Joint Interoperability Certification

What the Program Manager Should Know

Chris Watson

(Note: This article is an updated version of "Joint Interoperability Certification: What the Program Manager Should Know," by Phuong Tran, Gordon Douglas, and Chris Watson, Defense AT&L, *March-April 2006. This article reflects new policy passed since 2006.)*

Making sure systems can work together during joint operations has been a key problem for the Department of Defense. Interoperability testing and certification of systems are important because they help program managers consider such things as whether a system can work with systems belonging to other military services without unacceptable workarounds, and whether the systems conform to broader architectures designed to facilitate interoperability across DoD.

Watson *serves as outreach director for the Joint Interoperability Test Command. His experience encompasses over 20 years in the operation, training, and testing of military IT systems.*

DoD's process for certifying interoperability of information technology and national security systems (NSS) has evolved over the past few years. In order for this process to be effective, stakeholders must examine whether certification has been planned appropriately and whether a true understanding of the process exists. Program managers who have integrated this process into their overall development and testing schedule have normally transitioned into the field smoothly and provided the best support to their users. Program managers lacking a good understanding of the process have encountered interoperability problems too late in the acquisition cycle, causing delays and cost overruns, and worst of all, contributing to deadly mistakes at critical times. Program managers must understand the process and use it to their advantage. To accomplish this, a few basic questions need to be answered.

What is Interoperability?

As defined by DoD policy, interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces; and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end 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 life cycle and must be balanced with information assurance.

What is Interoperability Certification?

Interoperability certification is the process of ensuring that a system meets the joint interoperability requirements of its users. It includes the collection of the data (test) necessary to determine (evaluation) whether or not the system conforms to applicable interoperability standards and can effectively exchange all required information with all pertinent systems.

Why is Interoperability Certification Necessary?

Interoperability certification assures the warfighter that the combatant commander, Services, and agency systems can interoperate in a joint, combined, and coalition environment.

Who Certifies That a System is Interoperable in a Joint Environment?

The Joint Interoperability Test Command, an organizational element of the Defense Information Systems Agency, has responsibility for certifying joint and combined interoperability of all DoD IT and NSS. JITC facilities are strategically located at Fort Huachuca, Ariz.; Indian Head, Md.; and Falls Church, Va. The diverse capabilities and resources associated with each respective location allow the armed services to have access to a dynamic environment for laboratory tests and onsite field evaluations.

Interoperability certification assures the warfighter that the combatant commander, Services, and agency systems can interoperate in a joint, combined, and coalition environment.

What Systems Need to be Certified?

All IT and NSS that exchange and use information to enable units or forces to operate effectively in joint, combined, coalition, and interagency operations and simulations must be certified.

When Should Systems be Certified?

All systems must be certified before they are fielded. Fielded systems must be recertified every four years or after any changes that may affect interoperability. The program manager should contact JITC early in the acquisition program to ensure that certification is timely and cost effective.

What Does Certification Involve?

JITC follows the processes outlined in the Chairman, Joint Chiefs of Staff, Instruction 6212.01, "Interoperability and Supportability of Information Technology and National Security Systems," to perform its joint interoperability test and certification mission. The document establishes policies and procedures for developing, coordinating, reviewing, and approving IT and NSS interoperability needs. It also establishes procedures for performing interoperability certification using a new, net-ready approach.

Generally, the interoperability certification process consists of four basic steps. Joint interoperability testing and evaluation can be a repetitive process as conditions change. The steps are:

- Identify (interoperability) requirements
- Develop certification approach (planning)
- Perform interoperability test and evaluation
- Report certifications and statuses.

The Joint Interoperability Test Command has responsibility for certifying joint and combined interoperability of all DoD IT and NSS.

Identification of Interoperability Requirements

Establishing requirements is a critical step, and system sponsors must resolve any requirements/capabilities issues with the Joint Staff, J-6. The Joint Staff, J-6 must certify specific requirements/capabilities if system interoperability certification is required. JITC provides input to the J-6 requirements/capabilities certification process and uses the results as the foundation for the remaining three steps of the interoperability certification process.

The capabilities development process has been strengthened with the publication of CJCSI 3170.01, "Joint Capabilities Integration and Development System (JCIDS)." The JCIDS supports the Joint Staff and the Joint Requirements Oversight Council in identifying, assessing, and prioritizing joint military capability needs. As prescribed by the JCIDS process, JITC will participate in the technical assessment of all IT and NSS capability and requirements documents to ensure interoperability requirements are specified in measurable and testable forms. JITC assists in identifying requirements contained in sources such as the program's capability development document, capability production document, information support plan, tailored information support plan, or information support plan annexes.

Once requirements are identified, JITC develops a joint interoperability requirements matrix and confirms it with the appropriate operational command or agency. This matrix then serves as the basis for development of the certification approach.

Developing the Certification Approach

JITC's evaluation strategy will identify data necessary to support joint interoperability test certification as well as the test events/environments planned to produce that data. The current evaluation strategy is driven by DoD's architectural shift towards a network-centric operational environment.

The foundation of DoD's net-centric environment is the Global Information Grid. The GIG is the globally interconnected, end-to-end set of capabilities, processes, and resources for collecting, processing, storing, managing, and disseminating on-demand information to the warfighter. This environment compels a shift from system-to-system to system-to-service exchange to enable on-demand discovery of and access to all available information resources. As the GIG evolves toward a net-centric architecture, interoperability testing must also evolve. Increasingly, the requirement will be to test a system's ability to successfully discover and employ the appropriate information resources within the context of the GIG.

Net-Ready Key Performance Parameter

The main component of this new approach to interoperability testing is the Net-Ready Key Performance Parameter. The NR-KPP consists of measurable, testable, or calculable characteristics and/or performance metrics required for the timely, accurate, and complete exchange and use of information. It defines the performance attributes and creates the framework for identifying the information structure necessary to enable the functional capabilities identified in the requirements documents. The NR-KPP consists of the following five elements:

- Compliance with solution architectures
- Compliance with net-centric data and services strategies
- Compliance with applicable GIG technical guidance
- Compliance with DoD information assurance requirements
- Compliance with supportability requirements, including spectrum use and information bandwidth requirements.

A compliant solution architecture is being developed in accordance with the current version of the DoD Architecture Framework as guided by the laws, regulations, and policies defined in the rules and constraints of the DoD Information Enterprise reference, DoD Directive 8000.01. Compliant solution architecture descriptions assist DoD in understanding the linkages between capabilities and systems. Architecture products, or models, are grouped into eight viewpoints, or modeling perspectives—all, capability, data and information, operational, project, services, standards, and systems viewpoints—that logically combine to describe a program's architecture. The architecture is integrated when the data elements defined in one model are the same as architecture data elements referenced in another model. Each model within the eight viewpoints depicts certain architecture attributes. Some attributes bridge views together and provide integrity, coherence, and consistency to architecture descriptions.

Net-Centric Data and Services Strategy Compliance

Compliance with the net-centric data and services strategy is an essential prerequisite of net-centric operations.

In order for a capability with net-centric requirements to gain joint interoperability certification, program data and services must be exposed by making those data elements and services visible, accessible, and understandable to potential authorized consumers anywhere on the GIG. JCIDS requirements must document compliance with the DoD net-centric data strategy and DoD net-centric services strategy. Tactical systems, control systems, and weapons systems with time-critical constraints are exempted from the requirement to demonstrate compliance with the data strategy. The ultimate goal is that all elements of DoD are networked and able to share information. The result will be a dramatic improvement in operational effectiveness.

GIG Technical Guidance

GIG technical guidance is an evolving Web-enabled capability providing the technical guidance necessary for an interoperable and supportable GIG built on net-centric principles. GIG technical guidance provides a one-stop, authoritative, configuration-managed source of technical compliance guidance that synchronizes previously separate efforts. The GIG technical guidance aids program managers, portfolio managers, engineers, and others in determining where an IT or NSS fits into the GIG with regards to end-to-end technical performance, access to data and services, and interoperability. GIG technical guidance is also essential for ensuring technical interoperability of IT and NSS on the GIG.

Information Assurance

All IT and NSS must comply with applicable DoD information assurance policies and instructions. Information assurance is an integral part of net-readiness. DoD employs a defense in-depth strategy to establish and maintain an acceptable information assurance posture across the GIG. All GIG information systems shall implement information assurance elements and protection mechanisms that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Program managers must ensure that information assurance is fully integrated into all phases of their acquisition and upgrade, including initial design, development, testing, fielding, and operations.

Electromagnetic Environmental Effects

All IT and NSS systems must comply with electromagnetic environmental effects control and spectrum supportability policy. The spectrum supportability process includes national, international, and DoD policies and procedures for the management and use of the electromagnetic spectrum. All IT and NSS systems must be mutually compatible with other systems in their electromagnetic environment and not be degraded below operational performance requirements due to electromagnetic environmental effects.

All capability development documents, capability production documents, information support plans, and tailored information support plans for systems that exchange information with external systems will be reviewed and certified based on adherence to NR-KPP criteria. In turn, JITC will use the NR-KPP thresholds and objectives to ensure that all system information exchange requirements have been satisfied during all applicable test events. These test events must be conducted in an operationally realistic environment. That includes employing production representative systems, members of the user community as operators, and realistic messages and network loads.

Performing the Interoperability Evaluation

Interoperability evaluation often spans developmental test and operational test and evaluation, and it relies on multiple test events conducted by various organizations. The amount and type of testing will vary based on characteristics of the system being evaluated. A developmental test looks at how the system and its components meet the specifications to which that the contractor/vendor signed up to build. With the new acquisition strategies—such as spiral development—testers are involved earlier. That helps JITC collect information and data to reduce risk and time required for interoperability certification and operational testing or assessments. Verification of conformance to standards is one of the first steps in the interoperability testing process. As IT and NSS systems are designed, the developer is required to implement standards or products contained within the DoD IT Standards Registry. Early on in the development/acquisition cycle the particular IT and NSS (or components of that system) is tested to ensure the chosen standards are properly implemented. Conformance with DoD IT Standards Registry standards does not guarantee interoperability, but it is an important step toward achieving it. Developmental testing performed under government supervision that generates reliable, valid data can be used to determine technical capabilities and standards conformance status, and may supplement operational data for an interoperability evaluation.

Throughout the acquisition cycle, JITC will use any valid data from developmental test, operational test and evaluation, demonstrations, field exercises, or other reliable sources for interoperability evaluations. Complex systems involving

Compliance with the net-centric data and services strategy is an essential prerequisite of net-centric operations.

multiple evaluation events may require JITC to develop an interoperability certification and evaluation plan, which outlines how the system will be tested against approved requirements. Each potential data collection opportunity should be used in the overall certification process to get the best interoperability picture of the system in the most efficient manner possible.

Reporting Interoperability Status

Certification is based on Joint Staff-certified capabilities and requirements, the criticality of the requirements, and the expected operational impact of any deficiencies. Certification is applied to the overall system if all critical interfaces have been properly implemented and tested. Interoperability status represents the extent of which a system is interoperable, with respect to the elements of the NR-KPP, information exchanges, and other defined interoperability requirements.

What will JITC Do to Get Your System Certified?

When contacted by a program manager early in the acquisition process, JITC will:

- Assist in identifying joint interoperability requirements during the concept development/design phase of the program
- Ensure that interoperability is built into the system from the start
- Plan for the most efficient use of resources
- Assist the program manager in identifying solutions to interoperability problems necessary to get the system certified.

Interoperability is a key enabler to combat effectiveness.

JITC also has a range of tools available for system assessments and laboratory resources for testing virtually all types of IT and NSS systems.

What Will Happen if a Program Manager Fails to Participate in the Joint Interoperability Certification Process?

The answer to this question comes straight from CJCSI 6212.01:

4. Failure to meet Certification Requirements

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

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

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

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

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

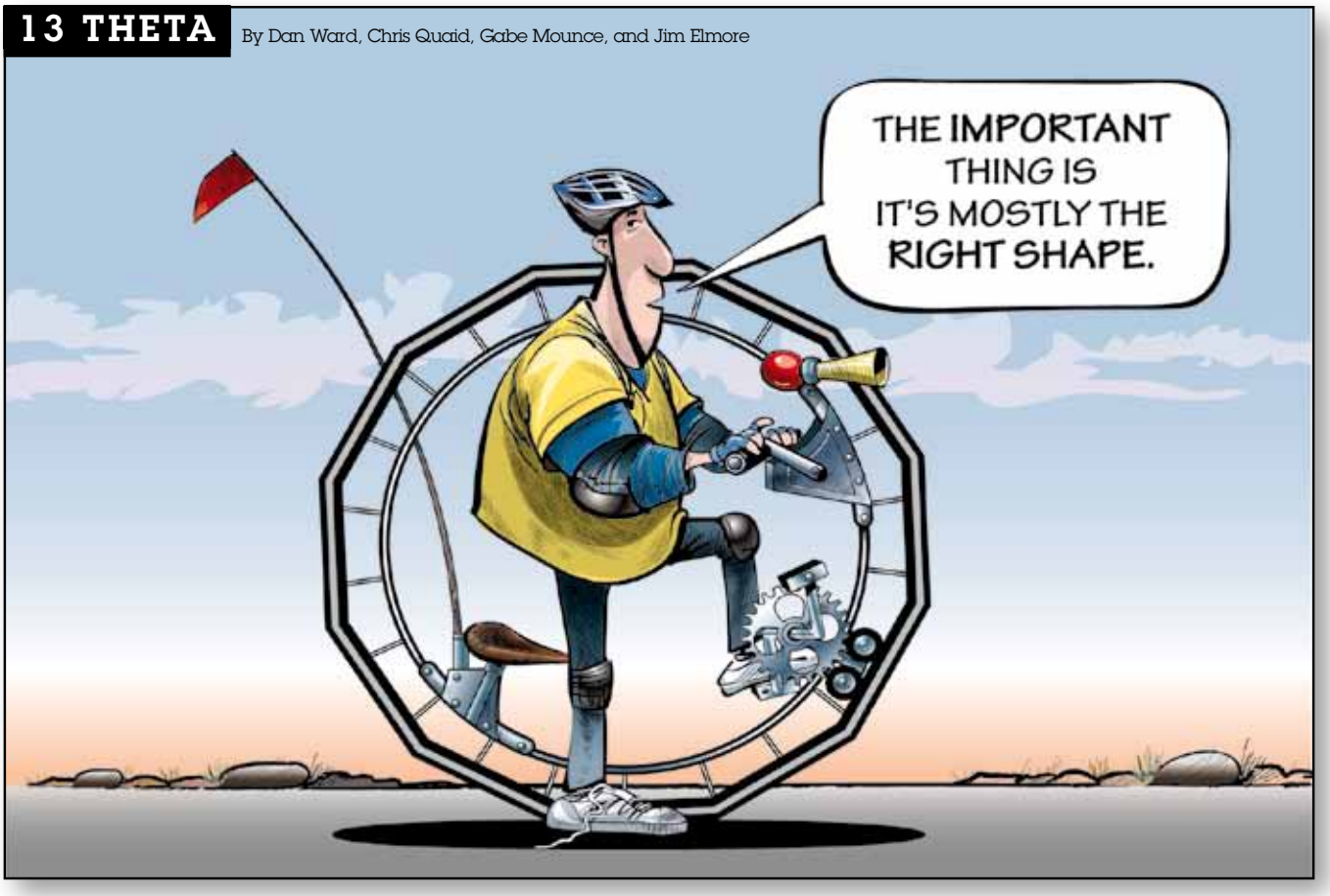
Of course, real-world capability development and testing are rarely simple, and DoD has provided several mechanisms for identifying and seeking solutions to current or foreseen interoperability problems. DoD policy clearly states that all IT and NSS systems, regardless of acquisition category, must be tested and certified for interoperability before fielding. The Military Communications Electronics Board Interoperability Test Panel (ITP) identifies, coordinates, and resolves IT and NSS interoperability policy and testing issues to ensure compliance with DoD policy regarding interoperability of IT and NSS during the requirements validation process and throughout the acquisition life cycle.

To further assist in monitoring compliance with DoD policy regarding interoperability certification, the ITP provides semi-annual interoperability status briefings to the Military Communications Electronics Board. The briefings typically provide the overall interoperability status of a functional area or family or system of systems to the Military Communications Electronics Board, identifying capabilities that may require additional attention or assistance to achieve full interoperability. When necessary, the ITP may nominate programs for inclusion on the interoperability watch list. Criteria for nominating programs to the watch list include, but are not limited to, the following:

- No plans for joint interoperability certification testing
- Failed joint interoperability certification tests and no plans for addressing identified deficiencies
- Lack of JCIDS or test documentation for defense technology projects and pre-acquisition demonstrations
- Known interoperability deficiencies observed during operational exercises or real-world contingencies
- Non-compliance with approved integrated architectures.

Once placed on the interoperability watch list, it is the program manager's responsibility to take corrective action to address interoperability deficiencies and report progress to the principals represented on the Interoperability Senior Review Panel. If interoperability issues are not adequately addressed, or if deficiencies persist, the program or system may be recommended for transfer to the OSD T&E Oversight List.

In certain cases, the ITP may grant an interim certificate to operate that may not exceed one year. The ICTO provides the authority to field new systems or capabilities for a limited



time, with a limited number of platforms, to support development efforts, demonstrations, exercises, or operational events without an interoperability test certification. It is the program manager's responsibility to submit the ICTO request. As the ITP executive agent, JITC provides recommendations to the ITP for or against the ICTO based on available interoperability data and an evaluation of the possible risk to the user and other connected systems. After reviewing the program manager's justification statements and JITC's recommendations, the ITP will then vote to approve or disapprove the request.

JITC issues special interoperability test certifications for systems or system components (e.g., network infrastructure components, voice/video/data components) that require interoperability test certification but are not subject to the JCIDS process. Requirements for these types of system components are derived from the unified capabilities requirements. Products that undergo successful testing and meet specified requirements defined within the unified capabilities requirements are placed on the unified capabilities approved products list.

Many legacy-fielded systems lack both interoperability testing and current requirements documentation. Programs scheduled to terminate may not require interoperability testing and certification and may request a legacy waiver if they meet certain criteria. Waivers under this option may be applied to versions, increments, blocks, etc. Program managers responsible for systems maintaining a continued GIG connection that will not require updated requirements documentation recertification and examination to maintain that connection to the GIG may also request a legacy waiver if specified criteria are met. Waivers under this option cannot be applied to versions, increments, blocks, etc.

Systems that possess no joint interfaces and no information exchanges (whether in development or already fielded) may be candidates for a joint interoperability testing exemption. A request for an exemption must be forwarded to the appropriate Military Communications Electronics Board ITP representative, and the Joint Staff, J-6 will either concur or not concur with the request typically within 30 calendar days of receipt.

Assurance of Interoperability for the Warfighter

Unquestionably, interoperability is a key enabler to combat effectiveness. JITC will continue to play an active role in the joint interoperability test and certification process. This proven process affords higher levels of assurance that warfighting systems will interoperate properly so that the battleground does not become the testing ground.

The author welcomes comments and questions and can be contacted at **chris.watson@disa.mil**.