecture design, and potential risks in the system design
- Identifies components of the Solution Architecture that are key to the DSS and GTG Compliance elements of the NR-KPP
- Identifies the optimum interfaces to test for adequate interoperability certification testing
- Provides traceability back to user requirements and mission threads
- Supports requirements analysis
- Supports test plan development
- Supports standards risk assessment
- Supports DSS and GIG compliance evaluation
- Provides a tool for tracking the interoperability certification progress

The IATM methodology and tool supports DoD policies and directives, provides clarity and scope to the test planning process, and facilitates consistently sound T&E strategies and interoperability assessments.

APPENDIX D – DATA AND SERVICES STRATEGY TEST PROCEDURES

This appendix provides the test methodology and high-level test procedures necessary to assess the Data and Service Strategy (DSS) element of the Net-Ready Key Performance Parameter (NR-KPP).

These steps are organized according to specific objects that the testers must examine rather than by requirement. Text blocks in the right-hand margin notify the reader of applicable requirements addressed by nearby test procedures.

PREPARE FOR ASSESSMENT

Obtain Requirements Documentation. Before testing, the Joint Interoperability Test Command (JITC) will receive the Joint Staff (JS)-certified requirements documents for the capability, system, or service to be tested or assessed. These may consist of a Capability Development Document, Capability Production Document, and Information Support Plan or Tailored Information Support Plan. This package should contain Department of Defense (DoD) Architecture Framework (DoDAF) viewpoints and Exposure Verification Tracking Sheet (EVTS). If these are not included with the JS-certified requirements documents, the tester must request the program manager or Point of Contact (POC) provide supporting DoDAF products (e.g., an Operational Activity Model) and other architecture descriptions. For programs with limited documentation, testers should request System Design Requirements, Standards Support Documents, segment specifications, Final Requirements Document, etc., from the POCs.

The Chairman of the Joint Chiefs of Staff Instruction 6212.01E and the Joint Oversight Council 010-081, 14 January 2008, require that interoperability test certifications be based on JS J-6-certified requirements documents. The JITC document #08-001, "JCPAT-E Search for J-6 Certified Requirements Documents," provides detailed guidance for obtaining these documents from the Joint Command, Control, Communications, and Intelligence Program Assessment Tool-Empowered repository. This document can be obtained from the JITC Intranet at the "Updates" tab.

Obtain data/service-sharing artifacts. The JITC testers will require all documents that explain or clarify the data/service sharing methods. Artifacts include data structures and models (i.e., entity relationship diagrams, taxonomies, and ontologies), data dictionaries and/or vocabularies, data schemas, and documentation for data access mechanisms, as appropriate. The JITC testers do not currently receive any of these artifacts. Nevertheless, they are necessary for assessment of the DSS element. Testers should request these items from the program office as well as a manifest listing of the items and their explicit versions and revision dates. The JITC testers should compare received artifacts against the architecture product viewpoints to identify

missing artifacts. Discrepancies should be reported to the program manager or POC. The JITC cannot complete testing without all appropriate artifacts.

Identify Shared Service and Data Assets. Testers must determine what data assets and services are required to be shared. The tester will use a program's completed Data and/or Service EVTS as a basis for determining what services and data assets are required to be shared. In many cases, the program will not have a completed EVTS, and the testers will have to contact the program's POCs to identify existence of services and data assets that are required to be shared.

"Authoritative source" data assets must be shared. "Authoritative data sources" are identified by the Community of Interest (COI) in which the capability participates. If the COI has identified any authoritative source data assets, these must be assessed as shared data assets.

ASSESS DATA SHARING REQUIREMENTS

The data sharing test procedures apply if the system produces or provides data that are shared with external users. Perform the following test procedures for each shared data asset.

1. Examine DoD Metadata Registry. Shared services and data assets are made understandable by publishing descriptive and explanatory artifacts and semantic and structural metadata in the DoD Metadata Registry (MDR).

For data assets, the MDR contains Information Resources (IRs) (or data sharing "artifacts") such as eXtensible Markup Language (XML) Schema Definitions, XML instances, data models (e.g., entity relationship diagrams), XML Style Language Translations (XSLT) documents, domain value documents, and taxonomies and ontologies (e.g., Web Ontology Language files). These and other appropriate artifacts are registered in the DoD MDR to enable discovery by unanticipated users and developers. The IRs are submitted to the MDR in a submission package. The Concept of Operations for the DoD MDR, Version 1, defines a submission package as "a zipped file containing the XML schema files and a manifest.xml file describing the information resources contained within the zip file."

If the data asset has an associated service (data access mechanism), the MDR submission package should also contain service artifacts such as Web Services Description Language (WSDL) or Web Application Description Language (WADL) files in addition to the data structures, models, and schemas. Other service artifacts may include user guides and readme files, Service Specifications, Service Level Agreements (SLAs), and access control policies.

- a. Login to the MDR. Web site address for the MDR is:
<https://metadata.dod.mil/mdr/homepage.htm>.

b. Verify that registry entries exist for all artifacts (as appropriate for the specified data asset).

Data is Understandable
- Register data artifacts in DoD MDR

c. Download all artifacts registered in the MDR. Verify that artifacts downloaded from the MDR are logically equivalent to the artifacts received from the program office. Verification of logical equivalency may require an automated software tool or a trained software engineer.

d. Verify the artifacts on the MDR are a proper reflection of the current system. Verify no outdated or developmental drafts are posted.

e. Verify that data asset/service documentation is sufficient to provide unanticipated users (developers) with adequate information to consume the data asset and/or service.

f. Verify that semantic vocabularies reuse elements of the Universal Core (UCore) standard. Verify that XML schema documents are valid; i.e., schema (.xsd) files conform to current industry standards (e.g., World Wide Web Consortium, UCore) and support associated data models. This may be tested during Global Information Grid (GIG) Technical Guidance (GTG) standards conformance testing using automated tools. Previous results may be used to answer this test procedure.

Data is Interoperable
- Base vocabularies on Universal Core (UCore)
- Comply with COI data-sharing agreements

2. Examine shared data location. A shared space is a data storage location that allows or enables the stored data to be accessible to authorized users. This includes anticipated users (i.e., known users with specific missions that have been granted access to the system) and unanticipated users (i.e., users without specifically defined missions who have been granted access to the system). An unanticipated user is a user which was not anticipated but who may be authorized to access the service.

a. Verify the content data that originated from the data asset is available in the shared space.

Data is Accessible
- Post data to shared space
- Provide serving (access) mechanism

b. Verify that the shared space provides serving mechanisms. Data access is generally accomplished via a service. Procedures for assessing serving mechanism are in step 7.

c. Verify that the content data is accessible to authorized end users. Verify that data are available to the system, capability, application, or user attempting to access it (within policy, regulation, or security guidelines).

d. Verify that the data provider has written policy for user access. A written

Data is Accessible
- Provide access policy

access control policy provides the steps by which a user/developer may request access to the service. If the data is not accessible to all users, verify a written policy on how to gain access is available to unanticipated users.

e. Verify that policy information is provided upon requests for access and upon attempts to login.

f. Verify that the written policy lists actions necessary to gain user access to data via user level credentials, system level credentials, or trust relationships (e.g., Access Control List).

g. Verify that policy details are implemented as described. Review written policy and verify that the access rights granted are equivalent to those stated in the policy. Testers should attempt to gain access using various authorizations. Verify that:

- unauthorized users cannot gain access
- authorized but unanticipated users can gain access upon following policy
- authorized users can gain access.

3. Examine the enterprise catalog. Data asset/service discovery occurs when a user performs a search using an enterprise search capability and discovers a data asset or service that suits a mission need. Data and services must be advertised by virtue of having been registered in the Net-Centric Enterprise Services (NCES) Enterprise Catalog or other compatible/federated enterprise catalog. The tester must have access to the catalog. Testers should obtain the location and login requirements of the enterprise or community catalog.

a. Login to the NCES Enterprise Catalog or other compatible/federated enterprise catalog. Execute a search for each data asset to be assessed. The tester must be provided with adequate knowledge of the data asset to determine appropriate search terms (keywords). The tester will "guess" appropriate "keywords" in an attempt to "discover" the specified data asset/ service.

- Access the GIG Gateway (also known as "Enterprise Search webpage").
- Enter keywords into search text box.
- Specify the COI/sponsor for the data by clicking on the appropriate check boxes.
- Click on the search button.

b. Verify that logical keywords (search terms) are suitable to find the data asset. Verify the data asset discovered is consistent with the keywords used to search for it. Verify data asset's search terms/keywords are appropriate for mission area or data type.

Data is Visible

- Use appropriate keywords for discovery
- Post discovery metadata in an Enterprise Catalog

c. Verify a catalog entry exists that describes the data asset. These are commonly referred to as "metacards." Each metacard should include information

about the data item (e.g., data file) to allow discovery and to provide security restrictions and pedigree of the data.

d. Verify the metacard contains DoD Discovery Metadata Specification (DDMS)-conformant metadata to include data pedigree and security metadata, and the authoritative source for the data (when appropriate). The purpose of the pedigree is to enable consumers to determine whether the asset is fit for their intended use and to enable them to track the flow of information, its transformations, and modifications, through assets. Notional metadata describing an asset's pedigree would include creation date, modification date, processing steps (including methods and tools), source and author (if known) status, and validation results against a published set of constraints. The Resource Descriptors elements of the DDMS allow identification of the author, publisher, and sources contributing to the data, allowing users and applications to assess the derivation of the data (i.e., data pedigree). This metadata allows users and applications to select data from known sources. Reliable and quality sources will become more widely used, enhancing overall data quality throughout the enterprise as more data sources become visible. The DDMS conformance may be tested during GTG standards conformance testing using automated tools. Results from testing that element may be used to answer this test procedure.

Data is Trusted - Provide information assurance and security metadata Data is Understandable - Publish semantic and structural metadata
--

e. Verify metadata logically correspond to the data described.

f. Verify that security metadata is accurate and appropriate.

g. Verify the authoritative source of data is correct (if applicable).

h. Verify the entry includes a link (e.g., Uniform Resource Identifier (URI)) to the data asset.

Data is Accessible - Publish active link to data asset
--

i. Verify the link is active and resolves to the data asset.

4. Collect and examine samples of the data asset(s). Collect data samples from each shared data asset. Ensure samples are representative of all data schemas.

a. Verify record-level database tagging and in-line document tagging comply with DDMS and include data pedigree and security metadata as well as an authoritative source for the data (when appropriate).

Data is Interoperable - Conform to DDMS

b. Verify that data samples (e.g., XML instance documents) conform to the data schema standards. This may be validated using automated test tools.

c. Obtain COI vocabulary definitions for comparison to the program data schemas and content. Verify XML instances conform to COI-developed vocabulary (semantics), as appropriate.

ASSESS SERVICE SHARING REQUIREMENTS

The service sharing test procedures apply if the system provides services that are shared with external enterprise users. Perform the following test procedures for each shared service.

5. Examine DoD MDR. For services, the MDR contains IRs (or service sharing "artifacts") (e.g., WSDL files and XSLT files) in addition to the data structures, models, and schemas (as appropriate). Procedures for examining the DoD MDR and data/service sharing artifacts are in step 1.

Services are Understandable - Publish service artifacts to DoD MDR
--

6. Examine available service registries. A service registry provides a location for data access mechanisms and other services to be advertised. The NCES Service Registry may be searched using the NCES Service Discovery service, which is available through the "GIG Gateway" (also known as the "Enterprise Search webpage"). The NCES Service Registry is also known as the NCES Universal Description, Discovery, and Integration (UDDI) Node.

a. Login to the NCES Service Discovery Service or other enterprise service registry. Execute a search for the service to be assessed. The tester must be provided with adequate knowledge of the service to determine appropriate search terms (keywords). The tester will "guess" appropriate "keywords" in an attempt to "discover" the specified service.

Services are Visible/Understandable - Publish a description of the service or access mechanism to the NCES Service Registry

b. Verify that a registry entry exists for the data access mechanism or service.

c. Verify that logical keywords (search terms) are suitable to find the specified service. Verify the service discovered is consistent with the keywords used to search for it. Verify that the service's search terms/keywords are appropriate for mission area or service type.

Service is Visible - Comply with enterprise-specified minimum service discovery requirements
--

d. Verify that the registry entry complies with enterprise-specified minimum service discovery requirements (e.g., UDDI).

e. Verify that the registry entry provides location of WSDL (or WADL) files, data schemas, and valid endpoints.

Services are Accessible

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

f. Verify that the registry entry provides an active link to the service. An active link is defined as a link that resolves to a working service node (or webpage).

g. Verify that the registry entry's metadata logically corresponds to the service it describes.

7. Examine service(s). The JITC testers must determine how the data asset is to be accessed. User access via web browser is accomplished using a Representational State Transfer (REST)-based approach. REST is a protocol used to allow user interaction on a Web site. Machine-to-machine access occurs when a software application (client) is used to access the data asset. Simple Object Access Protocol (SOAP) is commonly used in these client-server applications. The JITC tester must determine what type of serving mechanism is used and execute the appropriate method to access the data asset. For a REST-based application, the tester may only require a login account and password. However, a SOAP (machine-to-machine) application may require client emulation software such as SOAPUI. SOAPUI is a web service testing tool available at JITC.

a. Access the service. This may require a login action.

b. If the service uses a SOAP-based access method, verify that WSDL operations execute as required. This may be confirmed in operational tests and interoperability tests. The WSDL files are not required to contain valid web address information.

c. If the service uses a REST-based access method (e.g., a web interface), verify that WADL operations (Web site operations) execute as required.

d. Verify that service specifications or SLAs exist for

Services are Understandable

- Provide service specification or SLA

each service. A Service Specification Template serves as the common model for providing service description information. The SLAs define and advertise operational status and performance of services to consumers.

e. Verify that the service specifications captures the following information about the

Services are Trusted

- Include security mechanisms or restrictions in the service specification
- Operate services in accordance with SLA

service: what the service does; how users can access the service; which security mechanisms or restrictions apply to the service; POCs for the service

(e.g., the name, contact information for the service provider); service-level characteristics; and performance information.

f. Verify that the service is operated in accordance with (IAW) the published SLAs.

g. Verify that the service is available to the system, capability, application, or user attempting to access it (within policy, regulation, or security guidelines).

Services are Accessible - Provide an active link to the service in the NCES Service Registry
--

h. Verify that the WSDL (or WADL) is well-formed and accurately describes the service. Use an automated tool to assess the "well-formedness" of each WSDL or WADL.

i. Verify that WSDL operations execute as required. This should be confirmed in operational tests, interoperability tests, and standards conformance testing. The data schema and WSDL files are not required to contain valid web address information.

j. Verify that the service provides operational states, performance, availability, and security data/information to Network Operations (NetOps) management services. Examples include Enterprise Management, Content Management, and Network Defense services. If NetOps management services do not exist, this requirement is not applicable.

Services are Trusted - Provide NetOps Data (NetOps Agility) - Enable continuity of operations and disaster recovery for services

k. Verify that the service has a defined and functional Continuity of Operations Plan.

l. Verify Core Enterprise Services (CES), are being used IAW DoD Chief Information Officer (CIO) mandates. The goal is to use mandated CES or existing services to ensure system does not duplicate existing services to satisfy mission needs. The CES are enterprise assets that provide a commonly used service to multiple consumers.

Services use CES - CES are used IAW DoD CIO mandates
--

8. Examine the enterprise catalog. Data asset/service discovery occurs when a user performs a search using an enterprise search capability and discovers a data asset or service that suits a mission need.

Data and services must be advertised by virtue of having been registered in the NCES Enterprise Catalog or other compatible/federated enterprise catalog. The tester must have access to the catalog. Testers should obtain the location and login requirements of the enterprise or community catalog.

a. Login to the NCES Enterprise Catalog or other compatible/federated enterprise catalog. Locate the service to be assessed.

- Access the GIG Gateway (also known as "Enterprise Search webpage").
- Enter keywords into search text box.
- Specify the COI/sponsor for the data by clicking on the appropriate check boxes.
- Click on the search button.

b. Verify the entry includes a link (e.g., URI) to the service.

Service is Accessible

- Provide an active link to the service in the enterprise catalog

c. Verify the link is active and resolves to the service.

(This page intentionally left blank.)

APPENDIX E– REFERENCES

DEPARTMENT OF DEFENSE DOCUMENTS

JCIDS Document Review Checklist - for those with access to Groups on 'Cdxphu1' (T), this document is at: T:\PLANS & POLICIES TRAINING\JCPAT-E document review\nr-kpp document review checklist (E) version1.0, 12 May 2009.doc

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 15 December 2008 http://jitic.fhu.disa.mil/jitic_dri/pdfs/6212_01.pdf

Department of Defense (DoD) 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," 12 April 2006 <http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf>

DoD Architecture Framework (DoDAF) Version 1.5, 23 April 2007

http://cio-nii.defense.gov/docs/DoDAF_volume_I.pdf

http://cio-nii.defense.gov/docs/DoDAF_Volume_II.pdf

http://cio-nii.defense.gov/docs/DoDAF_Volume_III.pdf

DoDAF Version 2.0, Volume 1, "Introduction, Overview, and Concepts - Manager's Guide," 28 May 2009 http://jitic.fhu.disa.mil/jitic_dri/pdfs/dodaf_v2v1.pdf

DoDAF Version 2.0, Volume 2, "Architectural Data and Models - Architect's Guide," 28 May 2009 http://jitic.fhu.disa.mil/jitic_dri/pdfs/dodaf_v2v2.pdf

DoDAF Version 2.0, Volume 3, "DoDAF Meta-model Physical Exchange Specification - Developer's Guide," 28 May 2009 http://jitic.fhu.disa.mil/jitic_dri/pdfs/dodaf_v2v3.pdf

DoD Chief Information Officer (CIO) Memorandum, "DoD Net-Centric Data Strategy," 9 May 2003 <http://cio-nii.defense.gov/docs/Net-Centric-Data-Strategy-2003-05-092.pdf>

DoD CIO, "DoD Net-Centric Services Strategy," 4 May 2007
http://cio-nii.defense.gov/docs/Services_Strategy.pdf

DoD Directive (DoDD) 4630.05, "Interoperability and Supportability of IT and NSS," 5 May 2004 http://jitic.fhu.disa.mil/jitic_dri/pdfs/dd46305p.pdf

DoDD 3222.3, "Electromagnetic Environmental Effects Program", Sep 8, 2004
http://www.fas.org/irp/doddir/dod/d3222_3.pdf

DoDD 8000.01, "Management of the Department of Defense Information Enterprise,"
10 February 2009

DoDD 8320.02, "Data Sharing in a Net-Centric Department of Defense,"
2 December 2004 <http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf>

DoDD 8500.01E, "Information Assurance," 24 October 2002
http://jitic.fhu.disa.mil/jitc_dri/pdfs/850001p.pdf

DoD Discovery Metadata Specification (DDMS) <http://metadata.dod.mil/mdr/irs/DDMS/>

DoD Information Enterprise Architecture (DoD IEA) Version 1.1, 27 May 2009
http://cio-nii.defense.gov/sites/diea/products/DoD_IEA_v1_1_27May09.pdf

DoD Instruction (DoDI) 4630.8, "Procedures for Interoperability and Supportability of
Information Technology (IT) and National Security Systems (NSS)," 30 June 2004
http://jitic.fhu.disa.mil/jitc_dri/pdfs/i46308.pdf

DoDI 5000.61, "DoD M&S VV&A." 13 May 2003
<http://www.dtic.mil/whs/directives/corres/pdf/500061p.pdf>

DoDI 8500.2, "Information Assurance Implementation," 6 February 2003
<http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>

DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process
(DIACAP)," 28 November 2007 http://jitic.fhu.disa.mil/jitc_dri/pdfs/851001p.pdf

DoD Metadata Registry (MDR) <https://metadata.dod.mil/mdr/homepage.htm>

DoD STANDARD PRACTICE MIL-STD-3022, "Documentation of VV&A for Models and
Simulations," 28 January 2008 [http://www.everyspec.com/MIL-STD/MIL-
STD+%283000+-+9999%29/MIL-STD-3022_4197/](http://www.everyspec.com/MIL-STD/MIL-STD+%283000+-+9999%29/MIL-STD-3022_4197/)

DD FORM 1494, APPLICATION FOR EQUIPMENT FREQUENCY ALLOCATION, AUG
96 <http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd1494-1.pdf>

DEFENSE INFORMATION SYSTEMS AGENCY/JOINT INTEROPERABILITY TEST COMMAND DOCUMENTS

DISA INSTRUCTION 610-195-1, "Test and Evaluations" Verification, Validation, and
Accreditation (VV&A) of Modeling and Simulation (M&S) Used in Operational Test and
Evaluation (OT&E), 14 May 2007

JITC Guide to Test Documentation, June 2008 - for those with access to Groups on
'Cdxhfu1' (T), this document is at: T:\PLANS & POLICIES TRAINING\JITC Guide to
Test Documentation, JUN08 Final.doc

JITC Document #08-001, JCPAT-E Search for J-6 Certified Requirements Documents
<https://jiticnet.fhu.disa.mil/cert/updates/jcpat/08001.pdf>

JITC Instruction 380-50-02, "JITC Interoperability and Standards Conformance Test and Evaluation (T&E) and Certification Instruction," 28 September 2004

JOINT REQUIREMENTS OVERSIGHT COUNCIL DOCUMENTS

Joint Requirements Oversight Council (JROC), "Capabilities Production Document (CPD) for Net-Centric Enterprise System (NCES), Increment: One," 27 March 2008

JROC Memorandum (JROCM) 010-08, "Approval to Incorporate Data and Service Exposure Criteria into the Interoperability and Supportability Certification Process," 14 January 2008 http://jitic.fhu.disa.mil/jitc_dri/pdfs/seciscp.pdf

PROGRAM AND SERVICES DOCUMENTS

"Test and Evaluation Master Plan (TEMP) for NCES Increment One," 28 March 2008

United States Strategic Command (USSTRATCOM) Exposure Verification Tracking Sheet (EVTS) Guide, Version 1.5, 27 December 2007
http://jitic.fhu.disa.mil/jitc_dri/pdfs/evtsg.pdf

USSTRATCOM Data EVTS
http://jitic.fhu.disa.mil/jitc_dri/pdfs/data_evts.pdf

USSTRATCOM Service EVTS
http://jitic.fhu.disa.mil/jitc_dri/pdfs/sevts.pdf

LINKS

Defense Knowledge Online (DKO)
<https://www.us.army.mil/>

GTG Online
<https://216.181.4.90/gtg>

Net-Centric Enterprise Services (NCES) Service Registry
<http://uddi.xml.org/>

Net-Centric Enterprise Services (NCES) Enterprise Catalog
http://www.disa.mil/nces/product_lines/enterprise_catalog.html

SOAPUI
<http://www.soapui.org/>

(This page intentionally left blank.)