

**JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA 85613-7051**

JITC Instruction 380-50-02*

28 September 2004

INTEROPERABILITY

**JITC Interoperability and Standards Conformance
Test and Evaluation (T&E) and Certification Instruction**

1. **Purpose.** This instruction replaces Joint Interoperability Test Command Instruction (JITCI) 720-15-8 to update JITC policy and procedures and assign responsibilities for JITC Test and Evaluation (T&E) and for Information Technology (IT) and National Security Systems (NSS) joint interoperability and standards conformance certification. This instruction does not preclude the need to refer to basic guidance and direction in Department of Defense (DOD) interoperability policy documents. See enclosure 1 for a reference listing.
2. **Applicability.** The policy and procedures identified in this instruction apply to all military and civilian personnel assigned to or employed by JITC and contractors engaged in work on behalf of JITC, and to all JITC T&E and certification efforts.
3. **Authority.** This instruction implements the DOD information interoperability policy in the documents referenced in enclosure 1.
4. **References.** See enclosure 1 for references.
5. **Definitions.** Terms used in this instruction are defined in references (a), (f), (g), (l), and enclosure 2.
6. **Policy**
 - 6.1 **Interoperability.** DOD Directive (DODD) [4630.5](#) states that "IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and shall be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS." JITC must certify all IT and NSS for interoperability before fielding and upon changes affecting interoperability. JITC also provides test tools, procedures, and support systems for interoperability and standards conformance testing and validates test tools and procedures (including those developed by other organizations) for interoperability and standards conformance testing.

* This instruction cancels JITCI 720-15-8, dated 17 August 2001.

OPR: JTA

DISTRIBUTION: All JITC Military, Civilian, and Contractor Personnel.

6.2 JITC Interoperability Mission. While JITC provides many types of testing support, our unique DOD interoperability mission is to assess, test, evaluate, and certify systems for interoperability. JITC Action Officers (AOs) will educate themselves and inform the program managers (PMs)/proponents, as required, on DOD interoperability policy, universal reference resources (URRs) (sources for guidelines and attributes for integrated architecture products), and the JITC T&E and certification processes. However, all AOs shall coordinate with the lead AO and other divisions before contacting the PM/proponents for any purpose to ensure they receive one position. All JITC testers should be familiar with the DOD [4630](#) series and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) [3170](#) and [6212](#), especially enclosures A and M of [6212](#). JITC may conduct interoperability and standards conformance certification either in a stand alone environment or in conjunction with other T&E events. JITC's preferred T&E method is to combine the interoperability evaluation with other events, such as the Operational Test and Evaluation (OT&E). Enclosure 4 describes the certification process. Lead AOs and AOs must acquire a working knowledge of DOD and JITC interoperability policy and net-centric architecture material. They must also develop and follow the testing methodologies prescribed in this instruction.

6.2.1 One division will be designated as the lead division for each program/system. This division will be responsible for coordinating the testing/certification effort of a particular system. Typically, this division will be responsible for issuing the appropriate testing and certification products. Lead division procedures are detailed in paragraph 7 of this instruction.

6.2.2 The JITC Certification Panel Chairman or his delegated representative makes the lead division designation when JITC receives the first capability/requirements document or somehow learns of the system's existence. This designation is usually based on the type and amount of testing needed in each functional/mission area. The test divisions may appeal this designation by contacting the chairman and suggesting an alternative.

6.3 Capability/Requirements Document Review. JITC often becomes involved in new system acquisitions at the capability definition/requirements-generation stage. The Joint Capabilities Integration and Development System (JCIDS) has replaced the Requirements Generation System (RGS). CJCSI/[M 3170.01](#) and CJCSI [6212.01](#) describe JCIDS, and CJCSI [6212.01](#) also covers the transition from the RGS to JCIDS. Since JITC will test and certify using both systems, this instruction covers both JCIDS and RGS requirements. 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 form. In addition, JITC will review Test and Evaluation Master Plans (TEMPs) and recommend interoperability T&E criteria to acquisition managers, as requested. See enclosure 9 for the capability/requirements document review process.

6.4 System Certification. Interoperability certification involves determining the extent a system meets interoperability capabilities or requirements. JITC's mission has always been to answer the question:

- Can the system effectively exchange information end-to-end to accomplish its mission?

As the net-centric environment evolves, JITC's mission will also be to answer the question:

- Is the system net ready?

Interoperability is evaluated against Joint Staff (JS) J-6 certified requirements. The system must have a valid and certified Interoperability Key Performance Parameter (I-KPP) or Net Ready-Key Performance Parameter (NR-KPP) or other approved interoperability requirements. As the DOD transitions to the JCIDS, JITC will evaluate and certify to the NR-KPP. JITC uses JS J-6 certified interoperability requirements from an Operational Requirements Document (ORD), Capability Production Document (CPD), or Information Support Plan (ISP) to perform a Joint System Interoperability Test Certification. An ORD must contain an I-KPP, and the CPD/ISP must contain an NR-KPP. If a system does not have JS J-6 certified capability/requirements, JITC can not issue a Joint System Interoperability Test Certification. A system must also meet its I-KPP or NR-KPP in its intended operational environment for JITC to certify it as interoperable. This includes the ability to participate in joint operational networks and architectures.

6.4.1 Standards Conformance Certification. Standards conformance is the first phase of interoperability for many systems. CJCSI [6212.01](#) states: "DISA (JITC) Joint System Interoperability Test Certification evaluation will include standards conformance evaluation and certification, where applicable." The AO should consider several factors when determining if standards conformance certification is required. These factors include: use of military-unique features, standards maturity, and testing resource availability (both internal and external). Support divisions will coordinate any standards conformance testing/certification with the lead AO. Standards conformance is necessary, but not sufficient, to ensure interoperability. A system can not be fielded on the strength of a standards conformance certification. See enclosure 8 for detailed standards conformance policy.

6.4.1.1 JITC can perform standards conformance testing and certification against any standard (including North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs)) that can possibly affect interoperability. DOD IT, including NSS, and other U.S. and non-U.S. systems are eligible for a standards conformance certification. Standards conformance certification should be based on validated standards/standards profiles, but does not require JS J-6 certified requirements.

6.4.1.2 JITC may provide a standards conformance certification based upon an evaluation of data collected by other test agencies. This data must be sufficient to determine conformity to the specified standards/standards profiles.

6.4.1.3 A specific hardware/software configuration is certified as conformant to a specific standard/standards profile. Standards conformance certifications do not expire unless provided for in the Standards Conformance Testing Methodology for the particular standards testing program.

6.4.2 Joint System Interoperability Test Certification. JITC must provide an evaluation and interoperability certification, as appropriate, for all IT and NSS -- Acquisition Category (ACAT), non-ACAT, and fielded. A system must have JS J-6 certified requirements before JITC can issue any interoperability certification. JITC certifies that systems meet their interoperability requirements based on reliable performance data collected in an operationally realistic environment. An interoperable system is able to exchange information with other systems so the users/operators of all involved systems are able to effectively complete all missions dependent upon the exchanged information. The systems involved may be directly connected, members of system-of-systems (SoS) or family-of-systems (FoS), or indirectly connected systems exchanging data. Information transfers may involve automated two-way exchanges, one-way transfers, or processes that are fully or partially manual. Evaluation of information exchange involves both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

6.4.2.1 The amount of testing required to make an interoperability certification decision is based on several factors. These include the number and complexity of the interfaces, the interoperability requirements, the need for an operationally realistic test environment, the criticality of the information exchanged, and the risks involved with the technology being used. In each case, the test team must work out a cost-effective test approach that will lead to a definitive interoperability determination.

6.4.2.2 Joint System Interoperability Test Certifications will be forwarded to the JS J-6 for validation IAW CJCSI [6212](#).

6.4.3 Joint System Interoperability Test Certification – Specified Interfaces. JITC issues this certification when a system meets requirements for a subset of its critical interfaces. Even though this certification requires the system to have JS J-6 certified requirements, it is insufficient for obtaining a JS J-6 System Validation. The specified interfaces certification is an interim waypoint on the path to full system certification; the system is not being certified. One of the primary goals of this type of certification is to clearly identify which critical requirements are not met or have not been evaluated (otherwise, the system would normally meet at least threshold requirements sufficient to receive a full system certification).

6.4.4 Special Interoperability Test Certification. JITC issues this certification for systems or components requiring operational interoperability certification but are not subject to the JCIDS process. The JS J-6 does not need to certify I-KPP/NR-KPP requirements for these systems, nor will they issue a JS J-6 System Validation. JITC will coordinate with the JS J-6 to ensure these systems are not subject to JS J-6 interoperability and supportability certification. A specified interfaces form, similar to that for Joint System Interoperability Test Certification, may also be issued for the general category of Special Interoperability Test Certifications.

6.4.5 Extension of Certification. If a system has been modified, but JITC determines the modifications do not affect interoperability and no interfacing systems have changed significantly, the certification may be extended to cover the modified system version. The previous version of the system must have a current interoperability certification based on JS J-6 certified requirements. The system PM/proponent must provide sufficient information for JITC to independently make a determination of the impact of changes on interoperability. The extended certification will expire 3 years from the original certification date.

6.5 Recertification. Both systems and the interoperability environment in which they operate change over time. To ensure interoperability certifications are of sufficient frequency to be valid, all interoperability test certifications expire. Recertification is required as follows:

- When materiel changes (e.g., hardware, firmware, software modifications) affect interoperability
- Upon revocation of interoperability certifications or JS J-6 System Validation
- Upon automatic expiration 3 years after the date of the certification
- When non-materiel changes (i.e., Doctrine, Organization, Training, Leadership, Personnel, or Facilities) occur that may affect interoperability

The lead AO plays a key role in the recertification process. The JITC System Tracking Program ([STP](#)) provides a report that identifies expired certifications and certifications that will expire within 90 days. When a certification has expired or is about to expire, the lead AO will contact the PM/proponent to inform them of the expired/expiring certification. The lead AO may use the [sample letter](#) and follow-up letter provided for this purpose, or contact the PM/proponent with an e-mail. The lead AO should keep a record of this communication and enter an appropriate note into the system STP entry. The lead AO will coordinate all testing activities, as required. If a review of the circumstances for a particular system indicates no change in interoperability characteristics or requirements since the last certification, JITC may issue a new certification. See enclosure 8 for details on the recertification process.

6.6 Program/System-specific Policy and Generic Test Methodologies Policy. Enclosure 8 highlights current and newly established interoperability-related policies that impact JITC certifications.

6.7 Operational Test Readiness Reviews. Interoperability is one aspect considered in the decision to proceed to operational testing. When JITC receives a request to provide input to the Operational Test Readiness Review (OTRR) or Milestone C decision the lead system AO will produce the memorandum, coordinated with other appropriate divisions, to ensure JITC provides a consolidated position. See enclosure 4 for details on the OTRR.

6.8 Military Communications Electronics Board (MCEB) Status Briefing. JITC will provide a semiannual update on the status of JITC interoperability testing to the MCEB. The Chief, Plans, Policies and Warfighter Support Division, in conjunction with the JITC Corporate Board, will select specific functional areas and subjects to brief the MCEB, or the JS J-6 may recommend a topic. See enclosure 14 for the MCEB status of interoperability briefing process.

6.9 MCEB Interoperability Test Panel (ITP) Executive Agent (EA). JITC will assign an individual to serve as the EA for the MCEB ITP. The EA will perform the duties as outlined in the ITP charter and be responsible for providing material for the ITP portion of the JITC website, staffing and tracking of Interim Certificate to Operate (ICTO) requests, coordinating JITC's position on ICTOs, and executing related duties.

6.10 Annual Status Report. JITC will publish an annual report containing a summary of system interoperability test certification status of functional areas. Plans, Policies and Warfighter Support will be the lead division for this effort, with support provided by all other JITC divisions. The report will highlight significant accomplishments in each division and the status of interoperability for each functional area.

6.11 Memorandum of Agreement/Understanding (MOA/MOU). JITC MOAs/MOUs identify organizational responsibilities and procedures that facilitate coordination of joint activities pertaining to interoperability and standards conformance. Instructions and active MOAs/MOUs are located on the T: share under [MOA-MOU](#). JITC personnel shall follow these policies and procedures when it is appropriate to establish an MOA/MOU.

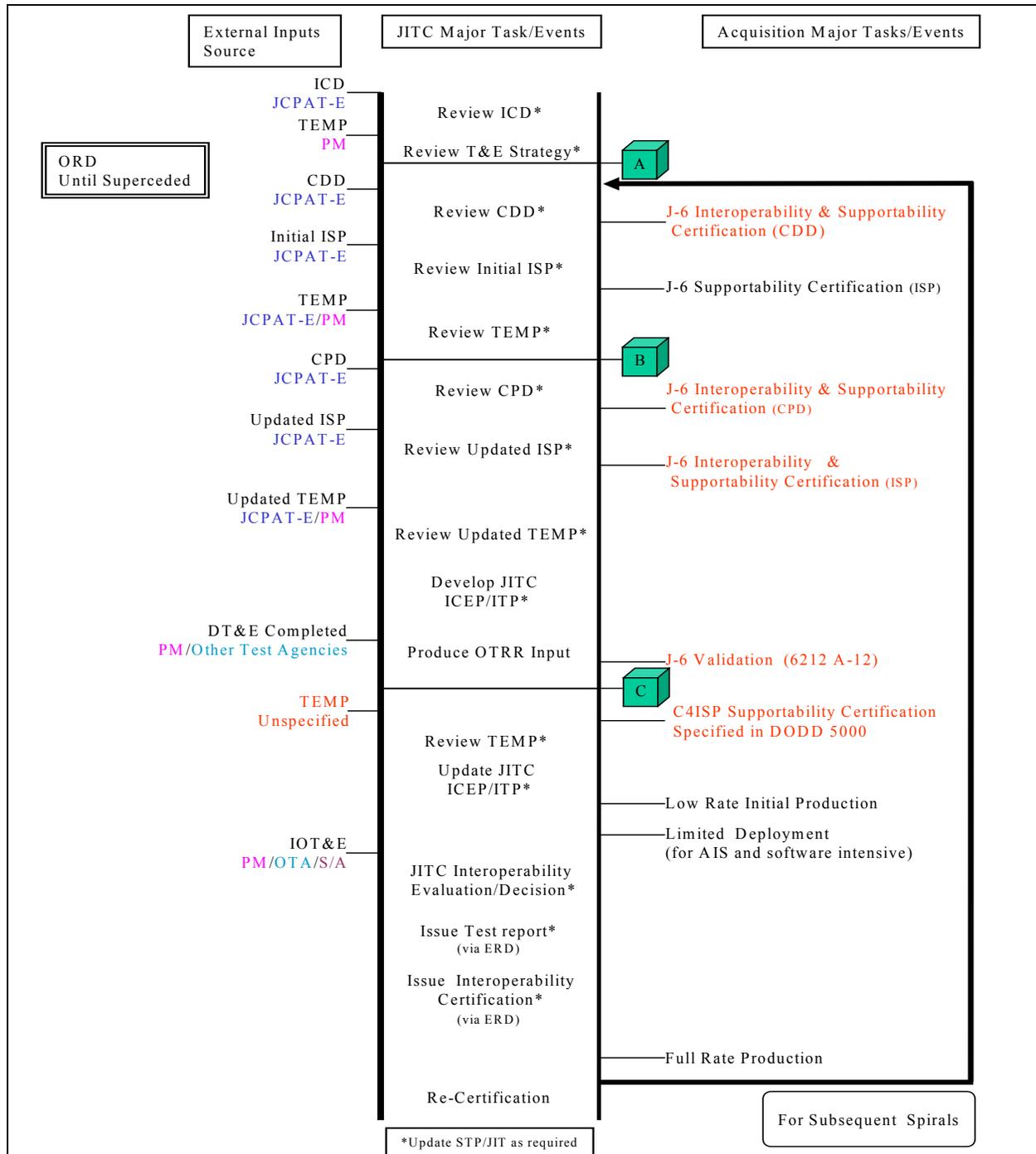
6.12 Overall DOD Interoperability Certification and Validation Processes. The JS J-6 Certification and Validation Process is composed of several sub-processes described in CJCSI 6212: the Interoperability Capability and Supportability Certification, the JITC Joint System Interoperability Test Certification, and NR-KPP compliance. Portions of each sub-process most relevant to JITC processes are described briefly in the following paragraphs. Figure 1 summarizes the overall DOD interoperability [certification and validation processes](#).

6.12.1 Interoperability Capabilities Certification. The JS J-6 will provide an Interoperability Capabilities Certification for CPDs before milestone C. The PM/proponents may use an ORD Interoperability Requirements Certification to support a milestone B or C decision until June 2005. ORDs developed in compliance with previous versions of CJCSI 6212 need to have the requirements verified by JS J-6. When interoperability requirements are waived by JS J-6, the J-6 will specify the source of requirements to use for an interoperability evaluation. JITC must base interoperability evaluations on JS J-6 certified interoperability requirements.

6.12.2 Joint Staff J-6 System Validation. The JS J-6 will validate the following have been accomplished:

- Capabilities interoperability and supportability certification
- JITC Joint System Interoperability Test Certification
- NR-KPP compliance

The JS J-6 system validation should occur before a full-rate production/fielding decision and is intended to provide life cycle oversight of interoperability requirements for IT and NSS. The JITC Joint System Interoperability Test Certification is a key component of this validation.



Legend			
CDD	Capability Development Document	JCPAT-E	Joint C4I Program Assessment Tool Empowered
CPD	Capability Production Document	JIT	Joint Interoperability Tool
DT&E	Developmental Test and Evaluation	OTA	Operational Test Agency
ERD	Electronic Report Distribution	OTRR	Operational Test Readiness Review
ICD	Initial Capabilities Document	PM	Program Manager
ICEP	Interoperability Certification Evaluation Plan	S/A	Service/Agency
IOT&E	Initial Operational Test and Evaluation	STP	System Tracking Program
ISP	Information Support Plan	TEMP	Test and Evaluation Master Plan
ITP	Interoperability Test Plan		

Figure 1. DOD Interoperability Certification and Validation Processes

6.13 JITC T&E Policy and Procedures. Plans and Policies Branch (P&PB) will develop and maintain JITC policy and procedures, including this instruction, to implement DOD interoperability policy and related T&E and reporting methodologies. A T&E and certification program will be established to:

- Develop and maintain policy and procedures
- Develop and conduct training
- Ensure development and maintenance of necessary test methodologies, tools, databases, web pages, and shared repositories of T&E and certification information
- Manage capability/requirements and related document review processes
- Review, approve, and assist in development of testing products
- Perform related management and administrative functions, including status reporting, coordination with JS, and resolution of T&E and certification issues

T&E and certification information will be made readily and widely available to the workforce in a timely fashion. This information will be distributed electronically and a shared repository shall be developed and maintained on the JITC networks. Policy changes and volatile information (e.g., distribution lists and JS J-6 POC information) shall be distributed by e-mail and a repository maintained in Command Information e-mail folders.

7. Procedures.

7.1 JITC Interoperability Certification Process. JITC uses four major steps to certify a system for joint interoperability. See enclosure 4 for additional details on the JITC certification process.

- Identify and verify interoperability capability/requirements
- Develop certification evaluation approach
- Collect and analyze interoperability data
- Determine interoperability status

7.1.1 Identify and verify interoperability capability/requirements. ORDs, CPDs, and ISPs are the primary source of interoperability requirements. The JS J-6 must certify these documents before they can be used to support a Joint System Interoperability Test Certification. (Capability Development Documents (CDDs) can be used for planning purposes, but cannot be used for the interoperability evaluation and certification.)

7.1.1.1 A lack of JS J-6 certified capabilities documents would normally prevent JITC from issuing an interoperability certification. However, JITC may still perform interoperability testing and publish interoperability test reports and assessments. For assessments, the AO can use available documents to determine preliminary requirements, then work with potential user communities to verify and assess the requirements criticality.

7.1.1.2 Interoperability requirements are derived from different sources depending on the specific situation. For ACAT programs, a current JS J-6 certified ORD or CPD shall be used.

For non-ACAT and fielded systems, an ISP shall be used unless a current, certified ORD or CPD is also available. For some programs/systems, a current JS J-6 certified I-KPP package may be appropriate if it is the only source of certified requirements. In special cases, other JS J-6 approved requirements may be used for Special Interoperability Test Certifications (e.g., Defense Switched Network (DSN) voice switch evaluation), but this situation requires coordination with JS J-6. Finally, if a waiver for the NR-KPP is granted, JS J-6 will specify the source of requirements for JITC interoperability evaluation.

7.1.1.3 The JITC AO should ensure the requirements are well defined, testable, and measurable. Poorly defined capabilities or requirements may require extensive interpretation and must be carefully reviewed with users to ensure a complete and accurate set of requirements has been defined. Architecture and mission-related documents validated by United States (U.S.) Joint Forces Command (USJFCOM) and certified by the JS J-6 should be consulted when available.

7.1.1.4 When the certification status of requirements is in question or certified requirements are found to be unusable (e.g., known to be bad), JS J-6 must be engaged to resolve the issue. Contact with JS J-6 to resolve issues must be coordinated through P&PB (JTAB).

7.1.2 Develop certification evaluation approach. To be cost effective, the evaluation of a system's interoperability must be integrated into the system's overall T&E and development processes. AOs should prepare an interoperability evaluation approach that identifies requirements, performance, testing environments and resources, and data collection opportunities. This plan may be anything from a memorandum indicating all interoperability data will be obtained in a single event, to an Interoperability Certification Evaluation Plan (ICEP). Changes in requirements, architecture, concept of operations, or the developmental/operational testing program may require changes in this overall plan. When a program is being developed in phases, the plans also must specify which requirements the system must meet at each phase. See enclosure 10 for ICEP and test plan guidance; see enclosure 6 for staffing procedures.

7.1.2.1 Separate from any ICEP, Interoperability Test Plans (ITPs) are written for individual test or data collection events. These plans detail the testing and data collection and analysis procedures that apply to that event. Generalized test plans may be applicable to some testing programs where the only variable is the specific system under test (i.e., test configuration, procedures, etc., remain the same).

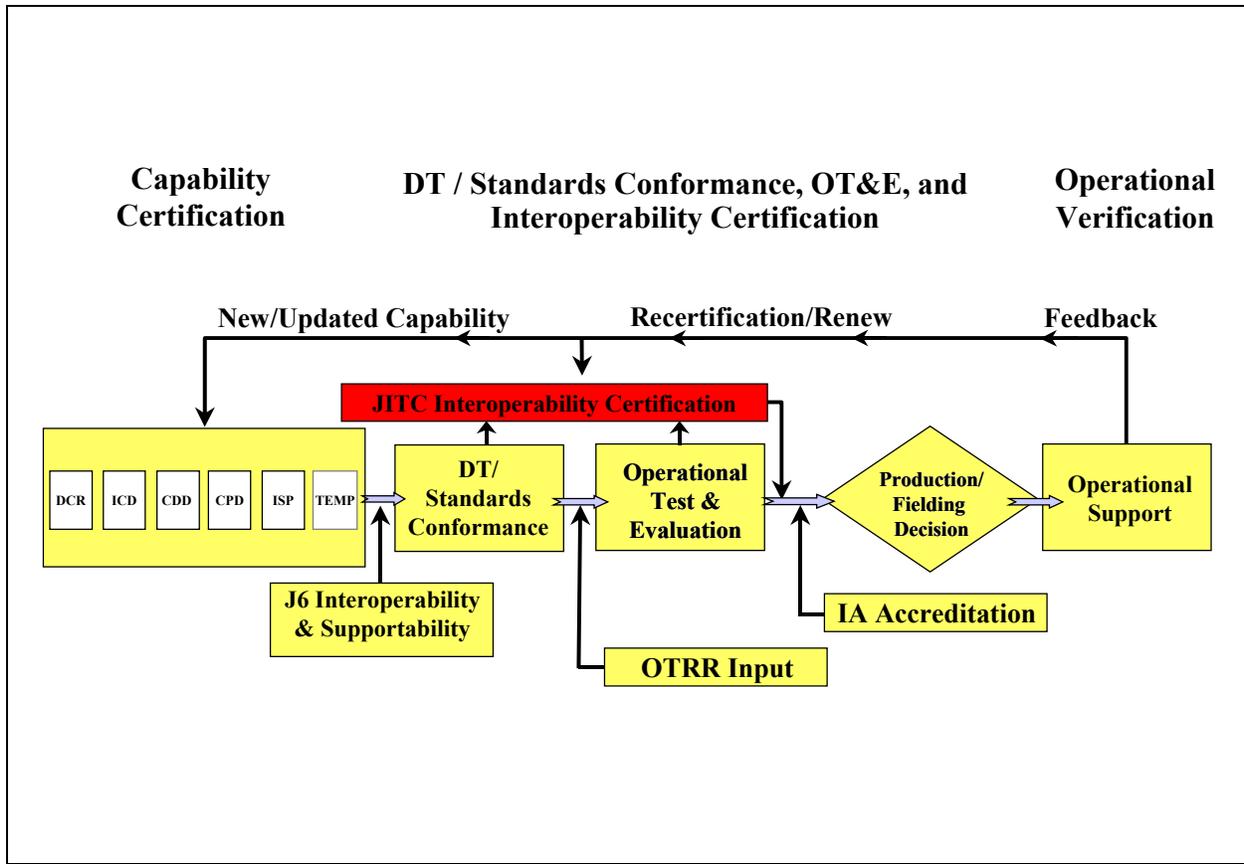
7.1.2.2 JITC-conducted tests will not commence until adequate test plans have been developed and approved by the JITC chain of command. Therefore, testing should be planned as soon as practicable to allow time for an adequate review and update and for coordination with other affected divisions.

7.1.3 Collect and analyze interoperability performance data. A Joint System Interoperability Test Certification must be based on testing or use in an operationally realistic environment. Information exchanged must be accurate, timely, and in a format that meets the users' needs. JITC, even if not conducting the test event, is responsible for ensuring data collection and analysis is properly performed in appropriate environments using operationally

realistic scenarios. Valid data from reliable sources can contribute to the interoperability evaluation. See enclosure 4 for a detailed explanation of the interoperability certification process.

7.1.4 Determine interoperability status. JITC can make a certification determination only after sufficient valid data has been collected to clearly establish the system's ability to meet user requirements. The interoperability evaluation must take into consideration "both the technical exchange of information and the end-to-end operational effectiveness of that exchange," and shall factor in appropriate standards conformance requirements. JITC publishes this determination in a certification memorandum distributed through the Electronic Report Distribution (ERD) tool. Possible certification products include the Joint System Interoperability Test Certification, the Joint System Interoperability Test Certification – Specified Interfaces, a Special Interoperability Test Certification, or a declaration that the system is not interoperable. See enclosures 4-7 for related products and associated processes.

7.2 Life Cycle Certification Processes. Figure 2 outlines the certification process. The process begins with the production and certification of capabilities (requirements) documents. The JS J-6 Interoperability Requirements Certification involves a review and certification of the CDD and CPD. The JS J-6 Supportability Certification involves an ISP review and certification. The JITC can use any valid data from standards conformance testing, Developmental Testing (DT), OT&E, and other reliable sources for interoperability evaluations. The interoperability evaluation and Joint System Interoperability Test Certification must be completed before the product (system/software) is fielded. JITC may also perform some or all of the Information Assurance (IA) portions of the NR-KPP, as coordinated with the system PM/proponent. This should also be completed before fielding. Additionally, JS J-6 system validation should occur before fielding. Once the system is certified and fielded, it moves into operational support where JITC continues to provide support throughout the system life cycle. If changes to the system or environment could affect interoperability, the process starts again at the document production/certification stage. At the end of 3 years, if system/software requirements have not changed, it will reenter the process at the JITC interoperability certification stage.



Legend			
CDD	Capability Development Document	IA	Information Assurance
CPD	Capability Production Document	ICD	Initial Capabilities Document
DCR	DOTMLPF Change Request	ISP	Information Support Plan
DOTMLPF	Doctrine, Organization, Training, Material, Leadership, Personnel and Facility	OT&E	Operational Test and Evaluation
DT	Developmental Test	OTRR	Operational Test Readiness Review
		TEMP	Test and Evaluation Master Plan

Figure 2. Life cycle Certification Processes

7.3 System Acquisition and Procurement Timelines. JITC participates in the capabilities document review process. The assigned JITC AOs should contact the developing systems’ program managers as early as possible to coordinate interoperability testing into the overall development and testing program. Joint System Interoperability Test Certification normally takes place after completion of OT&E to allow the certification decision to be based on the most realistic test data. Testing before OT may be used to assess standards conformance, generate Standards Conformance Certifications, furnish data for OTRR input, and to support a subsequent interoperability evaluation. If OT&E is not scheduled or not available for a system (e.g., status is fielded), then a Joint System Interoperability Test Certification – Specified Interfaces Certification may be possible based on testing interoperability in the available testing environment.

7.4 Lead Division/Lead Action Officer. The lead division will appoint one AO as the lead system point of contact (POC) – the lead AO. The lead AO will manage the system's entire testing and certification effort to include the entire cost estimate, total system requirements

review, and test product review (ensuring all requirements have been evaluated). Other divisions may provide support and test conduct when appropriate, but the lead division and lead AO will ensure the completion of an effective and efficient testing program. Supporting divisions will coordinate their activities with the lead AO. Typically, the lead division is responsible for issuing the appropriate certification product(s). Testing products (certification, assessment, status letters, etc.) will list the lead AO and the support test division POC. If a supporting division issues a certification product, the lead AO will review the product. The lead AO will establish an Integrated Test Team (ITT) consisting of the lead AO and support staff and representatives of all the support test divisions (i.e., support AOs) as soon as the program has been established with JITC. For new types of testing, coordinate with P&PB on developing an adequate test methodology. The lead AO will develop a charter for the ITT that clearly identifies the roles and responsibilities of each party involved in the test and evaluation. The lead AO will coordinate the actions of the ITT and represent JITC to the PM. Figure 3 presents a notional breakdown of a possible AO hierarchy. In the example, JITC is to test and certify a Command and Control (C2) system. The C2 Systems Division has assigned the lead AO from the C2 Systems Branch. The system is complex and requires the support of several other JITC test divisions. While each test division may perform testing and some type of certification (e.g., Standards Conformance, Specified Interface Certification), the lead AO from the C2 branch is responsible for the entire certification effort. See enclosure 3 for lead AO's responsibilities.

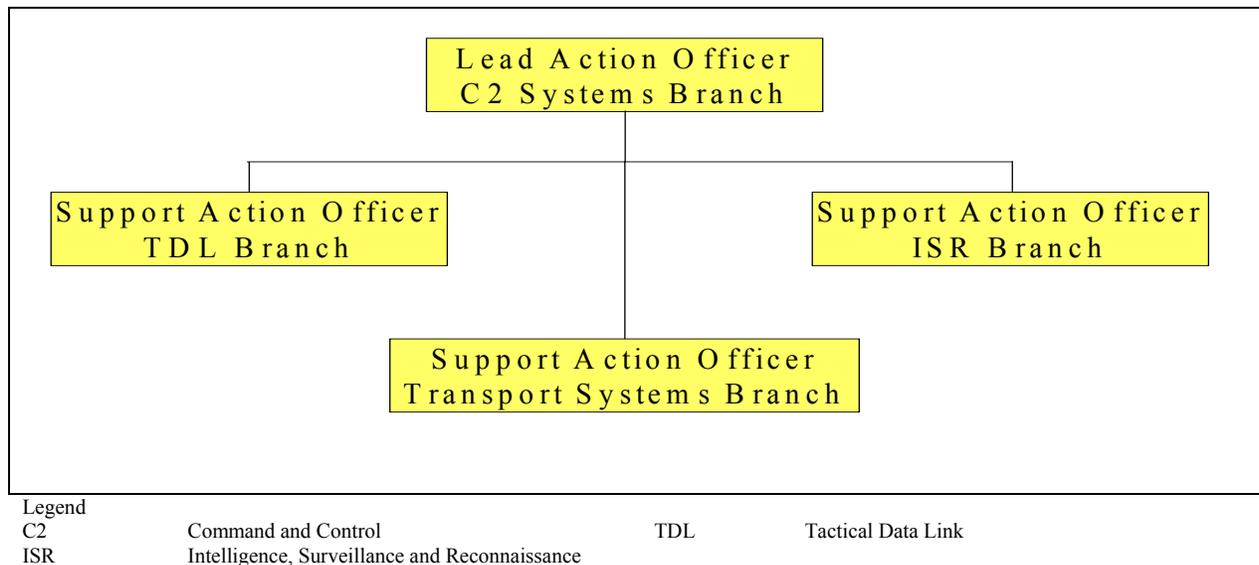


Figure 3. Action Officer Hierarchy Example.

7.5 Interoperability Reporting. The results of interoperability assessments, tests, and evaluations are documented in reports, and assessment and certification letters (DOD memoranda or commercial letters). The AO prepares these documents and submits them for review to the appropriate branch/division chiefs and P&PB. In the case of assessment, certification, status, and similar documents, they are also submitted to the JITC Certification Panel. This panel includes representatives from all JITC divisions, and helps ensure JITC certification practices and products are consistent across all divisions. The chief of the responsible division signs reports and most certification memoranda. In cases of significant

negative findings, non-certifications, or sensitive, controversial findings, the JITC Commander signs the document. See enclosure 6 for a summary of the JITC review process.

7.5.1 The authors of JITC test products and AOs reviewing such material should check the policy information contained in the Command Information directory of the JITC-FHU public Outlook™ folders, the [P&PB t: share](#), and [JITC Intranet](#) information before preparing documents to ensure compliance with the latest guidance and formats. If any special products are deemed necessary, the AO must contact P&PB for approval. This is necessary for consistency within the command, and because a new type of product may require changes in the various tools (e.g., STP and ERD), procedures, training, and even JITC policy.

7.5.2 JITC Presentation Certificates (not to be confused with certification letters) may be issued at the time a certification letter is issued, however, for interoperability certifications they shall only be issued when a system has met threshold or objective requirements. Presentation Certificates shall not be issued for assessments or "specified interfaces" interoperability certifications. Presentation Certificates are issued merely in recognition of achieving conformance or interoperability goals, and are not themselves certification documents.

7.6 Interim Certificate To Operate (ICTO). In certain cases, the ITP of the MCEB may grant a temporary waiver (not to exceed 1 year) from JITC joint interoperability certification requirements. The ICTO gives authority to field new systems or capabilities for a limited time, with a limited number of platforms, to support developmental efforts, demonstrations, exercises, or operational use. The PM/proponent submits an ICTO request. JITC's role is to provide a recommendation to the panel for or against the waiver based on available interoperability data and the risks involved in the proposed use for both system users and users of connected systems. See enclosure 13 for ICTO procedures.

7.7 System Tracking Program (STP), Electronic Report Distribution (ERD) Tool, and Joint Interoperability Tool (JIT). JITC maintains STP information on all systems involved in JITC T&E and certification processes. This database includes information on requirements document reviews, certification testing, certification letters, test plans, test reports, assessment letters, ICTOs, etc. JITC AOs shall keep this information current for their systems. STP information must be current before a letter or report is released for distribution. JITC products must be distributed electronically through the ERD tool. The ERD softcopy is the record copy that is entered into the JIT and STP, and is used to enter certification status and date into the STP. It is very important for all JITC personnel to ensure that the review processes, and STP and ERD procedures, are properly followed so that JITC interoperability databases are complete and accurate. P&PB will make a final review of documents submitted to the ERD, verify that there is an appropriate STP entry, and provide final administrative release authority. JITC test information will also be made available on the JIT, as will other items not stored in the STP, such as the quarterly Warfighter Lessons Learned Report. See enclosures 11 and 12 for STP and ERD policies, procedures, and responsibilities.

7.8 Configuration Management (CM). [JITCI 280-50-01](#), *Configuration Management*, will be followed when other formal CM processes have not been established for a test program. For T&E and interoperability purposes, CM processes will be used at a minimum to verify the

configuration of the testing environment, to include the system under test and interfacing system version identification. Configuration information, to include hardware and software (including firmware) version identification information, shall be documented in JITC test plans, reports, analysis (e.g., assessments), and certification and other appropriate documents (e.g., status letters).

7.9 JITC Product Format and Style. JITC T&E and certification products will follow JITC style guidance, however, quality, consistency, clarity, and reader comprehension shall take precedence. JITC organizational elements may provide additional technical content guidance, however, they shall not impose additional style constraints contrary to JITC overall guidance. Products should be uniform throughout the Command to better serve our customers, including the JS and Warfighter, and to improve the efficiency of document preparation and timely delivery of final products.

8. Implementation and Supplementation. Upon implementation of this instruction, all JITC T&E and certification efforts will follow the policy, procedures, and processes covered by this instruction. This instruction shall not be supplemented without the prior approval of the JITC Certification Panel Chairman or his delegated representative.

9. Waivers. Submit waivers or requests for exceptions to the provisions of this instruction to the JITC Certification Panel Chairman. Requirements based on DOD interoperability policy shall not be waived, unless the DOD policy specifically provides for doing so. Issues regarding CJCSI 6212.01 policy and procedures will be coordinated with the JS J-6 for resolution, as needed.

10. Responsibility. Responsibilities of JITC organizational elements are detailed in enclosure 3.

11. Effective Date. This instruction is effective immediately and remains in effect until superseded or replaced. All JITC T&E and certification methodologies and products shall comply with the provisions of this instruction no later than 3 months after publication. The instruction shall be reviewed, at a minimum, annually, for reissue, revision, or elimination, and upon any significant changes in DOD interoperability policy.



VICTORIA A. VELEZ
Colonel, USAF
Commander

14 Enclosures:

1. References
2. Glossary
3. Responsibilities
4. Certification Processes
5. Certification Checklist or Status Sheet For Action Officers
6. T&E Products and Certification Memorandum Staffing Process
7. Certification Memorandum Products -- Format and Examples

(Continued on next page)

8. Program/System-specific Policy and Generic Test Methodologies Policy
9. Requirements Documents Review Process
10. Test Plans and Test Reports – Guide to Content and Format
11. System Tracking Program (STP)
12. Electronic Report Distribution (ERD) Tool
13. ICTO Process
14. MCEB Status of Interoperability Briefing

Summary of Significant Changes. The entire previous instruction (JITCI 720-15-8) was rewritten to accommodate extensive changes in DOD policy and numerous changes to JITC policy and procedures, such as use of the ERD for electronic distribution of products.

This Page Intentionally Blank

REFERENCES

- (a) DOD Directive [4630.5](#), "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004.
- (b) DOD Instruction [4630.8](#), "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 30 June 2004.
- (c) DODD [5000.1](#), "The Defense Acquisition System," 12 May 2003.
- (d) DODI [5000.2](#), "Operation of the Defense Acquisition System," 12 May 2003.
- (e) DODI [5200.40](#), "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)," 30 December 1997.
- (f) [Interim Defense Acquisition Guidebook](#), 30 October 2002. (Formerly the DOD 5000.2-R Guide Book, 5 April 2002.)
- (g) CJCS Instruction [6212.01C](#), "Interoperability and Supportability of Information Technology and National Security Systems," 20 November 2003.
- (h) CJCSI [3170.01D](#), "Joint Capabilities Integration and Development System," 12 March 2004.
- (i) CJCSM [3170.01A](#), "Operation of the Joint Capabilities Integration and Development System," 12 March 2004.
- (j) DODD [5100.35](#), "Military Communications-Electronic Board (MCEB)," 10 March 1998
- (k) JITCI [210-85-01](#), "Documentation of Test and Evaluation Activities (Plans and Reports)," 1 October 2000.
- (l) Joint Publication [1-02](#), "Department of Defense Dictionary of Military and Associated Terms," 12 April 2001 (As Amended Through 9 June 2004).
- (m) [MCEB Publication 1](#), "Organization, Mission and Functions Manual," 1 March 2002.
- (n) "DOD Architecture Framework Version 1.0, [Volume I](#): Definitions and Guidelines," 9 February 2004.
- (o) "DOD Architecture Framework Version 1.0, [Volume II](#): Product Descriptions," 9 February 2004.
- (p) "DOD Architecture Framework Version 1.0, [Deskbook](#)," 9 February 2004.

(q) DOD Directive [5101.7](#), "DOD Executive Agent for Information Technology Standards," 21 May 2004

(r) JITC, "[JITC Guide to Plans and Reports](#)," 1 October 2000. (Enclosure to JITCI 210-85-01.)

GLOSSARY

JITC Test and Evaluation (T&E) and certification shall use DOD interoperability policy terms and definitions. The following is a listing from this instruction.

PART 1 – ACRONYMS

A

ACAT	Acquisition Category
AO	Action Officer
APB	Acquisition Program Baseline
ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration

C

C2IP	Combatant Commander Command and Control Initiatives Program
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISP	Command, Control, Communications, Computers, and Intelligence Support Plan
C,PP&WSD	Chief, Plans, Policies and Warfighter Support Division
CADM	Core Architecture Data Model
CC/S/A	Combatant Commands/Services/Agencies
CDD	Capability Development Document
CES	Core Enterprise Services
CIO	Chief Information Officer
CINC	Commander in Chief (used in reference only to the President of the United States of America per Secretary of Defense memorandum, 24 October 2002)
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CM	Configuration Management
COI	Community of Interest
COTS	Commercial-Off-The-Shelf
CPD	Capability Production Document
CRD	Capstone Requirements Document

D

DCF	Discrepancy Change Form
DCF-Win	Discrepancy Change Form – Windows
DCR	DOTMLPF Change Request
DCRA	Derivative Classification Review Agent

DCID	Director Central Intelligence Directive
DIA	Defense Intelligence Agency
DICE	Defense Interoperability Communications Exercise
DISA	Defense Information Systems Agency
DISA (JITC)	Defense Information Systems Agency, Joint Interoperability Test Command
DISN	Defense Information Systems Network
DISR	DOD Information Technology Standards Registry
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DOD CIO	Department of Defense Chief Information Officer
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOT&E	Director of Operational Test and Evaluation
DOTMLPF	Doctrine, Organization, Training, Material, Leadership, Personnel, and Facility
DSN	Defense Switched Network
DT	Developmental Testing
DT&E	Developmental Testing and Evaluation

E

EA	Executive Agent
ERD	Electronic Report Distribution
ETSI	European Telecommunications Standards Institute

F

FCB	Functional Capability Board
FHU	Fort Huachuca
FO	Field Office
FoS	Family of Systems
FOT&E	Follow-On Test and Evaluation

G

GAO	Government Accountability Office
GIG ES	GIG Enterprise Services
GES	GIG Enterprise Services
GIG	Global Information Grid
GSCR	Generic Switching Center Requirements
GSTP	Generic Switch Test Plan

I

I-KPP	Interoperability Key Performance Parameter
IA	Information Assurance
IAW	In Accordance With
ICA	Interface Control Agreement
ICD	Initial Capabilities Document
ICEP	Interoperability Certification Evaluation Plan
ICTO	Interim Certificate to Operate
IEC	International Electrotechnical Commission
IER	Information Exchange Requirement
IG	Inspector General
IH	Indian Head
IIC	Interoperability and Interconnectivity Capability
IOP	Interoperability
IOT&E	Initial Operational Test and Evaluation
IPR	In-Progress Review
ISO	International Organization for Standardization
ISP	Information Support Plan
ISRP	Interoperability Senior Review Panel
IT	Information Technology
ITP	Interoperability Test Plan
ITP	Interoperability Test Panel
ITT	Integrated Test Team
IV&V	Independent Verification and Validation
IWL	Interoperability Watch List

J

JCIDS	Joint Capabilities Integration and Development System
JCPAT	Joint C4I Program Assessment Tool
JCPAT-E	Joint C4I Program Assessment Tool - Empowered
JIT	Joint Interoperability Tool
JITC	Joint Interoperability Test Command
JITCI	Joint Interoperability Test Command Instruction
JMA	Joint Mission Area
JPD	Joint Potential Designator
JROC	Joint Requirements Oversight Council
JS	Joint Staff
JTA	Joint Technical Architecture

K

KIP Key Interface Profile
 KM/DS Knowledge Management/Decision Support
 KPP Key Performance Parameter

L

LISI Levels of Information System Interoperability
 LNO Liaison Officer

M

Max Maximum
 MCEB Military Communications-Electronics Board
 MDA Milestone Decision Authority
 MDAP Major Defense Acquisition Program
 MIL-STD Military Standard
 Min Minimum
 MNS Mission Needs Statement
 MOA/MOU Memorandum of Agreement/Understanding

N

NATO North Atlantic Treaty Organization
 NCES Net-Centric Enterprise Services
 NCOW Net-Centric Operations and Warfare
 NCOW RM Net-Centric Operations and Warfare Reference Model
 NCR National Capitol Region
 NII Networks and Information Integration
 NIPRNet Unclassified but Sensitive Internet Protocol Router Network
 NIST National Institute of Standards and Technology
 NR-KPP Net Ready Key Performance Parameter
 NSS National Security Systems
 NITFS National Imagery Transmission Format Standard

O

OASIS Open Artwork System Interchange Standard
 ORD Operational Requirements Document
 OSD Office of the Secretary of Defense

OT	Operational Testing
OTA	Operational Test Agency
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review
OV	Operational View

P

P&PB	Plans and Policies Branch
PDF	Portable Document Format
PK	Public Key
PKI	Public Key Infrastructure
PM	Program Manager
POC	Point Of Contact
PSTN	Public Switched Telephone Network

R

RGS	Requirements Generation System
-----	--------------------------------

S

S/A	Service/agency
SIPRNet	SECRET Internet Protocol Router Network
SME	Subject Matter Expert
SMTP	Simple Message Transfer Protocol
SoS	System of Systems
STANAG	Standardization Agreement
STP	System Tracking Program
SUT	System Under Test
SV	System View

T

T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TIWG	Test Integration Working Group
TM	Trade Mark
TPED	Task, Process, Exploit, Disseminate
TPPU	Task, Post, Process, Use

TV Technical View

U

UJTL Universal Joint Task List

URL Uniform Resource Locator

URR Universal Reference Resources

U.S. United States

USD (AT&L) Under Secretary of Defense (Acquisition Technology and Logistics)

USecAF Under Secretary of the Air Force

V

V&V Verification and Validation

PART II – DEFINITIONS

A

Accreditation. The process by which an Information Technology (IT) and National Security Systems (NSS) are evaluated for meeting security requirements to maintain the security of both the information and the information systems. A designated accreditation authority (DAA) is named for each system. Co-DAAs will accredit IT and NSS in certain cases involving interoperability or integration of multiple systems.

Acquisition Category (ACAT). Categories established to facilitate decentralized decision-making and execution, and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures.

Architecture. The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

Architecture Products. Architecture products are those graphical, textual and tabular items that are developed in the course of building a given architecture description and that describe characteristics pertinent to the purpose of the architecture. When used as part of an architecture description, all products, even those whose primary presentation is graphical, should contain explanatory text. A description of each product is provided in "DOD Architecture Framework Version 1.0, [Volume II](#) Product Descriptions," 9 February 2004.

Framework Product	Framework Product Name	General Description
AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
AV-2	Integrated Dictionary	Architecture data repository with definition of all terms used in all products
OV-1	High-Level Operational Concept Graphic	High-level graphical/textual description of operational concept
OV-2	Operational Node Connectivity Description	Operational nodes, connectivity, and information exchange needlines between nodes
OV-3	Operational Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships amongst organization
OV-5	Operational Activity Model	Capabilities, operational activities, relationships amongst activities, inputs, and outputs; overlays can show cost, performing nodes, or other pertinent information
OV-6a	Operational Rules Model	One of three products used to describe operational activity – identifies business rules that constrain operation
OV-6b	Operational State Transition Description	One of three products used to describe operational activity – identifies business process responses to events
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity – traces actions in a scenario or sequence of events

Framework Product	Framework Product Name	General Description
OV-7	Logical Data Model	Documentation of the system data requirements and structural business process rules of the Operational View.
SV-1	Systems Interface Description	Identification of systems nodes, systems, and system items and their interconnections, within and between nodes.
SV-2	Systems Communications Description	Systems nodes, systems, and system item and their related communications lay-downs
SV-3	Systems-Systems Matrix	Relationships amongst systems in a given architecture; can be designed to show relationships of interest, e.g., system-type interfaces, planned vs. existing interfaces, etc.
SV-4	Systems Functionality Description	Functions performed by systems and the system data flows amongst system functions
SV-5	Operational activity to Systems Function Traceability Matrix	Mapping of systems back to capabilities or of system functions back to operational functions
SV-6	Systems Data Exchange Matrix	Provides details of system data elements being exchanged between systems and the attributes of that exchange
SV-7	Systems Performance Matrix	Performance characteristics of Systems View elements for the appropriate time frame(s)
SV-8	Systems Evolution Description	Planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation
SV-9	Systems Technology Forecast	Emerging technologies and software/hardware products that are expected to be available in a given set of time frames and that will affect future development of the architecture
SV-10a	Systems Rules Model	One of three products used to describe system functionality – identifies constraints that are imposed on systems functionality due to some aspect of systems design or implementation
SV-10b	Systems State Transition Description	One of three products used to describe system functionality – identifies responses of a system to events
SV-10c	Systems Event-Trace Description	One of three products used to describe system functionality – identifies system-specific refinements of critical sequences of events described in the Operational View
SV-11	Physical Schema	Physical implementation of the logical data model entities, e.g., message formats, file structures, physical schema
TV-1	Technical Standards Profile	Listing of standards that apply to Systems View elements in a given architecture
TV-2	Technical Standards Forecast	Description of emerging standards and potential impact on current Systems View elements, within a set of time frames

Assessments. Assessments are data collection opportunities, such as demonstrations and exercises, lacking some aspect necessary for a complete interoperability evaluation. However,

assessments contribute valuable pieces of data reducing and simplifying the requirements for later testing. Other reasons for conducting assessments include program office requests, system functional validation, or opportunities for cost effective data collection before known system problems have been eliminated.

B

Certification. A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process. Certification consists of three forms of capability confirmation -- first, one that addresses system interoperability requirements; second, one that addresses supportability; and third, one that addresses total life cycle oversight of warfighter interoperability requirements. The two Joint Staff (JS) J-6 certifications and validation are discussed below.

Developmental and Production Capabilities Interoperability Certification. This certification occurs before each acquisition milestone (B, C). The Joint Staff (JS) J-6 certifies Operational Requirements Documents (ORDs), Capability Development Documents (CDDs), Capability Production Documents (CPDs) and Information Support Plans (ISPs) regardless of Acquisition Category (ACAT) level, for conformance with joint Information Technology (IT) and National Security Systems (NSS) policy and doctrine and interoperability standards. As part of the review process, JS J-6 requests assessments from the Services, Office of the Secretary of Defense (OSD), Defense Information Systems Agency (DISA), and Department of Defense (DOD) agencies.

Joint Staff (JS) J-6 Supportability Certification. The J-6 certifies to Office of the Assistant Secretary of Defense (OASD) Networks and Information Integration (NII) that programs, regardless of Acquisition Category (ACAT), adequately address Information Technology (IT) and National Security Systems (NSS) infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems. As part of the review process, JS J-6 requests supportability assessments from Defense Information Systems Agency (DISA) and Department of Defense (DOD) agencies. JS J-6 conducts a supportability certification for Capability Production Documents (CPD), before Milestone C for submission to OASD (NII) as part of the CPD review process.

Joint Staff (JS) J-6 Interoperability System Validation. The J-6 validation is intended to provide total life cycle oversight of warfighter capabilities interoperability. The J-6 validates the Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) interoperability system test certification, which is based upon a joint certified Net Ready Key Performance Parameter (NR-KPP), approved in the Capability Development Document (CDD), Capability Production Document (CPD), and Information Support Plan (ISP). The validation will occur after receipt and analysis of the DISA (JITC) interoperability system test certification. The JS J-6 will issue an interoperability system certification memorandum to the respective Services, agencies, and developmental and operational testing organizations.

C

Coalition. An ad hoc arrangement between two or more nations for common action.

Coalition Interface. Any interface that passes information between one or more U.S. Information Technology (IT) and National Security System (NSS) and one or more coalition partner IT and NSS.

Combined. Between two or more forces or agencies of two or more allies. (When all allies or services are not involved, the participating nations and services shall be identified, e.g., combined navies.)

Combined Interface. Any interface that passes information between one or more U.S. Information Technology (IT) and National Security System (NSS) and one or more allied IT and NSS.

D

Defense Agencies. All agencies and offices of the Department of Defense including the Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency/Central Security Service.

Developmental Testing. Developmental testing performed under government supervision that generates reliable, valid data can be used to determine technical performance capabilities, specification or standards conformance status, and may supplement operational data for an interoperability evaluation.

DOD 5000 Series. Department of Defense (DOD) 5000 series refers collectively to DOD Directive (DODD) 5000.1 and DOD Instruction (DODI) 5000.2.

DOD Component. The Department of Defense (DOD) Components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, DOD Field Activities and all other organizational entities within the Department of Defense.

DOD Information Technology Standards Registry (DISR). The DISR provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of

requirements. It defines the service areas, interfaces, standards (DISR elements), and standards profiles applicable to all Department of Defense (DOD) systems. Use of the DISR is mandated for the development and acquisition of new or modified fielded Information Technology (IT) and National Security System (NSS) throughout the DOD. The DISR replaced the Joint Technical Architecture (JTA).

E

Evolutionary Acquisition. The preferred approach that fields an initial operationally useful and supportable capability in as short a time as possible with the explicit intent of delivering the ultimate capability in the future through one or more increments. There are two approaches to evolutionary acquisition: 1) incremental, and 2) spiral. With the incremental approach, a desired capability and end state requirements are known at program initiation, and these requirements are met over time by the development and fielding of increments as technology maturity permits. With the spiral approach, a desired capability has been identified, but end state requirements are not entirely known at program initiation. Each increment of a spiral program provides the user with the best available capability at that time and then future requirements are developed and refined over time based on demonstration, risk management, and continuous user feedback. Spiral development is the preferred approach to evolutionary acquisition.

F

Family of Systems (FoS). A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capability needs. The mix of systems can be tailored to provide desired capabilities, dependent on the situation. An example of a FoS would be an anti-submarine warfare FoS consisting of submarines, surface ships, aircraft, static/mobile sensor systems, and additional systems. Although these systems can independently provide militarily useful capabilities, in collaboration they can more fully satisfy a more complex and challenging capability: to detect, localize, track, and engage submarines.

Follow-On Operational Test & Evaluation (FOT&E). The test and evaluation (T&E) that may be necessary after the Full Rate Production (FRP) Decision Review to refine the estimates made during operational test and evaluation (OT&E), to evaluate changes, and to reevaluate the system to ensure it continues to meet operational needs and retains its effectiveness in a new environment or against a new threat.

Full-Rate Production (FRP). Contracting for economic production quantities following stabilization of the system design and validation of the production process.

G

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in Subtitle III of Title 40, United States Code, as amended. The GIG supports all Department of Defense (DOD), National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

Includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, or services.

I

Increment. A militarily useful and supportable operational capability that can be effectively developed, produced or acquired, deployed and sustained. Each increment of capability will have its own set of threshold and objective values set by the user.

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

Information Exchange Requirements. Information exchange requirements (IERs) characterize the information exchanges to be performed by the proposed system(s). For Capability Development Documents (CDDs), top-level IERs are defined as those information exchanges that are between systems of combatant command/Service/agency, allied, and coalition partners. For Capability Production Documents (CPDs), top-level IERS are defined as those information exchanges that are external to the system (i.e., with other combatant commands/Services/agencies, allied and coalition systems). IERs identify **who** exchanges **what** information with **whom**, **why** the information is necessary, and **how** the information exchange must occur. Top-level IERs identify warfighter information used in support of a particular mission-related task and exchanged between at least two

operational systems supporting a joint or combined mission. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement.

Information Support Plan (ISP). Used by program authorities to document the Information Technology (IT) and National Security Systems (NSS) needs, objectives, interface requirements for all non-Acquisition Category (ACAT) and fielded programs. Information Support Plans (ISPs) should be kept current throughout the acquisition process and formally reviewed at each milestone, decision reviews and whenever the operational concepts, and IT and NSS support requirements change.

Information Technology (IT). Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. This includes equipment used by a Department of Defense (DOD) Component directly, or used by a contractor under a contract with the DOD Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS).

Initial Capabilities Document (ICD). Documents the need for a material approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects, and time. The ICD summarizes the results of the Doctrine, Organization, Training, Material, Leadership, Personal, and Facilities (DOTMLPF) analysis and describes why nonmaterial changes alone have been judged inadequate in fully providing the capability.

Initial Operational Test & Evaluation (IOT&E). Operational test and evaluation conducted on production, or production representative articles, to determine whether systems are operationally effective and suitable, and which supports the decision to proceed beyond Low-Rate Initial Production (LRIP).

Interim Certificate to Operate (ICTO). Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.

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.

Information Technology (IT) and National Security Systems (NSS) interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of 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.

Interoperability Test Certification. Interoperability Test Certification involves an evaluation of information interoperability with respect to interoperability requirements and capabilities. The Joint Interoperability Test Command (JITC) issues "full" system certifications when all critical interoperability requirements are met (i.e., all critical interfaces and top-level exchange requirements, or equivalent, are met) and there are no discrepancies with critical operational impact. JITC updates Joint Interoperability Test Certifications throughout a system's life cycle to reflect changes in the system, status, and environment. All JITC interoperability test certifications expire upon changes that may affect interoperability. Additionally, all certifications expire 3 years from date of issue.

Special Interoperability Test Certification. Issued for systems or system components (e.g., network infrastructure components) that require operational interoperability certification but are not subject to the Joint Capabilities Integration and Development System (JCIDS) process and do not need requirements certified by the Joint Staff (JS) J-6 (e.g., commercial switches being procured to operate in the Defense Switched Network (DSN)). JITC must coordinate with the JS J-6 to verify that the item is not subject to JS J-6 requirements certification.

Joint System Interoperability Test Certification -- Specified Interfaces. Issued when a system has adequately demonstrated operational interoperability for a subset of critical interfaces. A specified interfaces certification may not be sufficient to allow fielding. If military necessity warrants fielding of the system for the demonstrated capabilities, the system proponent should contact the Joint Staff (JS) J-6 to request a formal modification of the Net Ready Key Performance Parameter (NR-KPP) or the Military Communications-Electronics Board (MCEB)/Interoperability Test Panel (ITP) for an Interim Certificate to Operate (ICTO). The system must have JS J-6 certified requirements to receive this certification.

Joint System Interoperability Test Certification. Issued when a system has adequately demonstrated operational interoperability for all critical threshold requirements pertaining to a specific release. This full system certification attests that the system's interoperability is sufficient to support a fielding decision. Evaluation should continue until the status of all objective requirements can be determined and reported. The system must have JS J-6 certified requirements to receive this certification.

Interoperability Watch List (IWL). Established by the Under Secretary of Defense (Acquisition Technology and Logistics) (USD (AT&L)), the Assistant Secretary of Defense (Networks and Information Integration) (ASD (NII))/Department of Defense (DOD) Chief Information Officer (CIO), the Chairman of the Joint Chiefs of Staff, and the Commander, U.S. Joint Forces Command (USJFCOM) to provide DOD oversight for those Information Technology (IT) and National Security Systems (NSS) activities for which interoperability is deemed critical to

mission effectiveness, but interoperability issues are not being adequately addressed. IT and NSS considered for the IWL may be pre-acquisition systems, acquisition programs (any Acquisition Category (ACAT)), already fielded systems, or combatant commander-unique procurements.

J

Joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate.

Joint Capabilities Integration and Development System (JCIDS). A Chairman of the Joint Chiefs of Staff process to identify, assess, and prioritize joint military capability needs. The JCIDS process is a collaborative effort that uses joint concepts and integrated architectures to identify prioritized capability gaps and integrated Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities (DOTMLPF) solutions (materiel and non-materiel) to resolve those gaps.

Joint Integrated Architecture. An integrated architecture that defines desired mission area capabilities (e.g., Intelligence, Surveillance, and Reconnaissance) from the perspective of three views: operational, systems, and technical. The operational view describes joint capabilities and how they will be used, the systems view identifies the particular systems and integration necessary to achieve the desired operational capability, and the technical view identifies the standards to define and clarify technical and integration requirements.

Joint Potential Designator (JPD). A designation assigned by the Gatekeeper to specify Joint Capabilities Integration and Development System (JCIDS) validation, approval, and interoperability expectations.

JROC Interest designation will apply to all Acquisition Category (ACAT) I/IA programs and ACAT II and below programs where the capabilities have a significant impact on joint warfighting. This designation may also apply to intelligence capabilities that support Department of Defense (DOD) and national intelligence requirements. These documents will be staffed through the Joint Requirements Oversight Counsel (JROC) for validation and approval. All Capstone Requirements Documents (CRDs) will be designated as JROC Interest. Doctrine, Organization, Training, Material, Leadership, and Facilities (DOTMLPF) change proposals will also be designated as JROC Interest in accordance with Chairman Joint Chief of Staff Manual (CJCSM) 3170.01 Series.

Joint Integration designation will apply to ACAT II and below programs where the concepts and/or systems associated with the document do not significantly affect the joint force and an expanded review is not required, but Information Technology (IT) and National Security Systems (NSS) interoperability, intelligence or munitions certification is required. Once the required certification(s) are completed, the proposal may be reviewed by the Fictional Capability Board (FCB). Joint Integration proposals are validated and approved by the sponsoring Component.

Independent designation will apply to ACAT II and below programs where the concepts and/or systems associated with the document do not significantly affect the joint force, an expanded review is not required, and no certifications are required. Once designated Independent, the FCB may review the proposal. These documents are returned to the sponsoring Component for validation and approval.

K

Key Interface. Interfaces in functional and physical characteristics that exist at a common boundary with co-functioning items, systems, equipment, software, and data. They are designated as a Key Interface when one or more of the following criteria are met:

- The interface spans **organizational boundaries**. Different entities (service, agency, organization) have ownership and authority over the hardware and software capabilities on either side of the boundary.
- The interface is **mission critical**. Data from joint organizations, multiple services, and/or multiple agencies/organizations must move across the interface to satisfy joint information flow requirements. If systems are not interoperable at that interface, the ability to accomplish the mission is endangered.
- The interface is difficult or complex to manage.
- There are **capability, interoperability, or efficiency** issues associated with the interface.
- The interface **impacts multiple acquisition programs**, usually more than two (e.g. network points of presence, many-to-many or one-to-many connections).
- The interface is **vulnerable** or important from a security perspective.

Key Interface Profile (KIP). An operational functionality, systems functionality, and technical specification description of the Key Interface. The profile consists of refined Operational Views (OVs) and Systems Views (SVs), Interface Control Document/Specifications, Engineering Management Plan, Configuration Management Plan, Technical View (TV) with SV-TV Bridge, and Procedures for Standards Conformance and Interoperability Testing.

Key Performance Parameters (KPP). Those minimum attributes or characteristics considered most essential for an effective military capability. KPPs are validated by the Joint Requirements Oversight Counsel (JROC), for JROC Interest documents, and by the Department of Defense (DOD) Component for Joint Integration or Independent documents. Capability Development Document (CDD) and Capability Production Document (CPD) (KPPs are included verbatim in the Acquisition Program Baseline (APB).

L

Levels of Information System Interoperability (LISI). A model that is applied to information systems to gain a figure of interoperability between systems. Within the LISI model, systems are

evaluated by their use, application, sharing, and/or exchange of common procedures (to include technical standards), software applications, infrastructure, and data. The resultant value, from 0 to 4, indicates the interoperable maturity levels of Isolated (0), Connected (1), Functional (2), Domain (3), and Enterprise (4).

Low-Rate Initial Production (LRIP). The minimum number of systems (other than ships and satellites) to provide production representative articles for Operational Test and Evaluation (OT&E), to establish an initial production base, and to permit an orderly increase in the production rate sufficient to lead to Full-Rate Production (FRP) upon successful completion of operational testing.

M

Materiel. Equipment, apparatus, and supplies used by an organization or institution.

Milestone Decision Authority (MDA). The individual designated, in accordance with criteria established by the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD (AT&L)), by the Assistant Secretary of Defense (Networks and Information Integration) (ASD (NII)) (for Automated Information System acquisition programs), or by the Under Secretary of the Air Force (USecAF) (as the Department of Defense (DOD) Space MDA) to approve entry of an acquisition program into the next phase.

Milestones. Major decision points that separate the phases of an acquisition program.

Military Department. A department headed by a civilian Secretary appointed by the President and includes a Military Service (the Department of the Navy includes two Services).

Mission Needs Statement (MNS). A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept Exploration and Definition Phase of the Requirements Generation Process.

N

National Security System (NSS). Any telecommunications or information system operated by the United States (U.S.) Government, the function, operation, or use of which:

- Involves intelligence activities.
- Involves cryptologic activities related to national security.
- Involves command and control of military forces.
- Involves equipment that is an integral part of a weapon or weapons system.
- Is critical to the direct fulfillment of military or intelligence missions. This does not include automatic data processing equipment or services to be used for routine

administrative and business applications (including payroll, finance logistics, and personnel management applications).

Net-Centric. Exploitation of advancing technology that moves from an applications-centric to a data-centric paradigm - that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components.

Net-Centricity. Net-centricity enables user access and use of resources both collaboratively and asynchronously, regardless of time and place. It is the ability of a program or system to integrate with, offer services to, and exploit the services of a net-centric environment.

Net-Centric Operations and Warfare (NCOW). Describes how the Department of Defense (DOD) will conduct business operations, warfare, and enterprise management. It is based on the concept of an assured, dynamic, and shared information environment that provides access to trusted information for all users, based on need, independent of time and place. It is characterized by assured services, infrastructure transparency (to the user), independence of data consumers and producers, and metadata supported by information discovery, protection, and mediation. This fundamental shift from platform-centric warfare to net-centric warfare provides for an Information Superiority-enabled concept of operations. The NCOW Reference Model (RM) provides a common taxonomy and lexicon of NCOW concepts and terms, and architectural descriptions of NCOW concepts. It represents an important mechanism in DOD transformation efforts, establishing a common framework for net-centricity. It will enable capability developers, program managers, and program oversight groups to move forward on a path toward a transformed, net-centric enterprise. Parameter.

Net-Centric Operations and Warfare Reference Model (NCOW RM). The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest (CoI) services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized. The NCOW RM represents the objective end-state for the GIG. This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of military operations; Department of Defense (DOD) business operations; and Department-wide enterprise management operations. The NCOW RM is a key compliance mechanism for evaluating DOD information technology capabilities and the Net Ready Key Performance.

Net Ready. Department of Defense (DOD) Information Technology (IT)/National Security Systems (NSS) that meets required information needs, information timeliness requirements, has information assurance accreditation, and meets the attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. DOD IT/NSS that is Net Ready enables warfighters and DOD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that

leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all participants. Net-readiness requires that IT/NSS operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure seamless communications within and across diverse Media; information is in a common format with a common meaning; there exist common human-computer interfaces for users; and there exists effective means to protect the information. Net-Readiness is critical to achieving the envisioned objective of a cost-effective, seamlessly integrated environment. Achieving and maintaining this vision requires interoperability:

- Within a Joint Task Force/combatant command area of responsibility (AOR)
- Across combatant command AOR boundaries
- Between strategic and tactical systems
- Within and across Services and agencies
- From the battlefield to the sustaining base
- Amongst United States (U.S.), Allied, and Coalition forces
- Across current and future systems

Net Ready Key Performance Parameter (NR-KPP). The NR-KPP assesses information needs, information timeliness, information assurance, and net ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements:

- Compliance with the Net-Centric Operations and Warfare reference Model (NCOW RM)
- Compliance with applicable Global Information Grid (GIG) Key Interface Profiles
- Verification of compliance with Department of Defense (DOD) information assurance requirements
- Supporting integrated architecture products required to assess information exchange and use for a given capability

Non-Acquisition (Non-ACAT) Program. An effort that does not directly result in the purchase of a system or equipment for operational employment (e.g., science and technology programs, concept exploration or advanced development of potential acquisition programs).

O

Objective. The performance value that is desired by the user and which the Program Manager (PM) is attempting to obtain. The objective value represents an operationally meaningful, time critical, and cost effective increment above the performance threshold for each program parameter.

Operational Requirements Document (ORD). A formatted statement-containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each milestone beginning with milestone A.

Operational Test and Evaluation (OT&E). The field test, under realistic conditions, of any item (or key component) of weapons, equipment, or munitions for the purpose of determining the effectiveness and suitability of the weapons, equipment, or munitions for use in combat by typical military users; and the evaluation of the results of such tests.

Operational View (OV). The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish Department of Defense (DOD) missions. DOD missions include both warfighting missions and business processes. The OV contains graphical and textual products that comprise an identification of the operational nodes and elements, assigned tasks and activities, and information flows required between nodes. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges.

S

Sponsor. The Department of Defense (DOD) component responsible for all common documentation, periodic reporting and funding actions required to support the capabilities development and acquisition process for a specific capability proposal.

Standards. Standards as referenced in this instruction are Information Technology (IT) standards and include specifications, profiles, protocols, implementation conventions, Federal Information Processing Standards (FIPs), Military Standards (MIL-STDs), Defense Performance Specifications (MIL-PRFs), North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs), Allied Communications Publications (ACPs), Allied Data Publications (ADatP), guidelines, commercial item descriptions, standardized drawings, handbooks, manuals, tools, and other related documents relevant to the application and use of information and communications technology. They are software and hardware standards that are used for intelligence collection, data and information processing, information transfer, and information presentation/ dissemination. IT standards provide technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats, information content, interchange, and transmission of transfer. IT standards apply during the development, testing, fielding, enhancement, and life cycle maintenance of Department of Defense (DOD) information systems. Recognized standards include those produced as non-governmental national or international standards (e.g., ANSI and ISO), trade association/professional society standards, federal standards, military standards, and multinational treaty organization standardization agreements.

Standards Conformance Testing. This testing establishes the extent to which a system conforms to the requirements of a standard/standards profile or complies with levels specified in a standard. These standards may include government, commercial, or North Atlantic Treaty

Organization (NATO) standards as long as the requirements specified are measurable and testable. Conformance to applicable standards is necessary, but not sufficient for interoperability. Additional testing is required to ensure that all required information exchanges meet user requirements in the intended operational environment.

Supportability. The level that programs, regardless of Acquisition Category (ACAT), adequately address Information Technology (IT) and National Security Systems (NSS) infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems.

Sustainability. The ability to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materiel and consumables necessary to support military effort.

Sustainment. The provision of personnel, logistic and other support required to maintain and prolong operations or combat until successful accomplishment or revision of the mission or of the national objective.

System. For use in this publication, the term "system" refers to a system or program. A practical definition is that a "system" will follow the complete Joint Capabilities Integration and Development System (JCIDS) (Requirements Generation System (RGS)) process.

System of Systems (SoS). A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. An example of a SoS could be interdependent information systems. While individual systems within the SoS may be developed to satisfy the peculiar needs of a given user group (like a specific Service or agency), the information they share is so important that the loss of a single system may deprive other systems of the data needed to achieve even minimal capabilities.

System View (SV). The SV is a set of graphical and textual products that describes systems and interconnections providing for or supporting, Department of Defense (DOD) functions. DOD functions include both warfighting and business functions. The SV associates systems resources to the Operational View (OV). These system resources support the operational activities and facilitate the exchange of information amongst operational nodes.

T

Technical View (TV). The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The TV includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture.

Threshold. The minimum acceptable value that, in the user's judgment, is necessary to satisfy the need. If threshold values are not achieved, program performance is seriously degraded, the program may be too costly, or the program may no longer be timely. If the threshold values are not otherwise specified, the threshold value for performance is the same as the objective value; the threshold value for schedule is the objective value plus 6 months for Acquisition Category (ACAT) I and three months for ACAT IA programs; and the threshold value for cost is the objective value plus ten percent.

U

Universal Reference Resources (URRs). Reference models and information standards that serve as sources for guidelines and attributes must be consulted in building integrated architecture products. The following are the currently listed URRs: Department of Defense (DOD) Architecture Framework; DOD Core Architecture Data Model; Universal Joint Task List; Technical Reference Model; Global Information Grid (GIG) Architecture; DOD Net-Centric Data Strategy; DOD Metadata Registry; Net-Centric Operations Warfare (NCOW) Reference Model (RM); and the DOD Information Technology Standards Registry (DISR).

RESPONSIBILITIES

1. The Commander, JITC (JT):

1.1 Provides command oversight and direction for all JITC Test and Evaluation (T&E) and certification missions.

1.2 Is the signature authority for JITC Interoperability Test Non-Certifications.

2. The Deputy Commander, JITC (JT):

2.1 Reviews and approves all JITC T&E and certification products routed for DISA Form 9 approval.

2.2 Fulfills all responsibilities of the Commander in his/her absence.

3. The JITC Corporate Board:

3.1 Participates in selecting the subject(s) and issues for all flag-level interoperability venues such as Military Communications-Electronics Board (MCEB) interoperability status briefings and Interoperability Senior Review Panel (ISRP) briefings.

3.2 Reviews and guides JITC T&E and interoperability methodologies and ensures that long range plans adequately address JITC's evolving DOD interoperability mission.

3.3 Designates the lead division for functional/mission area responsibilities and synchronizes overlapping functional/mission areas. [Used as a basis for identifying lead divisions for requirements review and testing activities.]

3.4 Assists in resolving T&E and interoperability issues within JITC.

4. JITC Lead Division/Branch:

4.1 Provides system specific test support in coordination with any support divisions/branches and assumes responsibility for general support of designated functional/mission areas.

4.2 Maintains oversight of all test activities (including requirements review, proponent coordination, planning, budgeting, execution, reporting, certification, training, etc.) for which the division/branch is designated lead.

4.3 Coordinates with other divisions/branches on programs/systems that span functional/mission areas where other divisions/branches may be designated lead for a subordinate function/mission.

4.4 Establishes, in coordination with Plans, Policies, and Warfighter Support Division (JTA), guidelines and/or common practices (e.g., metrics, methods, plans, reports, etc.) specific to functional/mission areas.

4.5 Establishes, in coordination with JT, JTA, and DISA, a working relationship with designated functional/mission area domain leads (e.g., Functional Capability Boards (FCBs), Communities of Interest (COIs)) to address requirements/capabilities, resources, and status reporting.

4.6 Maintains awareness of the status of interoperability of systems and capabilities in their functional/mission areas.

4.7 Develops and retains subject matter expertise on functional and operational concepts, joint integrated architectures, and system-of-system/domain metrics.

4.8 Exercises signature authority on all products related to the designated functional/mission area.

5. JITC Division/Branch Chiefs:

5.1 Ensure that T&E and certification information is technically adequate and accurate, interoperability and conformance status is determined and reported properly, and that the test methodologies and status reporting is in compliance with DOD and JITC interoperability policy and procedures.

5.2 Ensure test plans/reports, certification packages, and related testing products are coordinated with the appropriate personnel/groups for review, approval, and release.

5.3 Ensure that the content and format guidance for documents is followed and that valid comments from the Certification Panel are incorporated into the final documents.

5.4 Ensure JITC's formal products are delivered to the customers in a timely manner, after proper review, approval, and release authorization.

5.5 Ensure Action Officers (AOs) are trained and comply with DOD and JITC interoperability policy and procedures, and consistency of products, entry and maintenance of required System Tracking Program (STP) and Electronic Report Distribution (ERD) information, and receive appropriate training in policy and procedures and acquire necessary technical expertise.

5.6 Plan and budget for testing resources, including tools and techniques and necessary infrastructure.

5.7 Assist in resolving T&E and interoperability issues within JITC.

5.8 Ensure that all personnel are responsive to interoperability status inquiries, requested document reviews, interoperability status reporting requirements, requests to review Interim Certificate to Operate (ICTO) Combatant Commander Command and Control Initiatives Program (C2IP) proposals, and generation of related products. Also, ensure that personnel supporting these various tasks coordinate with other divisions and AOs, as appropriate.

5.9 Ensure that JITC testing activities, and results, are adequately documented and preserved in the STP and other repositories to retain JITC's corporate knowledgebase.

5.10 Provide branch chiefs and subject matter experts (SMEs) as division representatives to the Certification Panel.

5.11 Assume responsibilities of a lead division, as appropriate. As a designated lead division, assigns the lead action officer (STP System Point of Contact) as required.

6. The Chief, Plans, Policies and Warfighter Support Division (PP&WSD) (JTA):

6.1 Chairs the JITC Certification Panel.

6.2 Resolves any T&E and interoperability issues.

6.3 Coordinates with the JITC Corporate Board to establish JITC T&E and certification policy and processes.

6.4 Provides overall direction to Plans and Policies Branch (P&PB) Chief and the MCEB Interoperability Test Panel (ITP) Executive Agent (EA) on T&E and interoperability related matters.

6.5 Designates the MCEB ITP Executive Agent.

6.6 Oversees all JITC T&E and certification policy development, publication, and related training programs, including approval of functional/mission area testing methodologies developed by lead divisions/branches.

7. The Automated Systems and Test Support Division (JTB):

7.1 Develops and manages the System Tracking Program (STP) to include:

7.1.1 Reviewing/approving STP access requests.

7.1.2 Assisting users in the operation of STP.

7.1.3 Approving the combining and deleting of system entries.

7.1.4 Assisting STP Coordinators in answering STP questions from internal and external customers.

7.1.5 Answering STP programmer's questions regarding the implementation of specific requirements.

7.1.6 Responding to internal data calls in support of other JITC Divisions, Commander, Annual Report, Performance Metrics, etc., that require development of special STP reports/queries.

- 7.1.7 Providing STP In-progress review (IPRs) to JITC Management.
- 7.1.8 Ensuring proper STP data storage and back-up procedures.
- 7.1.9 Maintaining STP servers at Fort Huachuca (FHU) and Indian Head (IH).
- 7.1.10 Responding to data calls in support of Government Accountability Office (GAO), Joint Staff (JS), Inspector General (IG), etc. Note: P&PB will be the lead if the task comes directly to the Commander or PP&WSD.
- 7.1.11 Reviewing/approving all completed discrepancy change forms (DCFs) prior to placement on STP production site.
- 7.1.12 Developing STP Training material.
- 7.1.13 Ensuring training material is placed on the Career Development Center (CDC) website.
- 7.1.14 Ensuring STP overview and training slides are up-to-date.
- 7.1.15 Providing ad hoc STP briefings/demonstrations to visitors.
- 7.1.16 Providing STP training to the workforce.
- 7.1.17 Performing requirements analysis.
- 7.1.18 Attending meetings with users to better understand their specific STP requirements.
- 7.1.19 Reviewing/approving STP Users' Manual.
- 7.1.20 Ensuring all STP marketing information is up-to-date: business cards, information card, fact sheet, slides in the command brief, JITC web pages, etc.
- 7.1.21 Contacting AOs that do not respond to STP Coordinators' request for information.
- 7.2 Manages the Electronic Report Distribution (ERD) System
 - 7.2.1 Develops and maintains the ERD.
 - 7.2.2 Assists users in the operation of the ERD.
 - 7.2.3 Provides ERD training to the workforce.
- 7.3 Manages the Joint Interoperability Tool (JIT)
 - 7.3.1 Develops and maintains the JIT.

7.3.2 Assists users in the operation of the JIT.

7.3.3 Provides JIT training to the workforce.

8. All JITC Branch Chiefs:

8.1 Assume the duties of members of the JITC Certification Panel, including participation in the review of products.

8.2 Assist in the development, review, and promulgation of JITC T&E and certification policy and procedures and test methodologies.

9. The Chief, Plans and Policies Branch (P&PB):

9.1 Serves as co-chairperson of the JITC Certification Panel.

9.2 Assumes all T&E and certification responsibilities of Chief, PP&WSD in his/her absence.

9.3 Designates document assessor POCs (primary and alternate) for the J-6 Assessment Tool - (JCPAT-E).

9.4 Resolves any T&E and interoperability issues.

9.5 Ensures that the responsibilities of the P&PB branch for T&E and interoperability are carried out.

10. Plans and Policies Branch (P&PB):

10.1 Develops and maintains the policies and procedures for JITC certification and related processes.

10.2 Provides training and assistance in implementing JITC T&E and certification and related processes, including requirements document review, test plan/report generation, certification processing, and related topics.

10.3 Conducts final review of documents submitted to the ERD, verifies that there is an appropriate STP entry, and provides administrative ERD release authority.

10.4 Ensures all final JITC products (e.g., plans, reports, letters) distributed through the ERD are entered into STP.

10.5 Ensures OSD Test and Evaluation List is entered into the STP.

10.6 Ensures interoperability and conformance status information is entered into the STP.

10.7 Ensures ERD and certification letter core distribution lists are updated.

10.8 Maintains interoperability policy and related T&E information at the following locations:

10.8.1 Outlook™ Certification Policy folders, and related information on the [Plans & Policies Training T: share drive](#). The share drive will contain training briefings, DOD interoperability policy and architecture information, JCPAT-E document review material, STP training slides and users' manual, and example JITC T&E and certification products.

10.8.2 [JITC Public Website](#) (interoperability testing and DOD policy references).

10.8.3 [JITC Intranet Website](#) (document development toolkit, and related material).

10.9 Provides a capability for managing JCPAT-E document reviews, including staffing of documents within JITC, providing documents to the JITC Technical Library and placing available unclassified documents in the "C4ISP" directory of the t: share drive, entering requirements document status and certification information into the STP, and review and posting of JITC comments to the JCPAT-E. The designated or alternate assessor POC is also responsible for the following:

10.9.1 Identifying the individuals within the organization who should review each document being assessed on the tool.

10.9.2 Assisting each document reviewer to obtain a username and password for a read-only account for the J-6 Assessment Tool.

10.9.3 Staffing the document internally to the document reviewers within the organization.

10.9.4 Reviewing the consolidated reviewer comment matrix for content and format, and submit to the J-6 Assessment Tool.

10.10 Provides a capability for the initial draft review through final ERD release approval for plans, reports, certification letters, etc. The review of plans shall verify that the requirements are valid for the proposed use (e.g., interoperability evaluation is based on JS J-6 certified requirements).

10.11 Provides a capability for managing the JITC Certification Panel processes.

10.12 Monitors the T&E and certification processes and assist in problem resolution.

10.13 Participates in the review and comment of DOD interoperability directives, instructions, and policy and procedures.

10.14 Coordinates efforts for reporting interoperability status and answering status inquiries.

10.15 Serves as the central POC between JITC and JS J-6, and other external organizations, on interoperability policy and certification related issues.

11. Warfighter Support Branch (WSB) (JTAA):

11.1 Coordinates with test divisions to ensure exercise support efforts are leveraged to support interoperability test certification mission. For each exercise/operation lead ITT and serve as overall coordinator of command support to that event.

11.2 Manages the review of Combatant Commander Command and Control Initiatives Program (C2IP) proposals, including the development of any tools and procedures specific to C2IPs, staffing of documents within JITC, and consolidation and review of JITC comments.

11.3 Coordinates with P&PB to obtain C2IP documents and for posting comments to the JCPAT-E.

11.4 Coordinates command's Memorandums of Agreement (MOA) and Memorandums of Understanding (MOU) with other commands and agencies.

11.5 Provides liaison officers to combatant commands to focus the Command's efforts on the warfighters' current and projected interoperability issues.

11.6 Increases operational effectiveness of the warfighter through predeployment planning support and on-site resolution of joint and combined C4I interoperability issues.

11.7 Manages contingency support deployment of JITC personnel.

11.8 Leads identification and resolution of joint and combined interoperability issues.

11.9 Coordinates on-site interoperability exercise assistance to the combatant commands consisting of pre-exercise planning and interoperability testing of proposed system configurations, on-site technical assistance, network/architectural analysis, documents network implementations, and operational assessment of combatant commands special interest items.

11.10 Operates a telephonic and electronic mail hotline to leverage JITC C4I test experience and resources to solve real time Joint and Combined interoperability issues.

11.11 Coordinates JITC combatant commands support activities with respective DISA field offices (FOs) and DISA desk officers.

11.12 Develops and maintains joint and combined C4I system exercise planning and reporting instructions with respect to C4I system interoperability.

11.13 Develops and distributes a Quarterly Warfighter C4I Lessons Learned Report technical document for managers, operators, and maintainers that outlines how JITC or other DOD organizations solved C4I joint interoperability issues.

11.14 Formulates, coordinates, and publishes the JITC Annual Report to CJCS on all JITC tests.

11.15 Manages the JITC Combined C4I interoperability test program. Works with on-site liaison officers (LNOs) and JITC divisions to identify yearly C4I interoperability and exercise issues for the combatant commands and develops the "spend plan" to support these issues.

12. Certification Panel Chairperson/Co-Chairperson:

12.1 Leads the development or revision of JITC T&E and certification policy.

12.2 Ensures JITC policy and procedures are in compliance with DOD interoperability policy and procedures and applicable Federal, international, and combined policy and procedures, including standards conformance T&E methodologies.

12.3 Resolves JITC T&E and interoperability and standards conformance certification issues.

12.4 Establishes and chairs the JITC Certification Panel and appoint a Certification Panel Facilitator. The Certification Panel will include Branch Chiefs and/or their representatives, P&PB personnel, as well as other designated JITC employees. An e-mail distribution list of members will be established and maintained, and an e-mail mailbox will be established for Certification Panel processing of products.

12.5 Reviews and approves all JITC T&E and certification products routed for Form 9 approval.

12.6 Convenes Certification Panel meetings or conduct electronic discussion forums, as required.

12.7 Makes a determination as to the appropriate division to be designated lead, based on functional/mission area responsibilities.

13. Certification Panel Members:

13.1 Assist in the development, review, and promulgation of JITC T&E and certification policy and procedures and test methodologies.

13.2 Actively participate in Certification Panel meetings.

13.3 Review documents staffed to the Panel and provide comments to the JITC Certification Working Group and JITC Cert Panel e-mail accounts.

14. Certification Panel Facilitator/Designated Alternate Facilitator:

14.1 Assists AOs with requirements, test planning, T&E, and certification, as required.

14.2 Maintains the JITC Certification Panel membership roster.

14.3 Staffs documents for Certification Panel review and ensure timely processing.

14.4 Assists the Certification Panel in the review of documents for technical content and format, including the review of documents not appropriate for full Certification Panel review.

14.5 Provides consolidated Certification Panel comments to the AO.

14.6 Reviews and approves designated products submitted to the ERD for release. Coordinates any necessary changes with the AOs.

14.7 Provides certification data for certification status reports, as required.

15. The Executive Agent, MCEB ITP:

15.1 Is responsible for ICTO staffing, coordination of JITC's position on ICTO requests, tracking ICTOs using the STP, ensuring the status of ICTOs is accurate, and keeping the JS J-6 and proponents informed of the status of ICTOs that are expired or need attention, and provide material for the STP and MCEB ITP portion of the JITC website.

15.2 Ensures that any policy related JITC position presented at the MCEB ITP, or to ITP members, represents JITC's position and is coordinated in advance with the Chief, PP&WSD.

15.3 Provides a distribution list (organizational postal addresses) for JITC certification memoranda (comprising appropriate members of the MCEB ITP), as needed.

15.4 Provides an e-mail distribution list (SMTP addresses) for the ERD core list for certification letter distribution, as needed. Each organization in the postal distribution list shall have one or more e-mail addresses.

15.5 Performs other duties related to the position of EA of the MCEB ITP, IAW the ITP charter and as coordinated in advance with the Chief, PP&WSD.

16. All JITC personnel responsible for T&E plans and reports, and status reporting, including all Branch Chiefs, Action Officers (AOs) and appropriate support contractors:

16.1 Gain familiarity with the following material: (These documents can be found on the [JITC Home Page](#), Outlook™ Public folder, or T drive)

16.1.1 [CJCSI 6212.01](#)

16.1.2 [CJCSI 3170.01](#)

16.1.3 [CJCSM 3170.01](#)

16.1.4 [DODD 4630.5](#)

16.1.5 [DODI 4630.8](#)

16.1.6 [DODD 5000.1](#)

16.1.7 [DODI 5000.2](#)

16.1.8 [Interim Defense Acquisition Guidebook](#)

16.1.9 Items in the "Certification Policy" folders in the Outlook™ JITC-FHU Public Folder and the T drive: [Plans and Policies Training Folder](#).

- Public Outlook folders:
 - [Public Folders](#)
 - [JITC WEST](#)
 - [Command Information](#)
 - [CERTIFICATION POLICY](#)

17. Lead Action Officers:

17.1 Are responsible for all AO responsibilities, in addition to the following.

17.2 Serve as the central/single JITC POC to coordinate all issues involving requirements, testing, certification, and funding, including any MOA/MOU with the system sponsor. This shall include ensuring that necessary test methodologies, test tools and procedures and support systems are available or developed, as needed. Any work for foreign customers shall be coordinated with the Business Management Branch (JTGB) (funding can be a serious issue).

17.3 Ensure that test tools and procedures (including those developed by other organizations) for interoperability and standards conformance testing are validated.

17.4 Establish an Integrated Test Team (ITT) that consists of the lead AO and support staff and representatives of all the support test divisions as soon as the program has been established with JITC. For new types of testing, coordinate with P&PB on developing an adequate test methodology.

17.5 Develop a charter for the ITT that clearly identifies the roles and responsibilities of each party involved in the test and evaluation.

17.6 Conduct periodic In-Progress Review (IPR) meetings to brief management on the status of the program, and ensure everyone on the team is on the same sheet of music. Ensure that we do not give conflicting information to our customers, personnel, or other organizations, especially the JS.

17.7 Ensure that the program's overall JITC T&E and certification strategy is technically sound and thoroughly evaluates the system's capability/requirements to minimize the risk to the Warfighter.

17.8 Identify the user(s) or user representative to assist in the assessment of the expected operational impacts of any discrepancies or the case where some requirements are not met.

17.9 Actively participate in those activities required for the division/branch to satisfy its responsibilities as the lead for a particular functional/mission area, as appropriate.

18. **Action Officers (AOs):**

18.1 Acquire working knowledge of the following material:

18.1.1 DOD Interoperability Policy (as noted above).

18.1.2 DOD Architecture Framework (DODAF)/CADM.

18.1.3 GIG Architecture

- GIG Architecture V1 & V2
- DISR (JTA standards)
- JMA/UJTLs/etc.

18.1.4 GIG ES/NCES

18.1.5 NR-KPP elements

- N-COW RM
- Information Exchange Architecture Products
- KIPs
- IA

18.1.6 JITC tools: STP, ERD, C2IP, TechLib

18.1.7 DISA/DOD tools: JCPAT-E, DISRonline (JTAonline), LISI InspeQtor

18.2 Understand the program/system/components under test sufficiently to represent JITC professionally and authoritatively at Test Integration Working Group (TIWG) or other meetings. (AOs should not rely totally on contractor support for expertise. AOs need to acquire adequate knowledge about the program/system under test to be able to determine whether JITC/ Program Manager (PM)/proponent plans are the right thing for the program.)

18.3 If a system will eventually require joint interoperability certification, assist the program/system sponsor to work towards that goal, regardless of the type of support initially requested. AOs should inform the PM/proponent about DOD interoperability policy and procedures and work with them in achieving interoperability.

18.4 Review system capability/requirements documents. Ensure the sufficiency and testability/measurability of the I-KPP/NR-KPP and other interoperability requirements. If problems are discovered with requirements, coordinate with P&PB first, notify the

PM/proponent, and coordinate with the JS J-6 to resolve issues as soon as possible. Copy P&PB on all correspondence with JS.

18.5 Prepare an Interoperability Certification Evaluation Plan (ICEP) and/or an Interoperability Test Plan (ITP) IAW with this instruction, as appropriate. Coordinate with the PM/proponent on JITC products. Ensure that the PM/proponent understands that we will perform an interoperability evaluation based on JS J-6 certified requirements, and will issue a certification letter as appropriate. Do not promise a certification letter!

18.6 Prepare and staff a strawman certification letter and summary report with P&PB to ensure that valid requirements were used for planning the test, all known issues have been worked out, expected outcome is identified, etc. This is to avoid any post-test surprises from Certification Panel comments, which could be a recommendation to not issue a certification.

18.7 Execute the appropriate plan(s): ICEP, ITP, and any other applicable plan (e.g., generic test plan, standards conformance standard test procedure, Key Interface Profiles (KIPs)).

18.8 Prepare and staff a test report, as appropriate, compliant with this instruction and [JITC Instruction 210-85-1](#), Documentation of Test and Evaluation Activities.

18.9 Prepare and staff status, assessment, certification, and related letters, compliant with this instruction.

18.10 Create/update STP entries and maintain ERD project distribution lists, compliant with this instruction. See enclosures 11 and 12, for ERD and STP processes.

18.11 Ensure that all JITC formal products go through the appropriate review processes and that the ERD is used for softcopy distribution. See enclosures 6 and 11, for document review and ERD processes.

18.12 Support requests for status, review of ICTO and C2IP proposals, etc., as assigned, and coordinate with other divisions and AOs, as appropriate.

18.13 Follow JITC policy and procedures, in coordination with the lead AO, when establishing an MOA/MOU is appropriate.

19. **Support Action Officers:**

19.1 Are responsible for all AO responsibilities, in addition to the following.

19.2 Coordinate all funding, T&E, and certification efforts with the lead AO.

19.3 Provide adequate technical support and expertise to the lead AO for document review, and test planning, execution, analysis, and reporting.

20. **System Tracking Program Coordinators:**

20.1 Manage access to the STP database.

20.2 Ensure that the STP is updated with capability/requirements document and certification status information, as available.

20.3 Update the STP database with test information (e.g., plans, reports, assessments, certification letters/summaries, Operational Test Readiness Review (OTRR)) received from the ERD tool or from other sources.

20.4 Notify AOs of incomplete information/discrepancies in STP and follow-up until the action is completed.

20.5 Assist AOs and external customers in all matters related to STP.

20.6 Provide training in the use of the STP.

20.7 Review products submitted to the Certification Panel to verify the correctness of the STP entries and provide comments to the AOs and JITC Certification Panel.

20.8 Review "Admin Alert" to periodically check for possible duplicate systems or missing/incorrect data.

21. **The JITC Technical Librarian:**

21.1 Processes classified and unclassified documents related to JCPAT-E document reviews, and other appropriate T&E and interoperability material.

21.2 Tracks and maintains accountability of all documents.

21.3 Ensures when possible that unclassified JCPAT-E documents are available via the TechLib32 tool either through scanned image files or softcopy versions of documents (e.g., C4ISP files on the t: share drive). The goal will be to have documents entered into the library and available electronically within 2 business days.

This Page Intentionally Blank

CERTIFICATION PROCESSES

1. **General.** In accordance with DOD interoperability policy (DODI [4630.8](#), CJCSI [6212.01](#)), all Information Technology (IT) systems, including National Security Systems (NSS), with external interfaces must be evaluated and certified by JITC. All systems (Acquisition Category (ACAT), non-ACAT, and fielded) whose Joint Potential Designator is not INDEPENDENT, must be certified before initial fielding and periodically throughout the system life cycle. The JITC certification process follows from the process described in CJCSI [6212.01](#), enclosure M.

2. **Four Step Process.** The JITC has established a four-step method to ensure systems are adequately evaluated during the certification process. These steps are: identifying capability/requirements, developing a certification approach (planning), testing/evaluating, and certifying/status reporting. An overview is provided in the main body of this instruction, while the material below adds additional considerations.

2.1 **Identifying and Verifying Interoperability Capability/Requirements.** If the desired product of the evaluation effort is a Joint System Interoperability Test Certification, then the system must have Joint Staff (JS) J-6 certified capability/requirements. The Joint Capabilities Integration and Development System (JCIDS) is described in CJCSI [3170.01](#). JCIDS is the process the JS J-6 uses to certify capability documents. See enclosure 9 for JITC's role in the JCIDS process.

2.1.1 All IT and NSS must have a JS J-6 certified Net Ready Key Performance Parameter (NR-KPP) prior to JITC Joint System Interoperability Test Certification. The JS J-6 may waive the requirement for an NR-KPP on a case-by-case basis. When waived, the source of interoperability requirements will be specified by JS J-6.

2.1.2 The Joint C4I [Command, Control, Communications, Computers, and Intelligence] Program Assessment Tool –Empowered (JCPAT-E) and the System Tracking Program (STP) can help determine if the system has JS J-6 certified capability/requirements.

2.1.2.1 The JS uses JCPAT-E as a repository for capability/requirements information. JCPAT-E resides on the SECRET Internet Protocol Router Network (SIPRNet). Before gaining access to this tool, an AO must first have SIPRNet access. Once the AO accesses the JCPAT-E, the AO will be able to use the search tool and look for the system's documents. Additionally, the AO should be able to determine if the JS J-6 has certified the documents. The AO will also be able to read the comments the assessors submitted on a particular document. (See enclosure 9 for further information on JCPAT-E access and use.

2.1.2.2 The STP is an UNCLASSIFIED database located on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and SIPRNet. It is available to users from a .MIL or .GOV domain. The STP will indicate if a particular system has certified requirements, based on information obtained from the JCPAT-E. However, the actual capability/requirements documents do not reside on the STP, and information obtained from the STP should be confirmed before use. An AO will need to access the JCPAT-E or JITC technical library for the documents. See enclosure 11 for an STP description.

2.1.3 System capability/requirements must be testable and measurable. Unless there is still a valid, certified Operational Requirements Document (ORD)/Interoperability Key Performance Parameter (I-KPP) package, a Capability Production Document (CPD) and/or an Information Support Plan (ISP) is used to identify interoperability requirements. The search for requirements should focus on the NR-KPP. This should lead to a detailed analysis of the interfaces and information exchanges defined in the integrated architecture products, and the implemented standards, as well as Net-Centric Operations and Warfare Reference Model (NCOW RM) compliance, KIPs compliance, and Information Assurance (IA) requirements. See enclosure 9 for JITC's role in ensuring testable and measurable requirements. Requirements will be more understandable if the AO also becomes familiar with related documentation, such as other JCIDS documents for the system and interfacing systems, interoperability and interconnectivity capability (IIC) profiles, Joint Functional Concepts, Joint Operational/Integrated Architectures, etc.

2.1.4 If the system does not have testable/measurable requirements, or there are other requirements issues, the AO must coordinate with the program manager (PM) and the JS J-6 to resolve the issue. JITC cannot make any changes to or ignore any JS certified requirements. This proscribes "moving" requirements to a later spiral or block or changing the criticality of requirements.

2.2 Develop a Certification Evaluation Approach (planning). The (PM/proponent and JITC will work closely to establish a strategy for evaluating interoperability requirements in the most efficient and effective manner, in an operationally realistic environment. This evaluation strategy identifies data necessary to support an interoperability evaluation as well as the test events/environments planned to produce that data. The PM/proponent should coordinate with JITC to integrate interoperability into the system's T&E documents (e.g., Test and Evaluation Master Plan (TEMP), test plans). Additionally, complex systems that depend on multiple evaluation events will require JITC to develop an Interoperability Certification Evaluation Plan (ICEP).

2.2.1 In order to develop the correct approach, an AO should follow this list of AO best practices.

2.2.1.1 Inform the PM/proponent about the interoperability evaluation and certification processes. This will give the PM/proponent an overview of the entire effort and will allow them to budget correctly.

2.2.1.2 Identify all of the valid interoperability requirements and criticality. The AO should find these defined in the applicable ORD/CPD/ISP. This is NOT the time to start paring down which of these requirements can be tested because of cost considerations.

2.2.1.3 Ensure all of the requirements are well defined and testable. If the system's requirements aren't testable and measurable, the AO must coordinate a remedy through the JS J-6. JITC cannot add or delete items or change the criticality and still consider the result as

certified requirements. This includes requirements moving from one block/spiral/increment to another.

2.2.1.4 Determine what test events are necessary to assess all of the requirements. This is where the AO determines how to test to ensure end-to-end interoperability in as operationally realistic environment as possible.

2.2.1.5 Identify the project constraints: time, equipment, funding, and personnel.

2.2.1.6 Perform a cost/benefit analysis: affordable confidence level. This is where we try to match the project constraints to the system requirements and determine which requirements can be affordably tested.

2.2.1.7 Prioritize testing – even if plans are to test everything, coordination with other JITC divisions is required to ensure that other testing is not competing for the same resources. (See CJCSI [6212.01](#), enclosure A, for organizational and functional prioritization of interoperability testing and certification. Scheduling conflicts that cannot be resolved within JITC will be submitted to the Military Communications-Electronics Board (MCEB) Interoperability Test Panel (ITP) for resolution.) Ensure, at a minimum, that all critical and higher risk (e.g., immature or evolving standards) requirements are thoroughly tested.

2.2.1.8 Coordinate with the Plans and Policies Branch (P&PB), PM/proponent, JS J-6, and MCEB ITP, as necessary.

2.2.2 The scope of testing will depend on several factors. The AO should consider risk to the warfighter when determining how much testing is sufficient. The quality of the data is more important than simply acquiring quantities of raw data. The AO needs to ensure there is sufficient data to maintain a reasonable confidence level. When determining the scope of effort an AO should consider the following:

2.2.2.1 Mission criticality.

2.2.2.2 System complexity. Large, complex systems with multiple information exchanges may require more thorough testing.

2.2.2.3 Number and criticality of the interfaces.

2.2.2.4 Maturity of technology.

2.2.2.5 Military unique features vs. commercial off the shelf (COTS) capabilities.

2.2.2.6 System performance in the field, exercises, and participation in other tests.

2.2.3 This process results in two types of plans: ICEP and Interoperability Test Plan (ITP). The product(s) used will depend on several factors. The complexity of the system (e.g., single item, FoS/SoS, number of external interfaces), development approach (e.g., COTS, spiral with

numerous increments), and the anticipated number of JITC and non-JITC conducted test events are important factors to consider. An ICEP establishes an overall plan on how a system or FoS/SoS will be evaluated. An ICEP will usually point to individual test plans for the details on testing component systems. All JITC conducted tests require a test plan, and some systems may need an ICEP. (Refer to [JITCI 210-85-01](#) and related guidance for further policy on test plans and reports.) In parallel with plan development, P&PB offers a preliminary review of draft test reports and certification letters (sans the results and conclusions, of course) to expedite the reporting process and reduce the risk of incorrect requirements or inadequate testing being discovered after conclusion of testing.

2.3 Testing (Collecting and Analyzing Interoperability Data). Interoperability testing frequently relies on data collected during other testing events to provide a cost effective interoperability evaluation. Test data from standards conformance testing, developmental testing, operational testing, interoperability tests, live/simulated exercises, and field use may contribute to an interoperability evaluation. The data should be comprehensive, accurate, and repeatable. The analysis should focus on conclusive results representing the entire range of operational uses, configurations, and conditions. Most importantly, the analysis must contain an assessment of expected operational impacts of any discrepancies. The goal is to provide the user with a complete picture of capabilities, problems, and risks.

2.3.1 When JITC is not the responsible testing organization, the system PM/proponent will coordinate interoperability test plans, analysis, and reports with JITC to ensure sufficient information is available to support a certification determination (per CJCSI 6212.01). System PM/proponent must coordinate testing changes (e.g., schedule, locations, scope, methodology, etc.) with JITC, since such changes may impact JITC's ability to certify the system.

2.3.2 When JITC is the responsible test organization, JITC will develop the necessary plans and reports and coordinate them with the system PM/proponent. Regardless of the responsible test organization, tests must employ production representative systems in an operationally realistic environment as practicable.

2.4 Determine the Interoperability Status. JITC uses data from various types of testing to produce interoperability reports and certifications, as appropriate. Interoperability evaluation will be an independent analysis of the data and determination of the operational interoperability status by JITC. To support the JS J-6 NR-KPP validation, Joint System Interoperability Test Certifications report on the interoperability status of individual interfaces, the status of top-level exchange requirements, and any other system interoperability performance parameters. JITC distributes Joint System Interoperability Test Certifications to the MCEB ITP members, JS J-6, the PM, and other interested, authorized parties. JITC interoperability products include those described in the next section, though not all products may apply to all systems.

3. T&E and Certification Products. The following describes the typical certification related products in the order in which they are normally produced. New types or variations of these products shall not be used without prior coordination with P&PB and the granting of a waiver for new products. This is necessary to ensure that impacts to JITC processes and tools are properly considered and action taken to update policy, procedures, training material, web pages,

interoperability databases and tools (e.g., STP and the Electronic Report Distribution (ERD) Tool). Similarly, standard terminology shall be used, especially for any items entered into databases (e.g., assessment status of "met", "not met", or "not tested" are valid entries in the STP, while terms such as "passed" are invalid). A division imposing unique requirements on the JITC T&E and certification infrastructure may be asked to fund part or all of any needed changes that are not of overall benefit to JITC. Presentation Certificates (not to be confused with certification letters) may be issued at the time a certification letter is issued, however, for interoperability certifications they shall only be issued when a system has met threshold or objective requirements. Presentation Certificates shall not be issued for assessments or "specified interfaces" interoperability certifications.

3.1 Standards Conformance Certification. Issued after technical testing against standards/standards profiles to describe the degree of conformance to that standard (e.g., conformance to MIL-STD-188-181). Additional testing may be required to determine compliance with standards profiles. JITC can perform standards conformance testing and certification against any standard that can possibly affect interoperability. Both U.S. and non-U.S. systems are eligible for a Standards Conformance Certification. Standards conformance is certified in a standards conformance memorandum (or commercial letter), and may be reported separately from interoperability status. All standards conformance testing and certification performed by a support division will be closely coordinated with the lead division. Distribution of Standards Conformance Certifications should include the ERD Conformance Certification Letter Core List.

3.2 Joint Interoperability Assessment. Issued following interoperability testing (Operational Assessments, JITC interoperability assessments, etc.) to provide feedback concerning interoperability strengths and weaknesses when a certification is not appropriate. An interoperability assessment is not sufficient to support a fielding decision. JS J-6 certified requirements are not necessary for an assessment, and not all requirements must be assessed, however, it is best to depict all of the requirements in the assessment letter, as is done for interoperability test certifications. Distribution of assessment letters may be limited to the PM/proponent and any other interested, authorized parties. Any systems, U.S. or not, are eligible for an Interoperability Assessment Letter.

3.3 OT Readiness Review (OTRR) Interoperability Statement. JITC input, as appropriate, to the OTRR assessing whether a system is ready for Operational Test and Evaluation (OT&E) from an interoperability perspective. JITC is directed to certify -- for all applicable IT and NSS programs -- to the Operational Test Agency (OTA) during (or before) the OTRR:

- The status of all IT and NSS interoperability and standards conformance issues.
- That all required Developmental Testing (DT) relating to IT and NSS interoperability has been successfully completed.
- That no outstanding issues preventing the commencement of OT&E remain. [[DODI 4630.8](#)]

For those programs where JITC has been involved, JITC will provide input to the OTRR covering interoperability aspects of the program based upon available pertinent information.

Since complete interoperability testing will not have been completed before OT, this input will usually be an informational status memorandum rather than a certification letter. When JITC is requested to provide input to the OTRR, or Milestone C decision, the lead AO will produce the memorandum, coordinated with other appropriate divisions to ensure that JITC provides a consolidated position. Distribution shall include the ERD Interoperability Certification Letter Core List (JS J-6 and MCEB ITP members). If requested, similar input will be provided for the Developmental Test (DT) processes.

3.4 Interoperability Test Certifications. Interoperability Test Certification involves an evaluation of information interoperability with respect to interoperability capabilities and requirements. See enclosure 8 for NR-KPP, I-KPP, and other evaluation methodologies. JITC issues "full" system certifications when all critical interoperability requirements are met (i.e., all critical interfaces and top-level exchange requirements, or equivalent, are met) and there are no discrepancies with critical operational impact. When appropriate, JITC issues "Specified Interfaces" certifications to provide the system interoperability status when only a subset of critical interfaces have been adequately demonstrated. JITC updates Interoperability Test Certifications throughout a system's life cycle to reflect changes in the system, status, and environment. All JITC interoperability test certifications expire upon changes that may affect interoperability. Additionally, all certifications expire three years from date of issue.

3.4.1 Special Interoperability Test Certification. Issued for systems or system components (e.g., network infrastructure components) that require operational interoperability certification but are not subject to the JCIDS process and do not need requirements certified by the JS J-6 (e.g., commercial switches being procured to operate in the DSN). JITC must coordinate with the JS J-6 to verify that the item is not subject to JS J-6 requirements certification.

3.4.2 Joint System Interoperability Test Certification -- Specified Interfaces. Issued when a system has adequately demonstrated operational interoperability for a subset of critical interfaces. A specified interfaces certification may not be sufficient to allow fielding. If military necessity warrants fielding of the system for the demonstrated capabilities, the system PM/proponent should contact the JS J-6 to request a formal modification of the NR-KPP or the MCEB ITP for an Interim Certificate to Operate (ICTO). The system must have JS J-6 certified requirements to receive this certification.

3.4.3 Joint System Interoperability Test Certification. Issued when a system has adequately demonstrated operational interoperability for all critical threshold requirements pertaining to a specific release. This full system certification attests that the system's interoperability is sufficient to support a fielding decision. Evaluation should continue until the status of all objective requirements can be determined and reported. The system must have JS J-6 certified requirements to receive this certification.

4. Special Considerations. The following highlights areas warranting special consideration when performing T&E and certification related activities.

4.1 Data Collection. All valid interoperability data should be used, as appropriate, in the interoperability evaluation and certification process. Each potential data collection opportunity

should be reviewed and used in the overall certification evaluation process to get the best interoperability picture of the system in the most efficient manner.

4.1.1 Developmental Testing – Developmental testing performed under government supervision that generates reliable, valid data can be used to determine technical performance capabilities, specification/standards conformance status, and may supplement operational data for an interoperability evaluation.

4.1.2 Standards Conformance Testing – This testing establishes the extent to which a system conforms to the requirements of a standard or complies with levels specified in a standard. These standards may include government, commercial, or North Atlantic Treaty Organization (NATO) standards as long as the requirements specified are measurable and testable. Conformance to applicable standards is necessary, but not sufficient, for interoperability. Additional testing is required to ensure that all required information exchanges meet user requirements in the intended operational environment.

4.1.3 Assessments – Assessments are data collection opportunities, such as demonstrations and exercises, lacking some aspect necessary for a complete interoperability evaluation. However, assessments contribute valuable pieces of data reducing and simplifying the requirements for later testing. Other reasons for conducting assessments include program office requests, system functional validation, or opportunities for cost effective data collection before known system problems have been eliminated.

4.1.3.1 Demonstrations and exercises offer the opportunity to identify systems in use that have not been certified and to verify the results of interoperability testing under field conditions. The usefulness of data from demonstrations and exercises depends upon the realism of the event and data availability. In many cases, the available data provides an incomplete picture of the system's ability to meet the users' needs. However, if the environment closely resembles the intended operational use, the conditions under which the system is operating can be effectively monitored to capture the data exchange, and the performance of the system of interest can be accurately measured, the data collection opportunity may be adequate to support even an interoperability evaluation. The Defense Interoperability Communications Exercise (DICE) provides one of these exceptional events.

4.1.4 Interoperability and Operational Testing – Interoperability testing must be conducted in an environment that is either equivalent to the intended operational environment, or one in which the aspects that could impact interoperability are realistic enough that users can be confident that test results are predictive of field performance. In many cases it may be necessary to conduct testing both in a controlled environment with full instrumentation and in an operational environment to measure the operational effectiveness of the information exchange.

4.2 Funding. Funding for interoperability certification, including planning, testing, analysis, and reporting is the responsibility of the system PM/proponent.

4.3 Other Certifications. JITC Joint System Interoperability Test Certification is focused on information exchanges and operational use over external system interfaces. There may also be

other certifications, validations, or accreditations required before fielding a system (e.g., DODI 5200.40 (DITSCAP), Information Assurance (IA) and security, electromagnetic spectrum, and authorization to connect to specific networks).

CERTIFICATION CHECKLIST OR STATUS SHEET FOR ACTION OFFICERS

1. This enclosure provides the Action Officer (AO) a guide for the certification process.

Certification Checklist

Initial Coordination	
1. Do we have Joint Staff (JS) J-6 certified requirements, i.e.: <ul style="list-style-type: none"> • Operational Requirements Document (ORD) with Interoperability Key Performance Parameter (I-KPP)?* • Command, Control, Communications, Computers, and Intelligence Support Plan (C4ISP)?* • I-KPP?* • Capability Development Document (CDD)?* • Capability Production Document (CPD)? • Net Ready Key Performance Parameter (NR-KPP)? • Information Support Plan (ISP)? • Generic Switching Center Requirements (GSCR)/ Generic Switch Test Plan (GSTP)? • Other?* 	
* -- requires coordination with Plans and Policies Branch (P&PB) (JTAB) and possibly JS J-6 before use.	
1.1. If the answer to the preceding question is negative, has the program manager (PM)/proponent initiated coordination through their channels with JS J-6 for waiver, or for approval for a Special Interoperability Test Certification?	
2. Do we have measurable, testable, information exchange specification in the relevant architecture framework products , i.e., Operational View (OV)-3, OV-6C, System View (SV-6), etc.?	
3. Are the OV-1*, SV-1*, and more detailed exchange definitions clearly traceable? Can we clearly trace from a specified system or other information exchange back to corresponding need lines in the OV-1 and/or SV-1? * -- or equivalent.	
4. Have we documented an unambiguous mapping between the specified information exchanges and the hardware and/or software interfaces we need to test to verify those exchanges?	
5. Have we identified interoperability-related requirements not specified in the standard architecture products, e.g., parallel/simultaneous operation, redundancy, quality of service, recovery capability, jam-resistance, accuracy, precision, etc.?	
6. Have we examined the standards profile (Technical View (TV)-1) and determined what standards conformance certifications or other verification is appropriate and/or available?	
7. Have we identified other Developmental Test (DT)/Operational Test (OT) results that are or will be available and initiated coordination to examine the relevant documentation?	

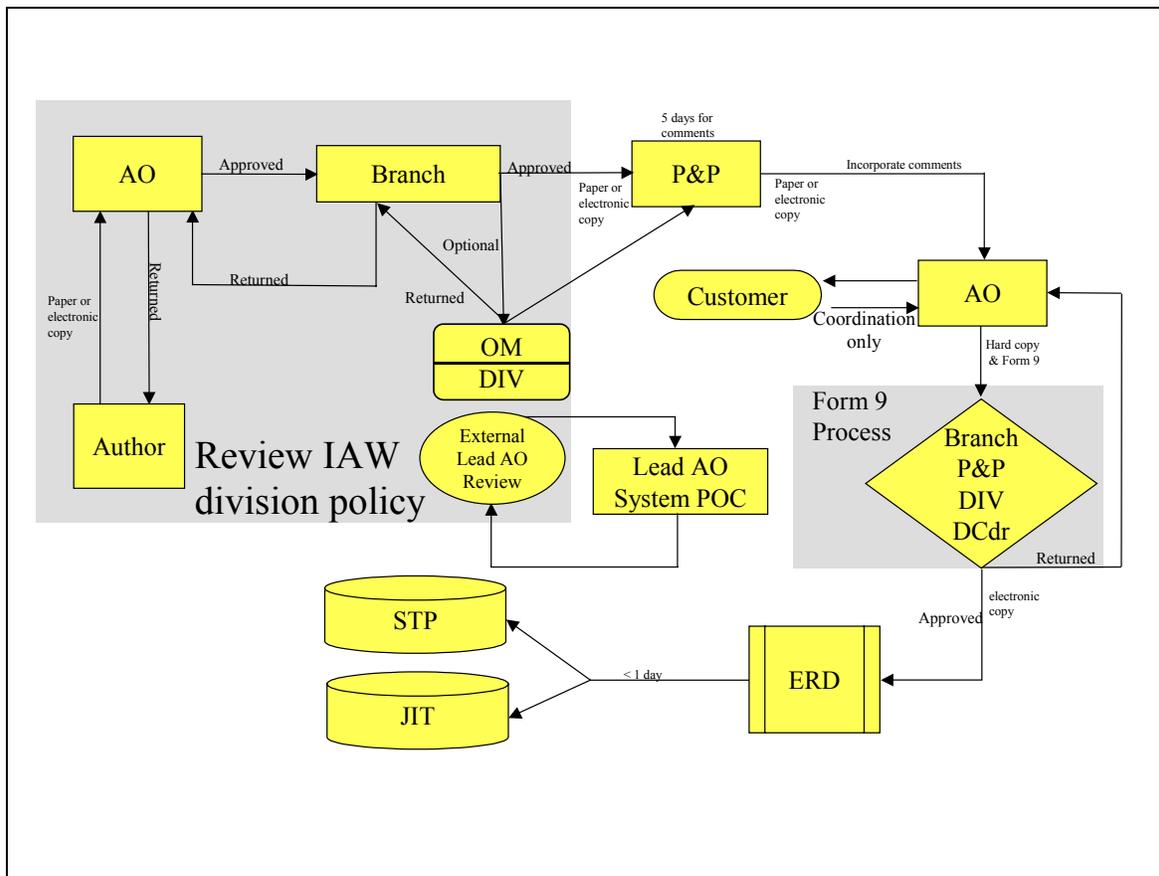
8. System Tracking Program (STP) actions: <ul style="list-style-type: none"> • Have we checked STP for this and related systems to see what system level actions may be required? • Have we updated the System Under Test (SUT) entry with the most current information? • Have we added any past or projected test/activities related to this certification? 	
9. Have we drafted a strawman certification memorandum and summary with exchange and interface matrices, architecture diagrams, and preliminary configuration data for local and P&PB review and identification of additional data requirements and format verification?	
10. Have we drafted strawman Interoperability Certification Evaluation Plan (ICEP) and/or Interoperability Test Plan (ITP) for preliminary local and P&PB review and consistency check with the strawman certification?	
11. Have we coordinated with the PM/proponent to ensure our data, test planning, and associated resource requirements are incorporated in the next version of the Test and Evaluation Master Plan (TEMP)?	
Test Planning	
1. Are all of the formally defined requirements reflected in our certification and test planning documents, even those we are not testing or evaluating?	
2. Are all of the interoperability-related requirements we identified outside the architecture framework products reflected in our planning?	
3. Can we trace each formal requirement we have identified, either in the standard framework products or elsewhere, directly back to the respective product, diagram, or text in the relevant requirements documentation?	
4. Have we established clear measures, and unambiguous criteria in terms of those measures, for determining, for each exchange or other requirement to be evaluated, whether or not to certify it?	
5. Have we identified appropriate user representatives for the system application domain or mission area to assess impact of any discrepancies that may be discovered in testing, and coordinated with them for review of such results?	
6. Have we identified, and assessed, potential test and certification impact, of known documentation or resource limitations, and provided placeholder paragraphs in our test planning and strawman test reporting documentation?	
7. Have we identified potential requirements ambiguities and initiated coordination to resolve them with the PM/proponent or PM/proponent coordination through their requirements channels with the JS J-6?	
8. Have we obtained and reviewed available DT/OT documentation and identified interoperability relevant results that may apply to our current certification efforts?	
9. Have we identified and documented the relevant configuration data (e.g., system and software versions, protocols/languages/formats and versions, or specifying documents and dates, relevant connection configuration data) for both primary exchanges to be evaluated and any alternate or work-around modes to be employed?	
10. Have we submitted the ICEP and/or ITP for the current effort to P&PB for formal review, and resolved any review issues raised?	

Certification Memorandum and Summary	
<p>Do the memo and summary follow the format and content guidance in the examples?</p>	
<hr/>	
<p>1.1. Letter (Memorandum):</p> <ul style="list-style-type: none"> • Does paragraph 2/4 (System and Interface/Exchange) clearly indicate the status of the overall I-KPP or NR-KPP, as well as individual exchange or interface results in appropriate tables? • Are the system and version tested and certification status clearly identified in the title and paragraph 2? • Are critical qualifications to the overall certification status clearly indicated in paragraph 2? • Are test dates, venues, and other significant test context clearly specified in paragraph 3 (Testing Information)? • Are the current versions of DODD 4630.5 and CJCSI 6212.01 identified as the first two references? 	
<hr/>	
<p>1.2. Summary:</p> <ul style="list-style-type: none"> • Does paragraph 5 (SUT Description) clearly indicate the nature and function of the system and its place in the associated Family of Systems (FoS) and/or System of Systems (SoS)? • Does paragraph 6 (Operational/System Architecture) contain an <u>operational/system</u> architecture (e.g., OV-1, SV-1), cite its source, and provide suitable supporting text? • Does paragraph 7 (System Interoperability Requirements) clearly identify required exchanges and interfaces and their mapping? • Does the information in paragraph 7 correlate clearly with the information provided in memorandum paragraph 4 (Interface/Exchange Status)? • Does paragraph 7 clearly identify any interoperability-related requirements in addition to the basic information exchange and interface requirements that were identified during coordination and planning? • Do paragraphs 8 and 9 (Test Network and System Configuration) contain sufficient network, test item, and interfacing system configuration and protocol information to clearly identify the system tested, interfacing systems, and relevant test environment constraints? • Does paragraph 10 (Testing Limitations) include limitations identified in coordination and planning and those identified or arising during test configuration and execution, to include alternate or work-around solutions? • Does paragraph 11 (Evaluation Results) state results for required exchanges, interfaces, and for the overall system? • Is assessed expected operational impact of anomalies or deficiencies indicated for individual exchanges/interfaces and for the overall system? 	

Review and Coordination	
1. Have you performed all branch or section internal review and staffing?	
2. Have you updated the STP system and test/activity record entries to reflect current test status, dates, Point of Contact (POC(s)) and interfaces?	
3. Have you forwarded softcopy of the completed letter and summary to the JITC Certification Panel for review?	
4. Have you addressed all the consolidated Certification Panel and STP coordinator comments in a revised draft?	
5. Have you forwarded your final draft folder:	
• With Form 9 attached and completed up to the JTAB initial block;	
• Hardcopy of the revised draft;	
• Hardcopy of panel comments, annotated with rationale, as appropriate, for comments not accepted, or clarifications where comments may have arisen from panel misunderstandings?	
• Electronic Report Distribution (ERD):	
• Is the correct core distribution list selected?	
• Have any additional addressees specific to this program or system been added?	
• Has the correct (final) version of the certification letter and summary been attached?	

TEST AND EVALUATION (T&E) PRODUCTS AND CERTIFICATION MEMORANDUM STAFFING PROCESS

1. **Introduction.** This enclosure covers the internal JITC staffing process used for Test and Evaluation (T&E) products and certification memoranda. These documents include: plans/reports, certification letters, extension certification letters, compliance and assessment letters, Operational Test Readiness Review (OTRR) input letters, and other status and related testing products. Specific examples and guidance for these types of documents are provided as part of this instruction package. Plans and Policies Branch (P&PB – JTAB) is responsible for managing and conducting formal JITC review processes.
2. **Distribution of Products.** The Action Officer (AO) will ensure the documents undergo the proper JITC review and staffing procedure before distribution to the customer. JITC delivers documents to all parties using the JITC Electronic Report Distribution (ERD) Tool. See enclosure 12 for the ERD process.
3. **JITC Review Processes.** There are three distinct review processes for JITC products, dependent on the type of document published (Plans/Reports, Certifications, and Miscellaneous Products). However, all of the formal reviews start with a thorough review at the AO and Branch Chief level. This ensures that the document is technically accurate and ready for formal review.
4. **Plans and Reports Review.** As the name implies, this process applies to Interoperability Certification Evaluation Plans (ICEPs), Interoperability Test Plans (ITPs), formal test reports, and similar documents. This process is illustrated in figure 6-1. Plans include: Interoperability Certification Evaluation Plans (ICEPs), Interoperability Test Plans (ITPs), Performance Test Strategies, Compliance Test Plans, Independent Verification and Validation (IV&V), etc. Reports include: Test Reports (e.g., Interoperability, Operational Test and Evaluation (OT&E), Joint Interoperability Certification Test Report, Quick Look, Performance Assessment, Follow-on Test and Evaluation (FOT&E)), Assessment Reports, etc.



Legend:

AO	Action Officer	OM	Office Manager
DISA	Defense Information Systems Agency	P&P	Plans and Policies Branch
DIV	Division Chief	POC	Point of Contact
ERD	Electronic Report Distribution Tool	STP	System Tracking Program
JIT	Joint Interoperability Tool		

Figure 6-1. Plans and Reports Review Process

4.1 The first steps in this process are accomplished in accordance with divisional policy. In general, the author will produce the document and present it to the AO for the first review. Once the AO is satisfied with the document, it is sent to the Branch Chief for review. The next step in the approval chain may be an optional review by the Office Manager (OM) and Division Chief. JITC policy states that documents will also be coordinated with the lead AO (system point of contact (POC)), as applicable. This lead AO review is an offshoot of the division review process and shall be completed before the document is transmitted to P&PB.

4.2 After a document passes the divisional review and any lead AO reviews, the AO will submit the document to P&PB for review. At this point, the AO should have created/updated associated System Tracking Program (STP) entries. P&PB will staff the document for review, with the goal of providing feedback to the AO within five 5 working days. Discrepancies with STP entries will be included in the feedback.

4.3 The AO will then review and incorporate P&PB comments in the document and correct STP entries, as appropriate. Additionally, the AO may provide a draft version of the plan or report to the customer of coordination purposes.

4.4 The next portion of the process involves Form 9 routing. Once again, this process starts at the branch level. Following any optional branch/division reviews, the document, in hard copy, and the Form 9 are routed to P&PB. P&PB will ensure that the document has gone through the initial review process. If not, the document will be returned to the AO for proper processing. If the initial review was accomplished correctly, P&PB will verify that any comments were adequately addressed. Following P&PB verification of required changes, the document is forwarded to the Division Chief and finally, the Deputy Commander.

4.5 Following Deputy Commander approval, the OM/AO will submit the document for ERD processing. The first step in the ERD process is to ensure that the project e-mail distribution list (ERD "recipient list") is correct. The OM/AO should verify that the document has been properly reviewed and received all necessary approvals. P&PB will make a final review of documents submitted to the ERD, verify that there is an appropriate STP entry, and provide final release authority. Once the document is distributed via the ERD (through e-mail), P&PB will ensure that the document is available on the STP and the Joint Interoperability Tool (JIT) servers.

5. Interoperability Test Certification Review. The formal certification review process applies to Interoperability Test Certifications. Interoperability evaluation concludes with a determination of the overall system interoperability status. The system may receive a "non-certification." If the system fails to achieve certification (or is otherwise sensitive or controversial), the JITC Commander must sign the memorandum before ERD submission. If the system is certified, the Division Chief may sign the certification memorandum. Figure 6-2 depicts the Certification Memorandum Review Process.

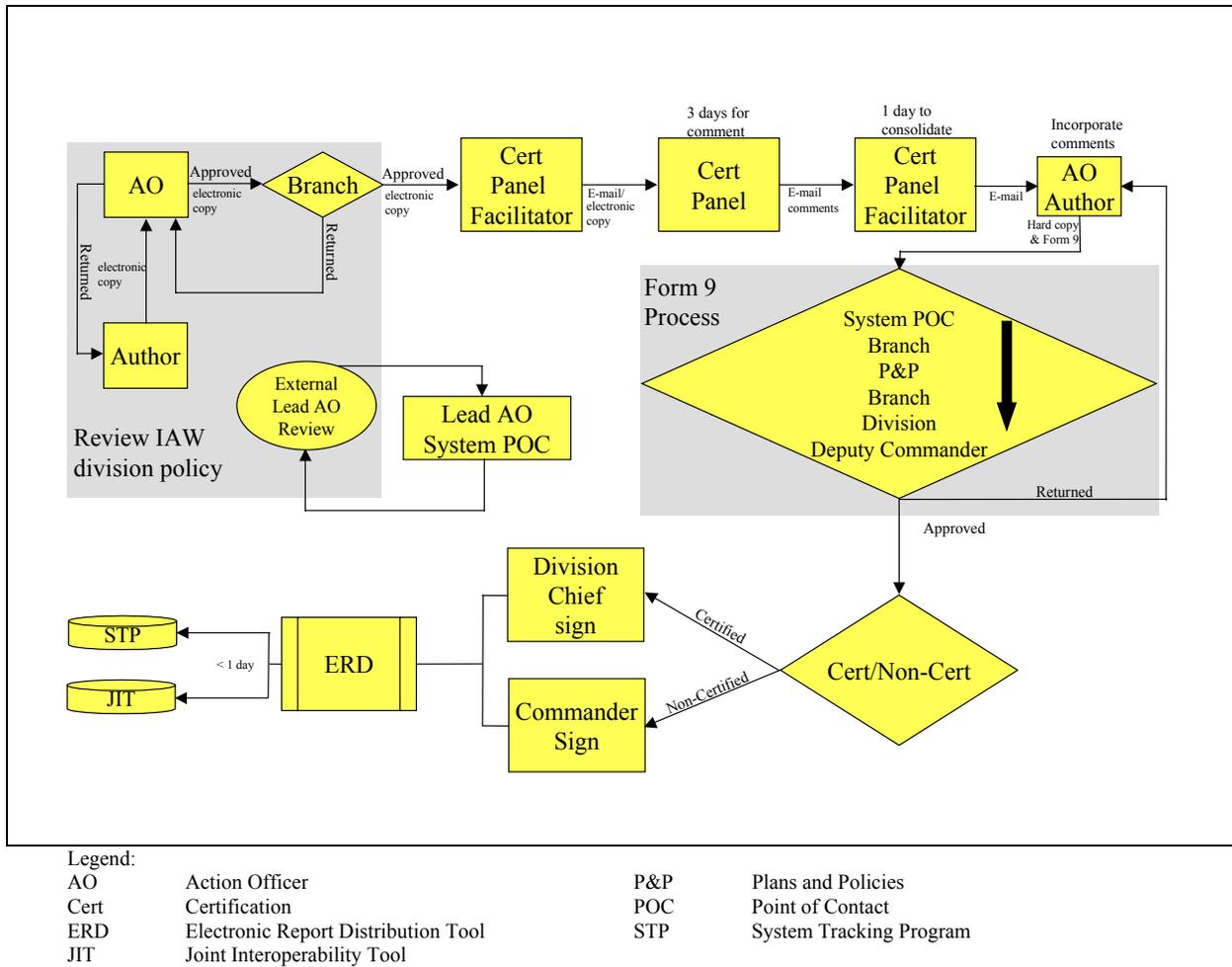


Figure 6-2. Interoperability Test Certification Memorandum Review Process

5.1 The beginning of this process is similar to Plans and Reports Review. After Branch Chief approval and coordination with the lead AO (system POC), a softcopy is sent (via e-mail attachment, with STP system/test identification and any special notes or instructions) to the [Certification Panel Facilitator](#). The facilitator (or designated alternate) will staff the document for review by the Certification Panel and other subject matter experts, as appropriate. The "Cert Panel" will review the document and provide comments to the facilitator by the suspense date specified in the staffing letter - usually three 3 working days. The facilitator will then provide a consolidated set of comments to the AO/lead AO. [STP Coordinators](#) will provide feedback on the adequacy of STP entries, so it is important to update the STP entries (including interface information) before submission to the Certification Panel. When the Certification Panel responds to the review tasking, they will use the "Reply to All" function in Outlook™. This gives the AO an advance copy of comments; allowing them to resolve potential issues and to start working on changes immediately to make the entire process more efficient. However, the AO is responsible for addressing all of the Certification Panel comments as provided in the consolidated set, and updating STP and ERD information.

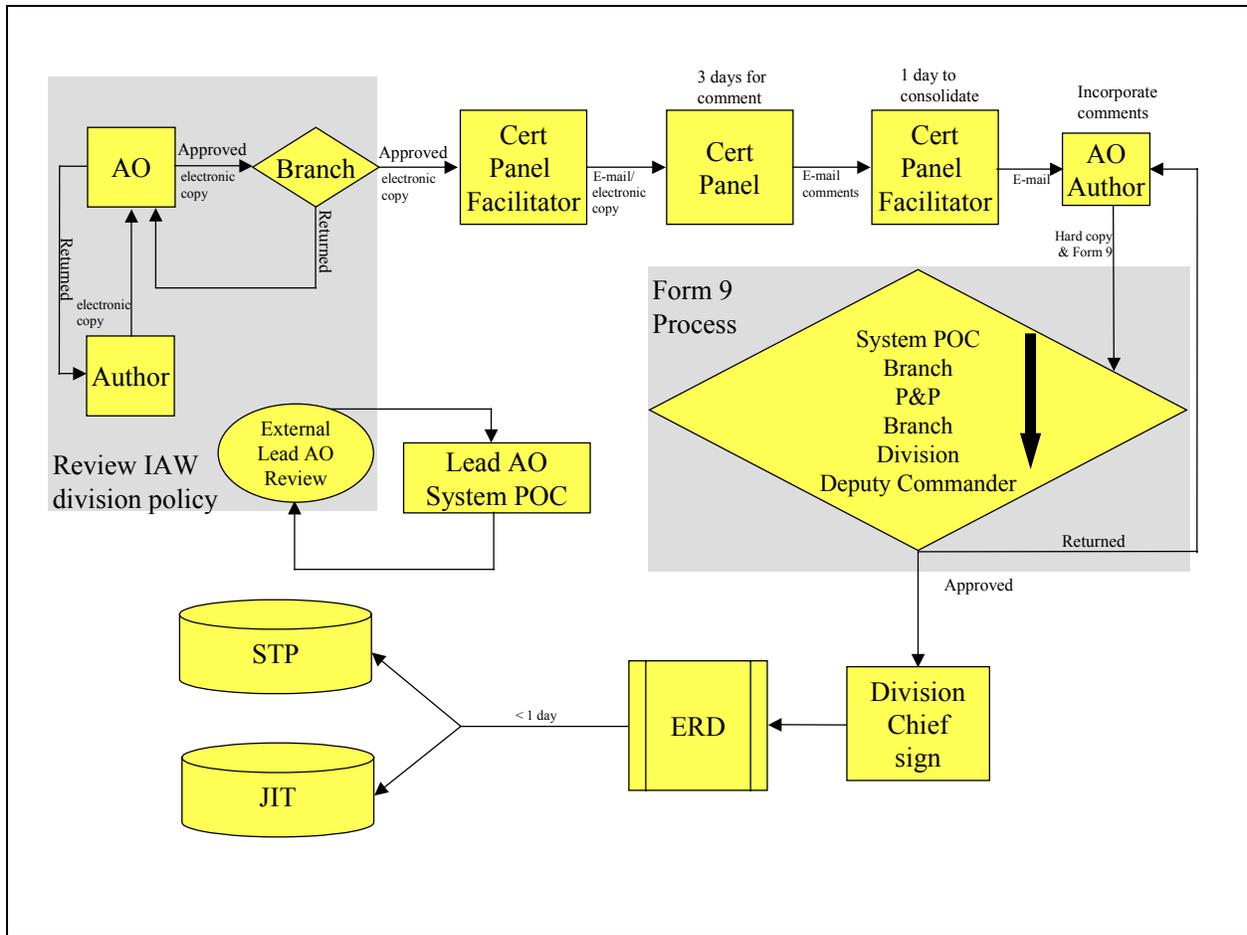
5.2 The certification memorandum Form 9 process is also similar to the other review processes. The initial Form 9 review for a certification document is the lead AO, if applicable, following the normal AO review and any optional reviewers (e.g., OM) per Branch/Division policy. The document will include the following routing as a minimum: JITC lead AO, Branch Chief, P&PB (Cert Panel Co-Chairperson), Branch Chief, Division Chief, and Deputy Commander. (For most divisions, this is followed by the OM for action leading to the ERD release.)

5.3 The next step in this process depends on whether the system interoperability status is an exceptional situation: a non-certification or otherwise sensitive or potentially controversial. As noted above, normally the Division Chief may sign and release the document to the ERD process, with the JITC Commander signing and releasing memoranda for exceptional situations. The document is then sent through the ERD process for distribution.

5.4 The ERD shall be used for distribution of certification letters, as with other T&E related products. P&PB will make a final review of documents submitted to the ERD, verify that there is an appropriate STP entry, and provide final release authority. Once the document is distributed via the ERD (through e-mail), P&PB will ensure that the document is available on the STP and JIT servers, and STP certification status information will be updated.

6. Standards Conformance Certification and Miscellaneous Testing Products. The last type of review process is actually two processes that differ in the requirement for a Form 9.

6.1 The first review outlined is for documents that require a Form 9. These products include: Standards Conformance Certifications (and non-conformance), Compliance Letters of various types, Interoperability Assessments, Functional Certifications, and similar documents. Figure 6-3 depicts this process.



Legend:
 AO Action Officer
 Cert Certification
 ERD Electronic Report Distribution Tool
 JIT Joint Interoperability Tool
 P&P Plans and Policies
 POC Point of Contact
 STP System Tracking Program

Figure 6-3. Miscellaneous Products Review Process

6.1.1 This process is almost the same as described for the Interoperability Certification Review. The significant difference is that the Division Chief has the signature authority for these documents, even in the case of non-conformance certifications.

6.2 The next review outlined is for those miscellaneous documents that do not require a Form 9. These products include: OTRR Input letters, Interoperability Status, and Compliance letters. This process is depicted in figure 6-4.

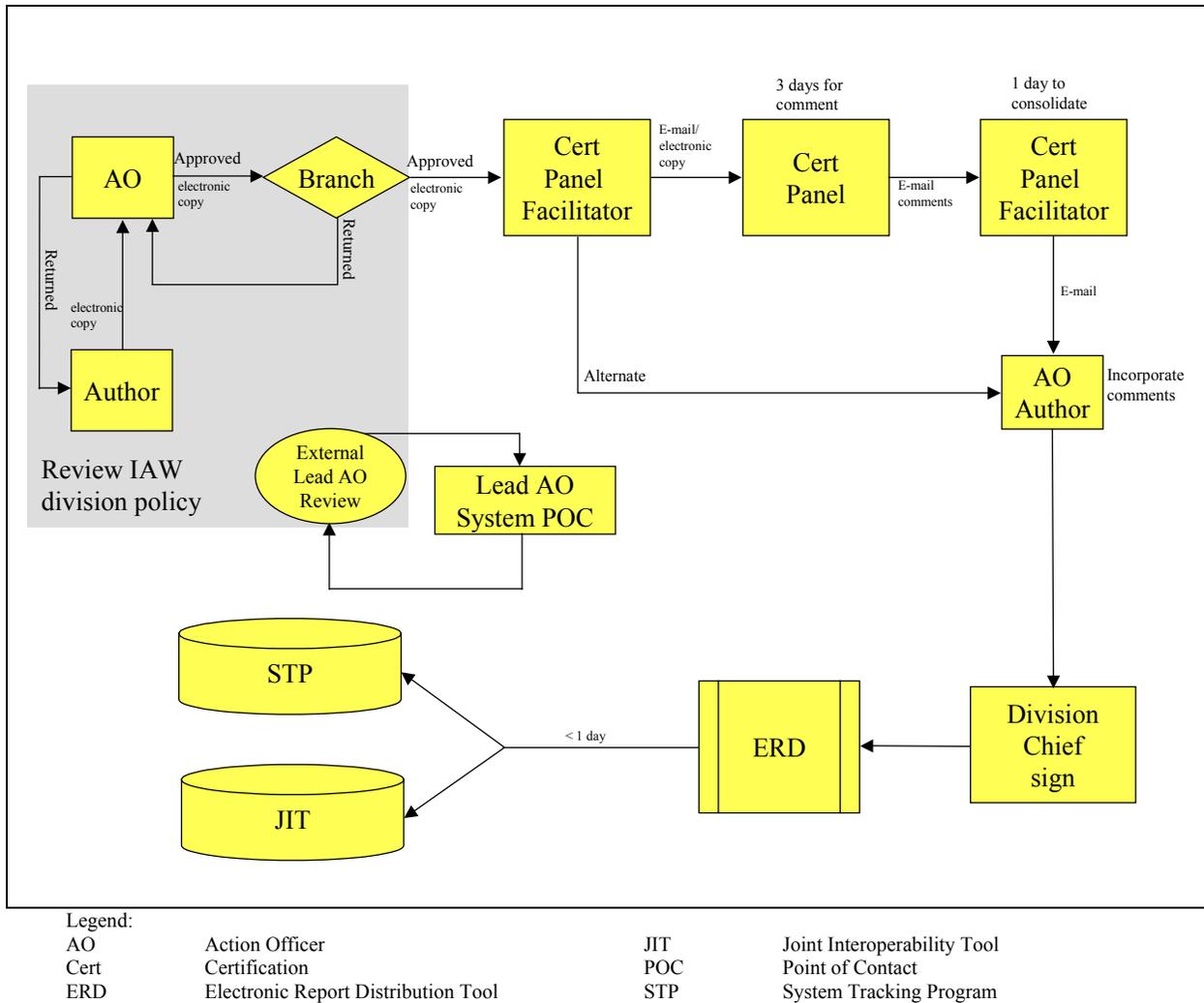


Figure 6-4. Miscellaneous Product Review – No Form 9

6.2.1 This process is much the same as the Interoperability Certification Review, without the Form 9 review portion. Depending on the circumstances, a review by the full Certification Panel may not be necessary; if so, the goal will be to provide any feedback within one 1 working day.

This Page Intentionally Blank

CERTIFICATION MEMORANDA PRODUCTS - FORMAT AND EXAMPLES

1. **Purpose.** This enclosure points to annotated examples of certification related products. This section covers those products involving the Interoperability Key Performance Parameter (I-KPP), as defined by documents produced under 6212.01B, and products associated with [6212.01C](#), including Net Ready KPP (NR-KPP) evaluation. Samples provided include:

1.1 Standards Conformance Certification (Commercial and Military)

- Conformance Certification
- Compliance Letters

1.2 Joint Interoperability Assessment

1.3 Operational Test Readiness Review (OTRR) Interoperability Statement

1.4 Joint Interoperability Test Certifications

- Special Interoperability Test Certification
- Joint System Interoperability Test Certification – Specified Interfaces
- Joint System Interoperability Test Certification

1.5 Administrative - Miscellaneous Letters

2. **Example Products.** The examples provide a basic template and guidance for those portions of products that are fairly stable. Policy/Procedures that are likely to change more frequently (e.g., Form 9 guidance, Joint Staff POCs, core distribution lists) are provided in the JITC Public Outlook Folders. Location of these items is:

[Example products](#) (T: share PLANS and POLICIES TRAINING)

Public Outlook folders:

All Public Folders
#DISA
Organizations
JITC
JITC-FHU
Command Information
Certification Policy

This Page Intentionally Blank

PROGRAM/SYSTEM-SPECIFIC POLICY AND GENERIC TEST METHODOLOGIES POLICY

1. **Purpose.** To identify specific policies that impact JITC Test and Evaluation (T&E) and certifications.

2. **Policies.** JITC T&E and certification must comply with the following special policies.

2.1 **Foreign Systems.** JITC can not issue a Joint System Interoperability Test Certification for foreign systems because these systems' interoperability requirements are not defined by the Joint Capabilities Integration and Development System (JCIDS)/Requirements Generation System (RGS) processes. Using an Interoperability Assessment, JITC can report interoperability testing results for foreign systems whose interoperability requirements are defined. JITC can also report on interoperability of U.S. and foreign systems in combined and coalition environments, when the requirements for interoperability in these environments are defined. There is also an exception in cases where a foreign system is U.S. sponsored and has defined interfaces with U.S. systems. Additionally, JITC can perform standards conformance certification for foreign systems for any standard affecting interoperability. In all cases involving a foreign nation customer, AOs shall coordinate with the Business Management Branch (JTGB) to resolve any funding issues, as there are constraints on how we can deal with foreign entities.

2.2 **Homeland Defense-Related Interoperability.** JITC T&E and interoperability methodologies will treat information exchanges with homeland defense (non-Department of Defense (DOD)) systems as any other external interface for the purposes of evaluating DOD system interoperability. Special policy for evaluating interoperability of homeland defense-related systems themselves has not been established. As with other systems without Joint Staff (JS) J-6 certified requirements, JITC cannot issue an interoperability test certification. However, JITC may produce assessments or standards conformance certifications, as appropriate.

2.3 **Stimulators/Simulators and Training Systems.** Stimulators/simulators and training systems, separate from operational systems, may be used in the development and testing of Information Technology (IT) and National Security Systems (NSS) and to support exercises. These devices may interoperate with other systems in the testing environment. Using these systems in a testing environment does not necessarily mean the test is not adequately operationally realistic. Potential differences between the test environment and the operational environment, and associated risks, must be considered before issuing any interoperability certification.

2.3.1 JITC may certify stimulator/simulator and training systems in the same manner as operational systems. These systems must have JS J-6 certified requirements (Interoperability Key Performance Parameter (I-KPP)/Net Ready KPP (NR-KPP)) for certification. JITC does not certify that these systems provide an accurate model of any particular environment. Certification memoranda should contain wording to the effect: "This is a certification of system conformance to interoperability standards, system interoperability, or system net-readiness. It is not a certification of system performance adequacy as stimulator or simulator in any specific environment or application. (Tailor the wording as appropriate.)" Modeling and Simulation

verification and validation (or similar type testing) techniques should be used to validate the systems.

2.4 Validation of Test Tools and Standards. Test tools (and any associated components such as test suites) and standards/standards profiles should be validated before T&E use. JITC does not have the unique mission to validate test tools or standards. However, we may contribute to the validation as requested by a standards body or perform validation under the authority used to establish a JITC testing program.

2.5 Information Assurance (IA). IT and NSS, including commercial and non-developmental items, must comply with applicable DOD IA policies/regulations and Director Central Intelligence Directives (DCIDs). This includes implementation of public key infrastructure (PKI) when required to ensure information security over all voice, video, and data transmission. Interconnection of systems operating at different classification levels will be accomplished by processes approved by the DOD Chief Information Officer (CIO) in conjunction with Defense Intelligence Agency (DIA) CIO. IA will be an integral part of all net-readiness efforts thus allowing appropriate security measures to protect mission data and system resources from all known threats. The methodology for any T&E and status reporting of IA attributes in System View (SV)-6 architecture views has not been determined. However, JITC shall verify that system and network configurations used in testing are representative of a realistic operational environment, to include IA characteristics of the environment.

2.6 "No Test" Status Letters. Previous JITC policy allowed use of a letter stating that there were no interoperability certification requirements for a system. (These letters were titled "Joint Interoperability Certification Requirements for..." and were based on JITC analysis of joint requirements.) Current DOD interoperability policy ([CJCSI 3170](#)) specifically assigns responsibilities for determining the Joint Potential Designator (JPD) and certifying capability/requirements. Neither of these responsibilities are assigned to JITC, therefore, JITC shall not issue an interoperability "no test" letter.

2.6.1 Issues with interoperability requirements shall be coordinated with the JS J-6 for resolution. JS J-6 certified requirements shall be used to determine the appropriate type and amount of testing required, including the situation where no operational testing is required. There are two situations where JITC testing may not be needed.

2.6.1.1 The JS J-6 capability/requirements certification memorandum may require the Program Manager (PM)/proponent to coordinate with JITC on interoperability testing and certification, even when there are no joint interoperability requirements. In this case, which could be considered an administrative error, JITC may provide the PM/proponent a letter confirming that there are no requirements to test. This shall only be done when the JS has certified the requirements and there is no NR-KPP or I-KPP to evaluate. This shall not be done if there is no JS J-6 certified requirements on which to base the determination, or if there are interoperability requirements, but JITC sees no need, or has no capability to test. (e.g., if the only information exchange is for Global Positioning System (GPS) data, JITC cannot issue a memorandum stating that the requirements do not need testing and certification.) In these situations, the PM/proponent should request a waiver from the interoperability requirements.

2.6.1.2 A new system version having only minor changes not affecting interoperability of the system or interfacing systems, nor otherwise impacting the operational interoperability environment may not require operational testing. JITC will use information provided by the PM/proponent and from other sources to decide if the previous certification still applies to the updated version (i.e., that the interoperability status remains unchanged). Since any system modification has the potential of adversely impacting interoperability, a risk assessment must be performed to determine the chances and consequences of impacts to interoperability. This situation will be documented in an extension of certification letter, as the determination of "no testing required" means that the interoperability status is unchanged from the previous version, in essence extending the previous certification to cover the new release. Another rare case of "no test" required applicable to expired certifications is discussed under extension of certifications.

2.7 Recertification and Extension of Certification. JITC interoperability re-certification is required upon any of the following events.

- When materiel changes (e.g., hardware or software modifications, including firmware) and similar changes to interfacing systems affect interoperability
- Upon revocation of interoperability certifications or JS J-6 system validation
- Upon automatic expiration 3 years after the date of the certification
- When non-materiel changes (i.e., Doctrine, Operations, Training, Logistics, Personnel, or Facilities) occur that may affect interoperability

Other than the case of an expired certification, any of these events will require additional operational interoperability T&E and certification in order to update the interoperability status.

2.7.1 Expired Certifications. If a review of the circumstances for a particular system indicates no change in interoperability characteristics or requirements or JS J-6 system validation since the last certification, a new certification may be issued upon expiration. A new certification is required to reset the 3 year validity period. This "re-issued" certification may not require operational testing. However, requirements certification and JS J-6 system validation status shall be reconfirmed. The status of all interfacing systems must be examined to ensure that their status or requirements with respect to the system under test (SUT) have not changed. The interoperability environment must not have changed, and the previously certified interoperability status should have been verified during exercises or deployments. Only if all of these conditions have been met should a new certification be granted without additional operational testing. An interim ("specified interfaces") certification where only partial requirements were certified because some requirements (critical or not) were not tested or implemented shall not be reissued. The goal is a full system certification of objective requirements.

2.7.2 Certification Extensions ("derived" certification). If a certified system has been modified, but JITC determines that the modifications do not affect interoperability and the interoperability environment and interfacing systems have not changed significantly, the certification may be extended to cover the modified system version. The system PM/proponent should provide a written statement that the modifications do not affect interoperability, along with sufficient information for JITC to independently make a determination of the impact of

changes on interoperability. The extended certification will expire 3 years from the date of the certification being extended (i.e., the extension applies only to the specific system versions being covered, not to the expiration date).

2.8 Revocation and Re-issuance of Certifications. There are situations that may warrant the rescinding, revocation, or re-issuance of a certification. These situations range from the need to correct simple administrative errors (e.g., wrong configuration identified) to serious cases where the JS J-6 fails to validate the interoperability testing and requests the status be reexamined. It is impossible to anticipate all of these situations and the appropriate actions. All such cases shall be brought to the attention of Plans and Policies Branch (P&PB) for resolution. The System Tracking Program ([STP](#)) information shall be adjusted to reflect the correct status. Everyone that received the original Electronic Report Distribution ([ERD](#)) shall be properly notified.

2.9 Standards Conformance Test Methodology. Standards conformance certification results from testing a system/component for conformity with standards/standards profiles (for information processing, content, format, or transfer). Conformity is characterized with a matrix (in the certification summary) showing whether an implementation (the hardware/software under test) meets the individual mandatory and optional requirements specified in the standard/standards profile. Certification is confirmation that the system/component meets - as a minimum - all of the mandatory and implemented optional requirements and that there are no critical discrepancies. Only interoperability test and standards conformance certifications are defined in DOD interoperability policy and procedures. Other types of products may be extremely useful to the PM/proponent; however, they do not satisfy DOD requirements for having to have standards conformance and interoperability certifications.

2.9.1 Standards conformance certification requires two basic components: conformity assessment tools and a conformance program. The conformance program should include a conformance testing methodology and framework (similar to the International Organization for Standardization ([ISO](#))/ International Electrotechnical Commission (IEC) 9646 series). National Institute of Standards and Technology (NIST), European Telecommunications Standards Institute (ETSI), Open Applications Group, and Open Artwork System Interchange Standard (OASIS) are other organizations with standards conformance (conformity) methodologies that provide good standards conformance methodology information. Reference should also be made to [DODD 5101.7](#) and related documents. When a JITC standards testing program does not have a formally defined methodology, ISO/IEC 9646 will be used as the basis for determining appropriate local processes. As a minimum, a standards conformance program will base testing and status reporting on implementation conformance statements and conformance test reports that indicate mandatory and optional protocol elements of the standard/standards profile. All mandatory and implemented optional requirements must be met for an implementation to be considered conformant. Vendor self-certification alone is not adequate for JITC to issue a standards conformance certification.

2.9.2 Standards conformance certification is based on detailed assessment of protocol elements and other specified requirements. Standards conformance certification means that all mandatory items, and all implemented optional items, are correctly supported. If an optional item fails, it must be removed or disabled. Standards conformance certifications should be based on a test

plan that has procedures to test all requirements. A table that shows all requirements (at a level sufficient to show at least the major capabilities supported), what is implemented, and the status. Status must be "rolled up" -- a higher-level item passes only if all subordinate elements pass or are not applicable. Most standards identify mandatory and optional items and don't necessarily identify the criticality. With complex standards there is almost never 100% conformance, so a status of "partially met" or "not met, but minor impact or workaround exists" may be appropriate (in effect factoring in criticality). Too little detail of analysis, less stringent rules for passing, and allowing numerous non-conformance issues are characteristics of assessments that should be documented in something other than a certification of conformance.

2.9.3 Standards compliance (verification, confirmation, validation, etc.) certification. DOD policy does not define a "standards compliance certification." Generally, one conforms to standards and complies with policy. There are few situations where a standards compliance certification would be appropriate. CJCSI 6251.01 requires systems to conform to MIL-STD-188-181, MIL-STD-188-182, and MIL-STD-188-183. Standards conformance certifications are issued for each of the MIL-STD assessments. It is appropriate to issue a standards compliance certification for CJCSI 6251, when all of the individual standards conformance requirements are met, except that a standards compliance certification is not defined in policy/procedures, nor implemented in the STP. Therefore, JITC does not officially issue standards compliance certifications.

2.9.4 Standards compliance letters are used to document standards conformity in situations where a formal standards conformance certification cannot be justified (e.g., analysis not sufficiently detailed and thorough). The term "compliance" is not entirely accurate, however, "compliance" letters lean more towards saying that an implementation complies with the intent of the standard, rather than strictly conforming to each item of the standard. JITC also uses the term "standards compliance" when other organizations issue a related standards conformance certification -- this is more a matter of avoiding the confusion of two "certifications," rather than a reflection of the test methodology, (i.e., some of these products meet the criteria for issuing a standards conformance certification, however, they are not treated as such.) Standards compliance letters must clearly identify what is meant by compliance, either directly or by reference to the testing methodology documentation. Compliance may be verified by a number of techniques, including analysis, inspection, demonstration, and testing, to include use of data from other sources (e.g., from a standards test body).

2.9.5 Characteristics of conformance and compliance testing programs include:

2.9.5.1 Conformance programs will have formal standards/standards profiles, documented testing methodology, validated test suites and tools, and implementation conformance statements and associated reports.

2.9.5.2 Compliance programs may not examine all protocol items and test each one for typical values, boundary conditions (e.g., min/max values or min/max length of data), invalid data (intentional bad data to determine if behavior under error conditions is correct), etc. If testing is more of the nature of sending a message and verifying it shows up on the other end (without

examining the 0s and 1s), then this type of data supports an interoperability assessment or standards compliance letter better than a standards conformance certification.

2.9.5.3 Standards conformance would allow discrepancy reports to be associated with individual protocol elements. If the granularity of test cases does not allow a determination to the level of protocol elements, then testing is probably not sufficient for determining standards conformance.

2.10 Interoperability Evaluation and Certification. Joint System Interoperability Test Certification is the part of the overall interoperability certification process that characterizes operational interoperability capabilities and assesses the operational impact of any discrepancies. Related processes are the JS J-6 requirements and supportability certifications and the JS J-6 Joint System Interoperability Validation. JS J-6 certified capabilities and requirements feed the Joint interoperability test evaluation process, and, in turn, Joint System Interoperability Test Certifications provide input to the JS J-6 Joint System Validation process and the Milestone Decision Authority (MDA) (or equivalent) fielding decision. Policy applicable to all types of interoperability test certifications includes:

2.10.1 Capability/Requirements shall be JS J-6 certified; all exceptions shall be coordinated with JS J-6, including any issues with certified requirements (i.e., "bad" requirements). All issues that require coordination with JS J-6 shall first be coordinated with P&PB.

2.10.1.1 All requirements shall be used for evaluation and the status reported. This includes critical (threshold) and all (critical plus non-critical -- objective) requirements. If requirements for increments were not clearly delineated by increment (phase, spiral, block, etc.), as mandated by DOD policy, all requirements shall be evaluated. Changing the increment or criticality of a requirement is a modification to the requirements that requires JS J-6 certification.

2.10.1.2 All external (top-level) information exchanges shall be evaluated, whether inter- or intra-DOD component (see [CJCSI 6212.01](#)).

2.10.1.3 Any other system interoperability requirements shall be evaluated. (e.g., some interoperability requirements do not appear in the integrated architecture products, such as a capability to communicate on two channels simultaneously.)

2.10.1.4 Standards conformance requirements, as documented in TV-1 products, or derived from other requirements and specifications, shall be evaluated and reported as appropriate for the complexity and maturity of the protocols.

2.10.2 Interoperability evaluation will be based on end-to-end testing of production representative systems in as realistic operational environment as practicable. This includes use of test scenarios with a typical message mix, loading that reflects normal and wartime modes, and benign and hostile environments.

2.10.3 Interoperability evaluation must assess the end-to-end exchange and operational use of information among systems. For the exchange to be assessed as meeting all requirements, the technical exchange and operational use must be confirmed, including associated attributes for

accuracy, completeness, timing, security, etc. Meeting the requirements means that not only the SUT functions correctly, but that the interfacing systems also performed as required, and that the network infrastructure also provides the necessary reliability, bandwidth, response times, security, etc.

2.10.4 Version identification information shall be provided for the SUT, interfacing systems, and net-centric components.

2.10.5 Status reporting on items shall include the criticality associated with the item, the status (e.g., certified, not tested), the degree of compliance (e.g., all critical requirements met, all requirements met), and the expected operational impact of any discrepancies. Expected operational impact includes the effects on the SUT, interfacing systems, and interoperability environment (e.g., net-centric services).

2.10.6 The interoperability certification memorandum shall include a statement on any conformance certification requirements, whether conformance has been conducted as a separate test or included in the interoperability testing.

2.10.7 Testing limitations shall be reported, including the impact they may have on interpretation of the results and conclusions. Any untested requirements shall be included in the testing limitations.

2.10.8 Life cycle interoperability evaluation will continue until objective requirements have been satisfied and certified, and then will continue as needed to satisfy re-certification needs.

2.10.9 Certification status will be verified during exercises and deployments throughout the life cycle. If indications warrant (e.g., serious interoperability problems are observed or reported, requirements or operational environment appear to have changed, configuration has changed significantly) interoperability assessments or complete evaluations will be performed to confirm and update the status, as necessary. Existing certifications will be revoked and non-certification and interoperability status memoranda issued as appropriate.

2.11 Interoperability Key Performance Parameter (I-KPP) Based Interoperability Test Certifications. Interoperability evaluation and status reporting for systems documented under the RGS system shall follow the following guidance.

2.11.1 Requirements shall be obtained from a JS J-6 certified ORD or certified I-KPP package. Some ORDs approved or directed by the JROC before JCIDS may still be valid. However, JROC approved ORDs, ORDs approved before 2001, and ORDs without an I-KPP statement require coordination with P&PB before use; coordination with JS J-6 may also be required.

2.11.2 The certification must address whether the I-KPP and individual top-level Information Exchange Requirements (IERs) and overall system interoperability performance have been met. The status of physical/logical interfaces is also reported.

2.12 Net Ready Key Performance Parameter (NR-KPP) Based Interoperability Test Certifications. For systems/programs subject to NR-KPP processes, the evaluation will determine the operational information interoperability status of the NR-KPP requirements (including interfaces, external (top-level) exchange requirements and other system interoperability requirements). Guidance specific to the NR-KPP process includes:

2.12.1 Requirements shall be obtained from a JS J-6 certified NR-KPP contained in a Capability Production Document (CPD) - alternatively an Information Support Plan (ISP) if a CPD is not required. If there is both a CPD and ISP with different requirements (or different JS J-6 certification status), JS J-6 must be consulted to resolve the issue. When the JS J-6 has granted a waiver for the NR-KPP requirement, an alternate JS J-6 approved source of interoperability requirements information will be specified by JS J-6. This alternate source shall then be used for JITC interoperability evaluation.

2.12.2 The certification must address the NR-KPP statement, with the four primary elements of the NR-KPP and associated performance attributes, and provide the status of standards conformance. (Note that the elements are not mutually exclusive – there is considerable overlap and interplay of the requirements of the pillars of the NR-KPP.)

- Net-Centric Operations and Warfare (NCOW) (dynamic) compliance (net-readiness: net-centric enterprise compatibility and interoperability).
- Information Exchange, including both the technical exchange and end-to-end operational effectiveness of the exchange.
- Key Interface Profiles (KIPs) compliance.
- Information Assurance.

2.12.3 As noted, in addition to reporting on the NR-KPP elements, standards conformance shall be reported separately where appropriate. A summary of the status reporting for these items follows.

2.12.3.1 NCOW (GIG [Global Information Grid] Enterprise Services (GIG ES (GES)) compliance (net-readiness). The NR-KPP statement includes: interfaces, services, policy-enforcement controls, and data correctness, availability, and data processing at the enterprise level and Joint Integrated Architecture. (Net-centric characteristics of the NCOW RM.) The static component of this element of the NR-KPP assesses compliance with the DODAF, NCOW RM, DISR (JTA), etc. Interoperability evaluation of this element involves dynamic testing that complement the static analysis. For example, standards conformance testing is the dynamic analog of the static DISR (JTA) compliance. JITC's evaluation of this element comprises compliance with GES that comprises Core Enterprise Services (CES) and Community of Interest (COI) services.

2.12.3.1.1 Initially CES will be compatibility and interoperability with Net-Centric Enterprise Services (NCES), eventually evolving to the objective GES. This aspect of net-readiness includes conformance to standards (of all types, including data as well as transmission protocols) and interoperability with core GES (NCES) services.

2.12.3.1.2 COI services includes static domain services (e.g., business, warfighter), and static COIs (e.g., DOD, IC). Eventually dynamic ("expedient") COI capabilities will be supported. Multiple COIs may be required for a system to achieve full functionality. The basic characteristics are identified in the *DOD Net-Centric Data Management Strategy*. Characteristics of GES related to evaluation include:

- JROC approved GIG CRD establishes need for capabilities; GIG Arch V2 defines the information environment for capabilities.
- Spiral development -- increments implemented as GES progresses. [Should examine capability strategy with capabilities and timeframe.]
- Transport is provided by GIG transport (DISN and tactical nets) -- i.e., transport is not specified as part of GES.
- Paradigm is TPPU (task, post, process, use) vs. old TPED (task, process, exploit, disseminate). A given system may be a provider or consumer of services, or both, and for the entire enterprise or a subset.

GES issues and challenges include:

- Telecommunications and network transport capability/requirements not currently defined with DODAF products, (e.g., voice switches are defined in GSCR.)
- Environment and enterprise management may have to be evaluated if they directly affect the SUT.
- Incremental development will require continuous evaluation of GES compliant systems.
- Changes will generally be asynchronous with SUT milestones.
- Services judged by availability, perceived reliability, ease of use, and speed; consumer feedback is essential.
- Different networks may have different core services (e.g., security requirements for SIPRNet and NIPRNet).
- There will be parallel operations of new/old paradigms during the transition (some systems will have to support both paradigms until a critical mass of net-centricity is available).

2.12.3.2 Information Exchange. This includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange. Exchange status is reported by physical/logical interface (SUT to system end nodes, as defined in architecture products), and external (top-level) exchange requirements. Interface status will include an identification of any KIPs associated with the interface and its compliance status. In addition to integrated architecture products, interface information is also available in the Levels of Information System Interoperability (LISI) profile (Interface Requirements Profile -- Interoperability and Interconnectivity Capability (IIC) Profile) and the ISP, including any interface control agreements (ICAs).

2.12.3.3 Key Interface Profiles (KIPs) are operational, systems, and technical specifications of key GIG interfaces. The 17 categories of KIPs comprise a wide range of interface specifications,

from complete interface requirements to merely protocol specifications for part of an interface. The KIP Implementation Statement includes additional information on the system compliancy requirements to the KIPs (i.e., not all systems may be required to implement 100% of a KIP specification). KIPs compliance will be reported in a separate table to clarify the overall KIPs compliance status, and will also be included in the reporting of other elements where appropriate (e.g., in the interface requirements matrix, where one or more KIPs may apply to an interface). KIPs compliance must be reported in sufficient detail to indicate the degree of compliance (for those cases where 100% compliance is not required), and the method of determining the compliance status (e.g., standards conformance testing, derived (from other formal testing), demonstrated). Any discrepancies must be assessed for expected operational impact.

2.12.3.4 Information Assurance (IA) is an integral part of net-readiness, and the NR-KPP describes how the system will implement IA policies and procedures. JITC will evaluate IA (or portions of IA requirements) when requested, and will report any known IA status as part of reporting the NR-KPP status. Usually, however, some portions of IA requirements (e.g., DITSCAP) may not be assessed until after JITC interoperability certification, and cannot be reported in the certification. IA requirements and attributes occur at various levels and cross all elements of the NR-KPP. Besides DITSCAP requirements, each information exchange includes IA attributes, which in turn can be rolled up to derive IA requirements for physical/logical interfaces. If public key infrastructure (PKI) technology is required, there may be a separate statement that PKI technology will be acquired as part of this effort, and PKI interfaces may also be specified as a KIP requirement.

2.12.4 Standards conformance requirements also appear throughout the NR-KPP, however, like KIPs, the status will be reported in a separate table and also be included in the reporting of other elements where appropriate (e.g., in the interface requirements matrix). With the net-centric paradigm, standards will play a critical role, therefore a thorough, consistent methodology must be applied when testing and certifying standards conformance. The system standards profile is documented in the TV-1, created with the help of the Levels of Information System Interoperability (DISR) online tool. Other standards requirements may be defined in LISI IIC profiles, KIPs derived from requirements documents (and other KIPs), etc.

2.13 JITC Certification Determination

2.13.1 Interoperability Test Certification. Interoperability test and evaluation quantifies to the Warfighter the degree to which a system will interoperate in relation to its overall joint, combined, and coalition interoperability requirements. The interoperability status also conveys the level of risk associated with the system meeting interoperability requirements by identifying the expected operational impact of any discrepancies. Status reporting is dependent on the form of requirements (e.g., I-KPP statements qualitatively differ from NR-KPP statements), and more specific advice is provided in the annotated product examples when appropriate. Following is general guidance to be used when determining the overall system interoperability and external exchange status.

2.13.1.1 JITC bases interoperability evaluations on JS J-6 certified requirements, the criticality of the requirements, and the expected operational impact of any deficiencies. An interoperability

status is determined for the overall system, if all critical interfaces have been implemented and tested. Interfaces (external information exchanges between systems) are assessed individually and contribute to the overall system status. Compatibility, including conformance to standards and standards profiles, interoperability, supportability, IA issues, etc. should be considered when providing interface and system certification status. The overall status must also take into consideration the cumulative effect of any discrepancies, including any technical impacts.

2.13.1.2 Interoperability certification letters are issued for systems and, whenever possible, provide the overall system interoperability status with respect to all of the required interfaces and other system interoperability requirements. System certification is confirmation that the system is interoperable and is ready for use in a joint/combined/coalition operational environment. Certification letters include the interoperability status of each external interface; however, the focus is on the overall system requirements, not merely what was available for testing. If critical interfaces are untested, a "specified interfaces" certification is used, assuming other tested requirements are met. If there are critical interoperability requirements that are not met, or the cumulative effect of problems may be expected to cause major operational problems (i.e., the system should not be fielded), the system is not certified.

2.13.1.2.1 The possible interoperability conditions for a system include:

- Interoperability Test Certification
- Interoperability Test Certification, Specified Interfaces
- Interoperability Test Non-Certification
- Interim Certificate To Operate (ICTO; issued by the ITP)
- "No Test" Requirements (see above on "No Test" letters)
- Other (legacy certification, untested/unknown)

2.13.1.2.2 JITC issues the first three types of certifications (that include "Joint" and "Special" categories), and performs analyses to confirm cases with no interoperability test certification requirements. It is important to distinguish between the JITC test certifications and certifications by other organizations (e.g., interoperability capability/requirements, supportability of ISPs).

2.14 Interface Certification

2.14.1 Interfaces are certified only as part of a system certification. There is no process for certifying individual interfaces. Interfaces are usually derived from top-level, external Information Exchange Requirements (IERs) or equivalent exchanges. The interface status is determined by the results of interoperability tests and other relevant information. Additional input may include the results of any previous interoperability testing, standards conformance testing, compliance with standards profiles, and results of interoperability capability/requirements and supportability certification efforts. Other performance parameters and interoperability issues and technical impacts may factor into the evaluation as well. Not all interfacing systems may participate in any one test or interoperability demonstration, so it is important to identify the specific configurations used for the certification.

2.14.2 Interfaces that meet all critical requirements and do not cause any major operational impacts will be certified. Remarks for each interface shall note any expected operational impacts – i.e., the degree or extent to which it is interoperable (see below). Requirements matrices must list all required (not merely tested) interfaces and provide an explanation for interfaces that are not implemented or tested; any plans to complete or test interfaces will be described. Valid status entries for interface requirements are:

- Certified
- Not Certified
- Not Tested

2.15 System Certification

2.15.1 Certification letters are issued for systems, which may have one or more interface requirements. Interfaces may be derived from, or specified in terms of, IERs, KIPs, etc., although the Operational Requirements Document (ORD), CPD, or ISP may contain a textual/tabular list and should contain a graphical representation of external interfaces in the architecture products. There may be additional interoperability related requirements (e.g., IA issues) that must be factored into the interoperability status. If only some of the interfaces are tested, the certification will still provide the status for all of the interfaces that have been tested to date. If there is insufficient data to establish a system certification status (i.e., there are untested or unimplemented critical interfaces), the letter shall indicate that the overall system is not certified, and will describe why an overall status cannot be determined at this time. This "specified interfaces" certification will certify those interfaces for which adequate data is available and the criteria are met.

2.15.2 An overall system interoperability status will be assigned to the system based on the criticality of requirements and the expected operational impact of all identified interoperability problems. The system status shall take into account the criticality and interoperability status of each interface, any overall system interoperability performance criteria, as well as any combined effects that may not have affected individual interfaces but may affect the system as a whole. The degree of system interoperability is expressed textually (see below). Future interface requirements are not used to determine the current interoperability test certification of the system, although future requirements should be listed in the matrix when known, and all current requirements must be addressed, not merely those tested or implemented.

2.15.3 Both interface and the overall system interoperability status must include remarks indicating the degree of interoperability and the severity of any expected operational impacts. A rationale must be provided which describes the reasoning behind assigning the interface and overall status. Results must be presented in terms of overall system interoperability, external system interfaces, and interoperability KPPs, IERs, KIPs, and other specified interoperability requirements, as applicable.

2.15.4 CJCSI 6212.01 requires testing in an operationally realistic environment. If the test environment differs significantly from the mission and threat operational environment, or results may be sensitive to the specific hardware/software platforms or networks used for testing, the

certification should be qualified to reflect this increased risk. The certification letter should state that the results are valid for a specific environment, and system interoperability should be verified before being deployed in a different environment. Certain testing limitations may also warrant qualifying the certification. For example, if testing was limited to a benign environment (e.g., clean networks, no information warfare activities), this should be mentioned.

2.15.5 System certification letters are normally issued after completion of an interoperability evaluation, and must reference any existing certifications still in effect. In some situations, it may be appropriate to issue, update, or revoke a certification for interfacing systems (i.e., those other systems interfacing with the primary system under test). Information from any of the sources used to evaluate interoperability may trigger a review, reevaluation, and certification of a system. Results from field, exercise, and demonstration support should be examined for any required changes to certifications.

2.16 Interoperability Status Determination

2.16.1 The following certification definitions should be used as a guideline for the terms used to describe various degrees of interoperability. Certification is based on JS J-6 certified capability/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 implemented and tested. Interoperability status represents the extent to which a system is interoperable with respect to interoperability KPPs, IERs, KIPs, standards conformance, and other stated interoperability requirements.

2.16.2 Critical requirements with deficiencies that may result in major operational impacts are grounds for assigning an interoperability status of "not certified." Non-certification may also result because of the cumulative effect of less severe problems or failed non-critical requirements. Because of the complex interrelationship of the factors determining interoperability, atypical situations must be handled on a case-by-case basis. If there are critical interfaces that are "not certified," the overall system status must be non-certified – either a "specified interfaces" or "non-certification" shall be used in this circumstance. If not all critical requirements are met and the system does not negatively impact the interoperability environment (e.g., degrade other systems) and does provide valuable capabilities, a specified interface certification may be most appropriate.

2.16.3 Interface and system interoperability status are an indication whether interoperability requirements are met and systems are interoperable. It is not necessarily an indication that the system being certified does or does not contain any faults. Although it is desirable to be able to isolate faults to a particular component, the interoperability status should reflect whether the system/interface works. In other words, the status is independent of whether faults exist in the system under test, an interfacing system, or the supporting communications infrastructure.

2.16.4 JITC categorizes the degree of interoperability of systems and system interfaces based on the possible operational impact of any interoperability deficiencies. AOs must work closely with the user community to assess the expected operational impact of discrepancies, providing appropriate input so any technical impacts are factored into the assessment. The operational

impact is key to determining whether or not to certify an interface or system. The tables below show the conditions which lead to a given status determination and the terminology used to describe the various degrees of interoperability.

Table 8-1. Guidelines for Determining Interoperability Status

Requirements Met	Operational Impact	Risk/Adverse Effects	Description (see table 8.2)	Status
All – all KPP requirements, IERs, and other IOP req's.	None	Low/None. No adverse effects to mission.	1	Certified
Some – all critical (threshold) KPP req's, IERs, other IOP req's.	Minor	Low. No adverse effects to mission.	2	Certified
Some – all critical (threshold) KPP req's, IERs, other IOP req's.	Moderate	Medium. Adversely affects operational or mission essential capability, or technical or life cycle support risk, but mitigating circumstances minimize the impact.	3	Certified
Fails some critical requirements.	Major	High. Adversely affects operational or mission essential capability, or technical or life cycle support risk.	4	Not Certified
Few or no requirements met.	Critical	Unacceptable. Prevents the accomplishment of an operational or mission essential capability, or jeopardizes safety or security.	5	Not Certified
Unknown – Not tested		Depends on criticality and operational impact.	6	Not Tested
Not implemented.		Depends on criticality and operational impact.	7	Not Certified

Table 8-2. Interoperability Status Descriptions

No. (from table 8.1)	Description
1	The system/interface meets all interoperability requirements (both threshold and objective) for a given increment.
2	The system/interface meets all critical interoperability requirements. No deficiencies have more than a minor operational impact with no adverse effect on capabilities essential for mission accomplishment. All critical system interoperability KPPs/interface IERs are met.
3	The system/interface meets some interoperability requirements. No deficiencies have more than a moderate operational impact that may involve delays, degradation, or work-arounds, but are unlikely to lead to critical mission failures. All critical system interoperability KPPs/interface IERs are met.
4	The system/interface does not meet some critical interoperability requirements. Deficiencies may have major operational impacts with adverse effects on mission essential capabilities that lead to critical mission failures.
5	The system/interface does not meet critical interoperability requirements. Deficiencies prevent the accomplishment of critical mission capability, or present a risk to safety or security.
6	The ability to meet interoperability requirements cannot be demonstrated, and any operational impacts are usually unknown. It is only rarely possible to assess an operational impact (e.g., where some negative results exist, but insufficient results to fully evaluate the interoperability).
7	An interface capability is not implemented (either in the SUT or interfacing system); therefore, it fails to meet requirements and is "not certified."

This Page Intentionally Blank

REQUIREMENTS DOCUMENTS REVIEW PROCESS

1. **General.** The cornerstone of any certification effort is testable and measurable requirements. The Joint Staff (JS) attempts to ensure requirements are adequate by mandating that these capability/requirements documents be JS J-6 certified. JITC acts as one of the assessors during this review/certification process. The process is described in CJCSI [3170.01](#), CJCSM [3170.01](#), and CJCSI [6212.01](#). This enclosure elaborates on the associated JITC processes.

2. **Overview.** JITC becomes involved with the Joint Capabilities Integration and Development System (JCIDS) process when the program sponsor submits a JCIDS document to the J-8 Knowledge Management/Decision Support (KM/DS) tool. The Gatekeeper will then determine how the capability affects the Joint Force and assign the document a Joint Potential Designator (JPD). This JPD will determine how the document will be reviewed and certified. The Action Officer (AO) can find additional information on this subject in CJCSM [3170.01](#).

3. **Initial Action.** The JITC review process begins when there is a document staffed for review, and Joint C4I [Command, Control, Communications, Computers, and Intelligence] Program Assessment Tool – Empowered (JCPAT-E) personnel send an e-mail notification to the assessors, including JITC for most documents. The Plans and Policies Branch (P&PB) will download the document from the JCPAT-E site on the SECRET Internet Protocol Router Network (SIPRNet) terminal and provide it to the JITC Technical Library. P&PB will assign the document to a lead division and appropriate support divisions for review. The lead division will be responsible to review and comment on the document. The responsible AOs can obtain the document from the technical library (hardcopy), online image files with the TechLib32 tool, or the JCPAT-E tool on the SIPRNet. Since the Indian Head location does not have ready access to the JITC Technical Library, the office manager or AO will download the document for review.

3.1 Some documents have slight differences in handling procedures. While the DOD is transitioning from the Requirements Generation System (RGS) to the JCIDS, JITC will still be reviewing Command, Control, Communications, Computer, and Intelligence Support Plans (C4ISP) and updated Operational Requirements Documents (ORDs). JCIDS replaces the C4ISP with the Information Support Plan (ISP) as part of the JS J-6 interoperability capability/requirements certification process. P&PB can download C4ISPs and ISPs (and sometimes the final version of requirements documents, such as the ORD) from a C4ISP JCPAT-E tool. When available, unclassified documents are placed on Groups on the CDXFHU1 server ("T: Drive") in the "[C4ISP](#)" directory. The AO will access these unclassified documents from the JITC network drive or obtain their own read-only access to the DISA JCPAT-E tools. Classified documents will be available at the JITC Technical Library, or the AO can download them from the SIPRNet JCPAT-E tool. JITC is also responsible for reviewing the Combatant Commander Command and Control Initiatives Program (C2IP) submissions, Test and Evaluation Master Plans (TEMPs), and other related acquisition and requirements types of documents. The C2IP process is outside the scope of this instruction, but special tools and procedures are on the JITC Intranet ([JITCnet](#)) ([C2IP Review link](#)).

4. **Action Officer Review.** AOs will usually have several days, or even weeks, to review a document. However, the time allotted for review is limited, so the review should be initiated

immediately. The AO should use the appropriate review [checklist](#) and must return comments in the appropriate assessor's comment matrix. (Checklists, comment matrices, and other related JCPAT-E review material are also on the T: drive (under the Plans and Policies folder) in the "[JCPAT Document Review](#)" directory. CJCSI [6212.01](#) contains the original source for the checklists, procedures for assessing documents, and includes definitions of the comment categories (i.e., critical, substantive, administrative).) AOs should observe the following:

4.1 JITC is responsible for validating interoperability requirements of the Capstone Requirements Document (CRD), Initial Capabilities Document (ICD), Capability Development Document (CDD), and Capability Production Document (CPD).

4.2 Ensure the Net Ready Key Performance Parameter (NR-KPP) is fully defined, to include the required integrated architecture products.

4.3 Ensure the CDD and CPD are compliant with any applicable CRDs.

4.4 Thoroughly review the document, even if the document is in preliminary draft (Stage I), and even if not the lead AO.

4.5 Ensure the requirements are testable and measurable. Ensure timeliness, accuracy, correctness, and criticality information is provided.

4.6 Ensure the document complies with applicable guidance.

4.7 For Stage II documents, review the entire document and ensure that previous JITC and other organizations' valid comments were satisfactorily incorporated.

4.8 Provide critical comments (i.e., non-concur) during Stage II review, if it is warranted. Stage II review is the last chance to ensure that JITC will have valid requirements for testing. The AO should coordinate critical comments with the document proponent/author before submitting them.

4.9 Always use the latest criteria checklist to conduct the review. These checklists are not all inclusive, merely general guidelines, and the AO is responsible for ensuring that documents comply with applicable interoperability policy and provide sufficient information to perform an adequate interoperability evaluation, including any necessary standards conformance evaluation.

4.10 Comments must be submitted in a timely manner and follow the required format and instructions. When filling out the comment matrix, the reviewer should enter the Government AO's information, even if a support contractor conducts the review. The lead AO is responsible for rolling up any comments from support divisions, resolving any issues if conflicts exist, and updating STP information, as needed. The lead AO must also coordinate the review as follows:

4.10.1 Send an e-mail to the applicable support divisions (identified on the tasking e-mail) and the Office Managers (OMs) notifying them who the lead AO is.

4.10.2 Set a corresponding suspense date to get the comments from the support divisions in time for consolidation and to resolve any conflicts. Negative replies are requested.

4.10.3 Request the support divisions send back the name of the reviewer for that division.

4.10.4 Coordinate with the support divisions on the lead AO suspense date, if no comments have been received by the due date.

4.10.5 Indicate on the e-mail submitting comments to P&PB that all support divisions' comments have been incorporate.

4.10.6 Confirm with the support division whether they plan to submit any comments on the document.

4.11 Documents are assigned to JITC for technical review and not administrative comments. A concur without comments, or only admin comments, should be made only after a thoroughly adequate review is performed.

5. **Submitting Actions.** The lead AO/OM shall submit (via e-mail to "[JITC Doc Review](#)") the division approved unclassified comment matrix and related information to P&PB before the JITC suspense date. P&PB will upload the AO's comment matrix to the JCPAT-E, and post the recommendation, completing the tasking. Classified comments will be provided and coordinated in an appropriate manner for the classification level. Information provided to P&PB shall include the following, as a minimum:

5.1 Lead Division Recommendation: Concur, Concur with Comments, Non-Concur

5.2 Reviewer(s): <office symbol>/AOs names

5.3 Lead Division Chief concurrence: name of approving official

5.4 Notes: [E.g., STP entry has been made/updated; document sponsor contacted for non-concur.]

6. **Applying for Joint C4I Program Assessment Tool - Empowered (JCPAT-E) access.** JCPAT-E is the JS J-6 tool used to access documents submitted to the JCIDS system. In order to obtain these documents from the system, the AO must first apply for access.

6.1 Since the JCPAT-E resides on the SIPRNet, the AO will first need to have that access. The AO must complete a DD Form 2875. This form, to include completion instructions, is located in Formclient. After gaining SIPRNet access, the AO should navigate to the JCPAT-E site and follow the instructions to obtain access. (<http://jcpat.ncr.disa.smil.mil>)

6.2 After completing the access request to the SIPRNet site, the AO can apply for access to the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) site. This site will allow

access to unclassified C4ISPs and ISPs. Access the site at the following URL: <http://jcpat.ncr.disa.mil> and select "request account" and follow the online instructions.

7. Searching JCPAT-E for certified/Stage III documents. The AO can use the following procedures for searching the JCPAT-E. (Further details are on the [T: drive](#).)

7.1 Access the SIPRNet and go to the JCPAT-E homepage (<http://jcpat.ncr.disa.smil.mil>).

7.2 Once on the homepage, select the J-6 Assessment Tool.

7.3 Select Assessor/Reviewer access.

7.4 Enter user name and password; these items are case sensitive.

7.5 The tool will present the default search option. The AO can search this screen for any documents in active review.

7.6 To obtain a listing of all certified documents, select CERTIFIED item located on the left hand menu.

7.7 To obtain a listing of all Stage III certified documents, select STAGE III item located on the left hand menu.

7.8 To search for a specific certified document type or system requirements document, select search located at the upper right and then enter the search criteria. Select FUZZY SEARCH, and then select SEARCH.

7.9 To search for any requirements document, select the J-6 Search tool on the left side menu. Enter the search criteria and select SEARCH.

7.10 To print a document, select PRINT from the menu. After the printing is complete, the AO will need to complete the security review process. First, stamp each page with the applicable classification on the top and bottom of each page. Then, stamp the date on the lower right of each page. Finally, present the entire print run to a Derivative Classification Review Agent (DCRA) for review and signature.

TEST PLANS AND TEST REPORTS - GUIDE TO CONTENT AND FORMAT

1. **Purpose.** This enclosure points to the JITC Guide to Plans and Reports. JITC Policy for overall test documentation is contained in JITC Instruction [210-85-01](#), Documentation of Test and Evaluation Activities. This instruction applies to all test plans and reports, including those for interoperability testing. The instruction directs writers to use the [JITC Guide to Plans and Reports](#) for content and format of these documents.
2. **Document Development Tool Kit.** The JITC Guide to Plans and Reports and the JITC documentation instruction can be found on the JITCnet under the Doc Development Tool Kit menu choice or accessed by clicking on the hyperlink below.

[DOC DEVELOPMENT TOOL KIT](#)

This Page Intentionally Blank

SYSTEM TRACKING PROGRAM (STP)

1. **General.** The JITC's System Tracking Program ([STP](#)) is an on-line database that tracks systems' progress toward joint interoperability certification. STP monitors the complete life cycle of Information Technology (IT) and National Security Systems (NSS) from capability/requirements document status, to Interim Certificate to Operate (ICTO), through test and evaluation, and culminating with joint interoperability certification status.

2. **Applying for an Account.** STP is available on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and SECRET Internet Protocol Router Network (SIPRNet). Instructions for requesting access are provided below.

2.1 NIPRNet Instructions:

2.1.1 Access the NIPRNet and go to the STP homepage <https://stp.fhu.disa.mil>.

2.1.1.1 Click "Apply for STP User Account"

2.1.1.2 Complete the on-line form

2.1.1.3 Click "Submit Request"

2.1.1.4 A username and temporary password will be e-mailed within two workdays. STP NIPRNet is available to .MIL or .GOV domain users only. Contractors applying for STP access must have a government sponsor and a need to know.

2.2 SIPRNet Instructions:

2.2.1 Access the SIPRNet and go to the STP homepage <http://stp.fhu.disa.smil.mil>. STP SIPRNet does not require a user account (i.e., username and password). Access to the STP SIPRNet is open to all cleared personnel with access to a SIPRNet workstation.

3. **Information in the System Tracking Program.** Information is JITC's final product, and it needs to be readily available to our Action Officers (AOs) and customers. STP provides a single repository of unclassified information to determine a system's interoperability certification status, such as:

- Capability/requirements document status
- ICTO status
- System certification results
- Interface certification results
- Certifications, assessments, test reports, and other evaluation results

4. Source of System Tracking Program Information.

4.1 The majority of the system information is obtained from the following sources:

4.1.1 Joint C4I [Command, Control, Communications, Computers, and Intelligence] Program Assessment Tool – Empowered (JCPAT-E) - System capability/requirements document information

4.1.2 United States Military Communications-Electronics Board (MCEB) Interoperability Test Panel (ITP) – ICTOs

4.1.3 Office of the Secretary of Defense (OSD), Director, Operational Test and Evaluation (DOT&E) - Test and Evaluation Oversight List

4.1.4 Major Defense Acquisition Program (MDAP) List

4.1.5 JITC AOs

5. Primary Users.

5.1 JITC AOs, Contractors, and Management

5.2 Warfighters

5.3 Joint Staff (JS)

5.4 Program Managers (PM)

5.5 Combatant Commanders

5.6 Acquisition Executives

6. Responsibilities.

6.1 JITC AO:

6.1.1 Create and maintain system information when assigned as the JITC System POC, to include the fields listed below. AOs are responsible for maintaining the accuracy of their system entries; however, they may create/modify their Form 1 to request contractor support to enter/maintain system entries.

- Program Name
- Previous Program Name
- System Name
- Previous System Name

- Nomenclature
- Test/Activity Information
- System Point of Contact (POC) Information
- Mission Area(s)
- Acquisition Category (ACAT)
- CC/S/A (Combatant Command/Service/Agency)
- System Description
- JITC Division/Branch POCs
- JITC Comments
- Interoperability Comments
- Initial Source of information on the system
- Interface Information, i.e., Name, Software Version, Criticality

Note: This information must match the interoperability matrix depicted in the final system interoperability test certification letter.

6.1.2 Identify STP requirements/enhancements using any of following methods:

6.1.2.1 Discrepancy Change Forms (DCF) on DCFWin – Use the path:
Start/DISANet/DISANet Site Applications/MSSG Applications/DCFWin

6.1.2.2 STP Feedback – Click "Feedback" in STP

6.1.2.3 STP e-mail - JITC STP Support jitcstp@fhu.disa.mil

6.1.3 Attend STP Users' Group meetings to discuss STP requirements

6.1.4 Attend STP training classes

6.2 Plans and Policies Branch (P&PB):

6.2.1 Verify that the system entry (including interface information) is correct. STP entries must be correct before P&PB provides Electronic Report Distribution (ERD) technical and administrative release approval.

6.2.2 Enter capability/requirements document status obtained from the JCPAT-E.

6.2.3 Enter certification information, e.g., certification date/status, interface status/comments. P&PB will obtain this information from the certification letter distributed through the ERD.

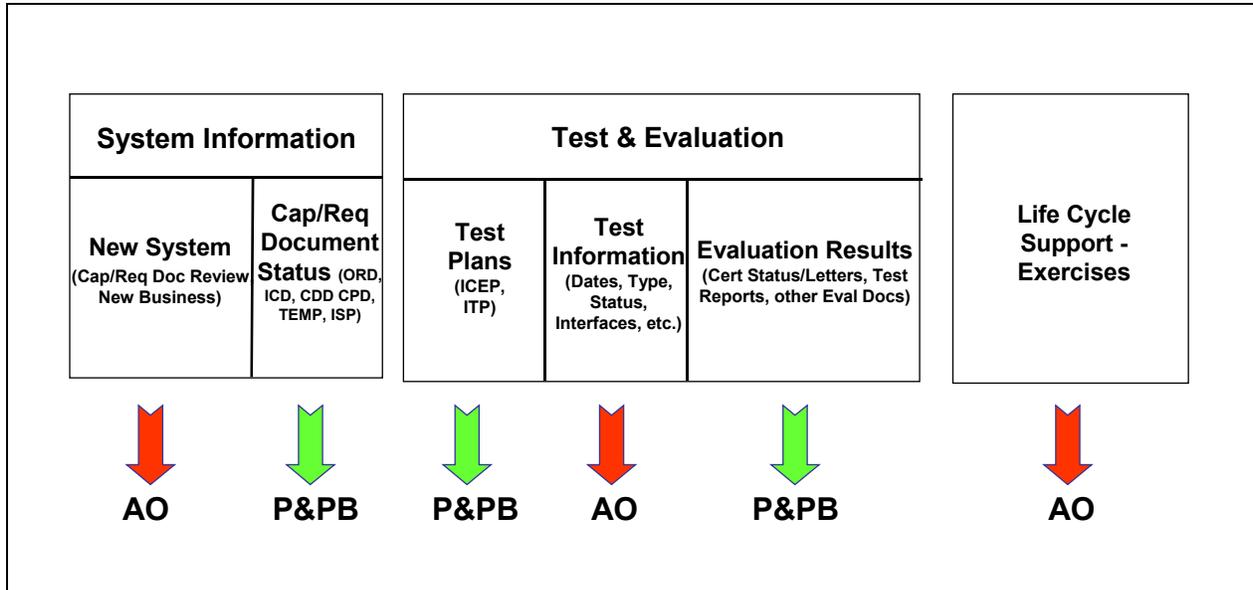
6.2.4 Ensure that STP database is updated with all documentation distributed through the ERD, to include test plans, test reports, certification letters, assessment letters, and other evaluation documents. All documents must be distributed through the ERD before they entered into STP.

6.2.5 Chair the STP Users' Group meeting.

- 6.2.6 Enter/maintain OSD Test and Evaluation List in STP.
- 6.3 Automated Systems and Test Support Division (AS&TSD):
 - 6.3.1 Manage STP Support and Data Entry Task.
 - 6.3.2 Review/approve STP access requests.
 - 6.3.3 Approve the combining and deleting of systems.
 - 6.3.4 Develop training material and provide STP training to the workforce.
 - 6.3.5 Provide STP briefings/demonstrations to visitors.
 - 6.3.6 Validate data entered into STP and send e-mails reminding Action Officers to enter/update system information.
 - 6.3.7 Serve as central point of contact for Action Officers and customers who have STP questions.
 - 6.3.8 Develop and maintain STP Users' Manual.
 - 6.3.9 Review/approve all DCFs prior to placement on the STP Production Site.
- 6.4 Division/Branch Chiefs:
 - 6.4.1 Periodically review the STP Management Report to ensure the correct JITC System POC (lead AO) is identified for systems in their Division/Branch.
 - 6.4.2 Notify STP Coordinators jitcstp@fhu.disa.mil, or STP Division POC, if assistance is required to change the JITC System POC, or modify any information in STP.
 - 6.4.3 Ensure Action Officers update and maintain their STP entries.
- 6.5 STP Division POCs:
 - 6.5.1 Obtain STP requirements from Division employees.
 - 6.5.2 Attend all STP Users' Group meetings and present/discuss Division requirements.
 - 6.5.3 Assist employees in their Division by showing them how to search, insert or update system and test/activity information.
 - 6.5.4 Update required system entries in the absence of JITC System POC. STP Division POCs have the ability to enter/update system and/or test/activity information for anyone within their

Division.

7. **Data Responsibility.** Figure 11-1 summarizes *who* is responsible for ensuring *what* information is entered in the STP.



- Legend:
- | | | | |
|------|---------------------------------|------|--|
| AO | Action Officer | ICEP | Interoperability Certification Evaluation Plan |
| Cap | Capability | ISP | Information Support Plan |
| CDD | Capability Development Document | ITP | Interoperability Test Plan |
| Cert | Certification | ORD | Operational requirements Document |
| CPD | Capability Production Document | P&PB | Plans and Policies Branch |
| Doc | Document | Req | Requirement |
| Eval | Evaluation | TEMP | Test and Evaluation Master Plan |
| ICD | Initial Capabilities Document | | |

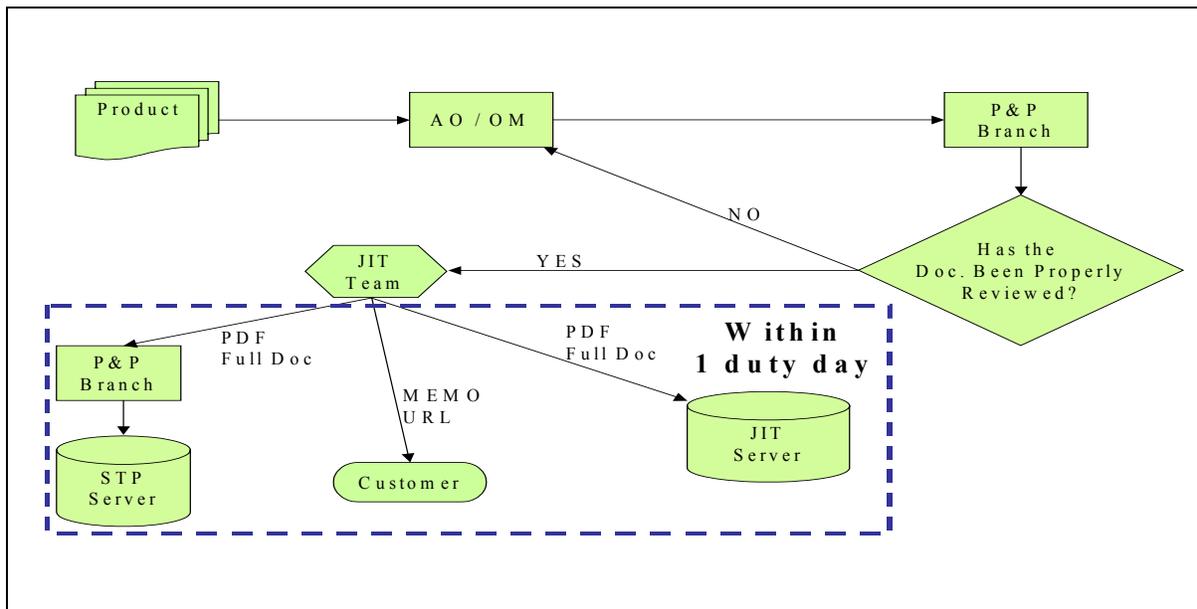
Figure 11-1. STP Data Entry Responsibilities

This Page Intentionally Blank

ELECTRONIC REPORT DISTRIBUTION TOOL

1. **General.** The [Electronic Report Distribution](#) (ERD) Tool is JITC’s primary method to distribute formal products (test reports, certification documents, test plans, etc.) to our customers. ERD reduces the time required to get products to our customers. Additionally, ERD reduces JITC’s postage and handling costs. JITC’s Automated Systems and Local Area Network Operations Branch (JTBB) is responsible for ERD. ERD is available on JITC's Intranet web site (<http://jitcnet.fhu.disa.mil/>). ERD instructions are located within the tool and will not be discussed in this enclosure. See enclosure 6 for document review processes.

2. **ERD Process.** ERD process is depicted in figure 12-1. The action officer (AO) or the office manager can submit the document to ERD from their own workstation. Distribution lists should include the proponent and any other interested, authorized parties. Standards Conformance Certifications shall include the ERD "Conformance Cert Letter Core List." Interoperability certifications of all types (including "extension of certification") shall include the ERD "Interoperability Cert Letter Core List." The tool notifies Plans and Policies Branch (P&PB) there is a document to review. Their first step is to ensure the document has gone through the review process described in enclosure 6. If the document hasn't been formally reviewed, P&PB will return the document for proper staffing. If the document passes this final review, it will be sent to the Joint Interoperability Tool (JIT) team and be delivered to the customer.



Legend			
AO	Action Officer	PDF	Portable Document Formant
JIT	Joint Interoperability Tool	STP	System Tracking Program
OM	Office Manager	URL	Uniform Resource Locator
P&P	Plans and Policies		

Figure 12-1. ERD Process

3. **ERD Results.** The customer will receive an e-mail with a portion of the signed product in Portable Document Format (PDF). For Certification documents, the customer will receive the certification memo, but not the testing summary. For Test Reports, the customer will receive the

title, signature, and executive summary pages. For all documents, the customer will receive a Uniform Resource Locator (URL) address for the entire product on the JIT server. Additionally, most products will be available on the [System Tracking Program](#) (STP) tool.

4. **Applicability.** All unclassified and non-proprietary JITC documents shall be distributed to our customers using the ERD. Sensitive, proprietary, or classified documents must still go through the appropriate JITC review and approval processes, with consideration given to the classification (e.g., do not e-mail classified documents on the NIPRNet). Below is a list of document types that are considered test related and require distribution using the ERD. This is not an inclusive list.

- Plans and reports of all types
- Certification letters (Interoperability Test and Standards Conformance)
- Compliance letters
- Assessment letters
- Operational Test Readiness Review (OTRR) letters
- Recommendation to Proceed letters
- Interoperability Status letters

5. **Document Archiving and Limited Distribution.** All JITC testing related documents submitted via the ERD are entered into the [STP](https://stp.fhu.disa.mil/) (<https://stp.fhu.disa.mil/>), and are viewable to all authorized .mil/.gov STP users. Additionally, all documents distributed via the ERD are entered into the [Joint Interoperability Tool](http://jit.fhu.disa.mil/) (JIT) http://jit.fhu.disa.mil, and are viewable to all authorized JIT users, i.e., .com/.mil/.gov users. It is the AO's responsibility to notify P&PB and the [STP Coordinators](#) if a document should not be viewable by all STP or JIT users. Appropriate rationale should be provided to P&PB, and approval will be handled on a case-by-case basis. It is recommended that AOs also review the STP's "System Documentation" link for all their systems, and notify the P&PB as soon as possible if a historical document is listed that should not be viewable to all STP/JIT users.

INTERIM CERTIFICATE TO OPERATE (ICTO) PROCESS

1. **General.** An Interim Certificate to Operate (ICTO) is a temporary waiver, not to exceed 1 year, from joint system interoperability test certification. In accordance with CJCSI [6212.01](#), an ICTO is the authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use.

2. **Overview.** The Interoperability Test Panel (ITP) is one of seven panels that support the Military Communications-Electronics Board (MCEB). The ITP identifies, coordinates, and resolves Information Technology (IT)/National Security Systems (NSS) interoperability testing issues; including ICTO request approval. The ICTO process, format, meeting minutes, and active letters are located at JITC's ITP website (<http://jitc.fhu.disa.mil/itp.htm>). All ICTO letters and status information are located in JITC's System Tracking Program (STP) <https://stp.fhu.disa.mil> under Main Menu/Reports/ICTO Report.

2.1 The ITP Chairman (Joint Staff (JS) J-6) decides whether to grant an ICTO. The ITP members vote to approve or disapprove the ICTO.

2.2 Decision to grant an ICTO is based on the following information:

- Initial test results
- First system to implement an interface
- Assessed impact on the operational systems / networks
- Urgent operational need
- Plan for future certification

2.3 An ICTO is not appropriate for systems that failed to meet identified interoperability requirements during joint system interoperability testing.

2.4 Fielded systems that do not have a certified Capability Production Document (CPD) or Information Support Plan (ISP) must request an ICTO in order to continue operating.

2.5 An ICTO will not exceed 1 year; however, the ITP may consider an extension.

3. Policy

3.1 The ITP Executive Agent (EA), who is the JITC National Capitol Region (NCR) Liaison Officer, will contact the appropriate JITC Division Chief or Action Officer (AO) to obtain JITC's position on an ICTO request. JITC only provides a recommendation for (or against) the ICTO, and does not submit requests for ICTOs. Only the Program Manager (PM)/proponent can request an ICTO.

3.2 The assigned AO must review the ICTO, and thoroughly research the system before providing a recommendation.

3.3 To ensure a consolidated JITC response, the AO will coordinate with respective JITC Point of Contact (POC(s))/lead AOs if the ICTO topic crosses into another Division's mission/functional area, or if additional expertise is required to review the ICTO request.

3.4 The AO will coordinate the recommendation with their Branch Chief, Division Chief, and copy the Chief, Plans and Policies Branch (C,P&PB) before notifying the ITP EA.

4. **Procedures.** The procedures for processing an ICTO are discussed below and depicted in Figure 13-1.

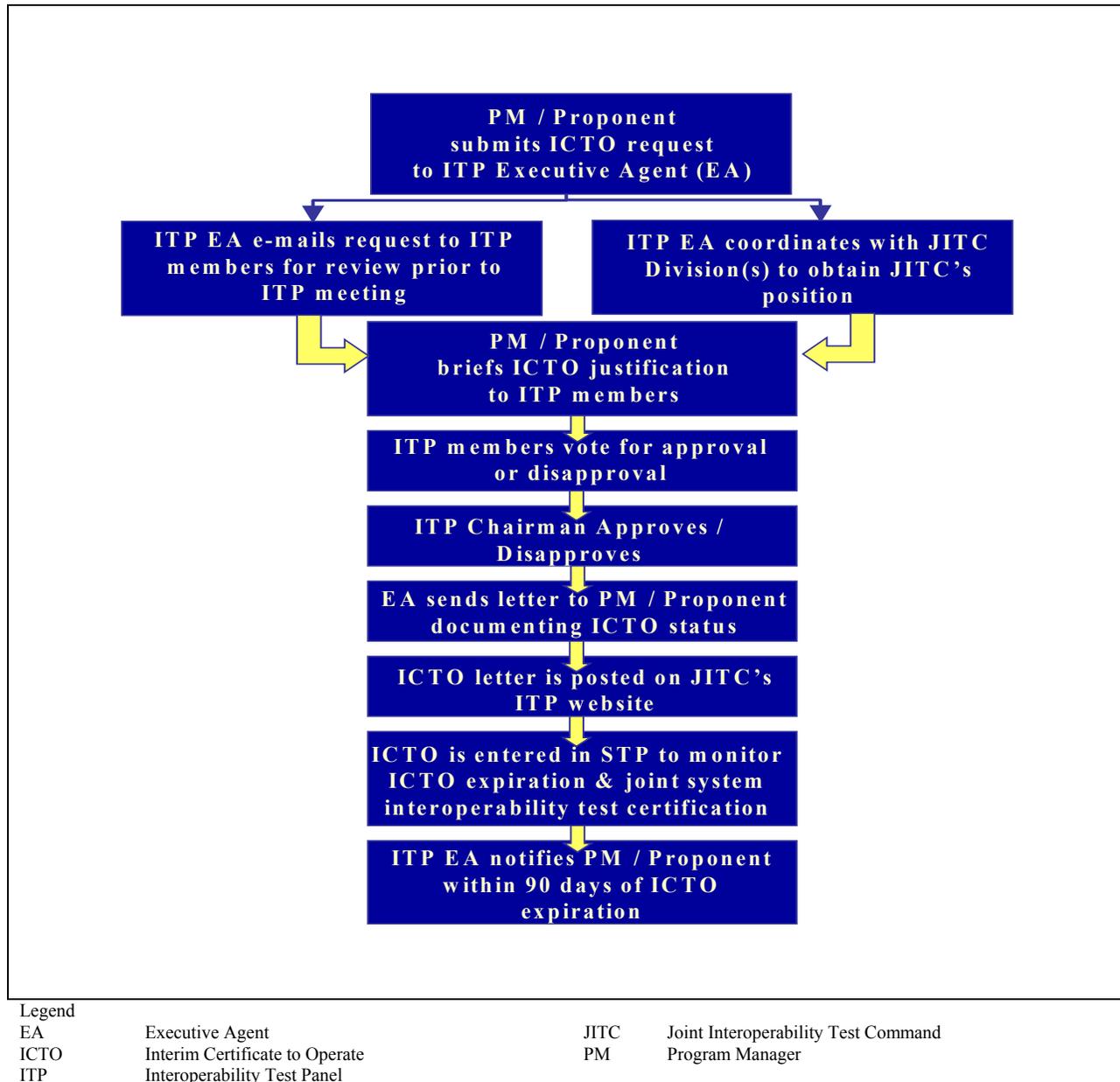


Figure 13-1. Interim Certificate to Operate (ICTO) Process

4.1 Program Manager (PM)/proponent completes an ICTO request form and sends the form to the ITP EA. The ICTO request form is located at JITC's ITP website:

<http://jitic.fhu.disa.mil/itp/ictoinfo.htm>. The form can be sent to the ITP EA three ways.

4.1.1 Mail the form to:

Joint Interoperability Test Command (JITC)
Attn: ITP Executive Agent
101 Strauss Ave, Code 1348
Indian Head, MD 20640-5035

4.1.2 Email to the ITP EA at ITP_EA@ncr.disa.mil

4.1.3 Submit online at JITC's ITP website: <http://jitic.fhu.disa.mil/itp/ictoinfo.htm>

4.2 A copy of the form should be sent to the combatant command/service/agency (CC/S/A) representatives for coordination. If the mandatory sections of the form are not completed, the request will be returned for completion before it is submitted for ITP member review.

4.3 The ITP EA will e-mail the ICTO request to the ITP members for review before the ITP meeting (meetings are typically scheduled every other month). If urgent out-of-cycle processing is required, the ITP members will process the ICTO electronically or telephonically.

4.4 The ITP EA will e-mail the ICTO to the respective JITC Division Chief or AO (if known) to obtain JITC's recommendation. JITC's internal review of the ICTO is discussed below.

4.4.1 If the ITP EA does not know the Subject Matter Expert's (SME) identity, the ITP EA will ask the appropriate Division Chief to assign the ICTO to an AO for SME review. If the SME is not available, the assigned AO will inform the SME of JITC's recommendation.

4.4.2 AO will review the ICTO, and thoroughly research the system to determine if an ICTO should be granted.

4.4.3 AO will use JITC's System Tracking Program (STP) to determine previous testing and certification status.

4.4.4 AO will coordinate with respective JITC POC(s) if the ICTO topic crosses other Divisions, or if additional expertise is required to review the ICTO request.

4.4.5 AO will e-mail the recommendation to their Branch and Division Chief for review and approval. Additionally, the AO will provide a copy of the recommendation to C,P&PB.

4.4.6 After Division Chief approval, the AO will e-mail the JITC's ICTO recommendation to the ITP EA, sending a copy of the e-mail and recommendation to their Branch Chief, Division Chief, and C,P&PB.

4.5 The ITP EA will invite the PM/proponent, via the submitting CC/S/A, to the next scheduled ITP meeting to brief the system and the justification for requesting an ICTO. The assigned AO is invited to attend this briefing (at their Division's expense) to obtain additional information that may be useful in providing a recommendation for the ICTO.

4.6 The ITP members will then vote to approve or disapprove the ICTO. For Defense Switched Network (DSN) or Public Switched Telephone Network (PSTN) systems/equipments, the ITP will vote and make a recommendation on approving the ICTO to ASD/NII as the DOD CIO. The ITP will not make a positive recommendation on a DSN or PSTN ICTO request without the concurrence of the ASD/NII ITP member.

4.7 The ITP Chairman (Joint Staff (JS) J-6) will approve or disapprove the ICTO.

4.8 The ITP EA will forward the ICTO letter to the PM or proponent, and the ITP e-mail distribution list documenting the ICTO status.

4.9 The ITP EA will post the ICTO letter on JITC's ITP website, and enter the letter and associated ICTO information into the STP. The STP monitors ICTO expiration and joint system interoperability test certification status.

4.10 The ITP EA will use STP to generate an Expiring ICTO Alert. This alert provides a list of ICTOs that have expired or will expire within 90 days.

4.11 When an ICTO has expired, or is within 90 days of expiration, the ITP EA will notify the PM or proponent that action is needed. If a satisfactory resolution cannot be attained, the ITP EA will notify the responsible ITP CC/S/A representative for corrective action. It is the responsibility of the ITP CC/S/A representatives to ensure resolution of all expiring or expired ICTOs.

**U.S. MILITARY COMMUNICATIONS-ELECTRONICS BOARD (MCEB)
STATUS OF INTEROPERABILITY BRIEFING PROCESS**

1. **General.** In accordance with DODD [5100.35](#), the mission of the Military Communications Electronic Board (MCEB) is to:

1.1 Coordinate between DOD Components; DOD and other governmental departments/agencies; and between DOD and representatives of foreign nations, on military communications-electronic matters, including Information Technology (IT) and National Security Systems (NSS), referred by the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the military departments, and other DOD components.

1.2 Provide guidance and direction to combatant commands, services, and agencies (CC/S/A).

1.3 Furnish advice and assistance, as requested, to the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the military departments, and other DOD components.

2. **Overview.** In accordance with [MCEB Pub 1](#), the Interoperability Test Panel (ITP) is required to provide the MCEB a semi-annual (or as requested) interoperability status briefing. JITC usually presents this briefing on behalf of the ITP. The MCEB brief can be an informational or decisional brief. After coordination with the Joint Staff (JS) J-6, the Chief, Plans, Policies and Warfighter Support Division (C, PP&WSD) will recommend a subject or issue to JITC's Corporate Board, or the MCEB may request a specific topic. Examples of previous MCEB briefings are located at JITC's ITP website: <http://jitic.fhu.disa.mil/itp/tstatus.htm>.

3. **Policy.** The C, PP&WSD will notify the division responsible for briefing the MCEB approximately 6 months in advance. It is the responsibility of the lead division to:

3.1 Be prepared to brief the MCEB by continually tracking the interoperability 'big picture' status with respect to functional areas assigned to their division.

3.2 When notified of the requirement to brief the MCEB, assign a functional area expert to brief the MCEB. The Deputy Commander may also assign the briefer, as needed.

3.2.1 The selected briefer must:

- Have thorough knowledge of the functional area or topic.
- Be well spoken and able to answer questions from all military service levels, to include 3-Star level.
- Represent JITC in a professional manner.
- Present the briefing throughout the entire MCEB briefing cycle if the topic requires a decision/action from the MCEB Principals.

3.3 Perform a thorough review and analysis of their assigned functional area/topic.

3.4 Report the status of interoperability on the selected functional area, or provide issues/supporting information on the assigned topic.

3.5 For those systems that are reported as "red," ensure the Program Manager has been notified of the requirement for joint system interoperability testing and certification. An initial contact letter example is under: [\\CDXFHU1\GROUPS\PLANS & POLICIES TRAINING\Example products - cert letters - etc\](#).

4. **Procedures.** Provided are the procedures for preparing a briefing and information paper for the MCEB.

4.1 All briefings must include an information paper.

4.2 Use the briefing slide and information paper templates located under [T: Share – MCEB Briefings\MCEB Briefing & Info Paper Guidance](#). Please refer to the MCEB On-line Support Tool for the latest guidance, templates, schedules, and Points of Contact (POCs) for requesting access: <https://www.jsJ-6giganalysis.com>.

4.3 Use the general guidelines shown below for the briefing slides.

- No more than eight slides (not including backups)
- Minimize use of colors, graphics, and bitmaps to reduce size of briefing
- Do not remove the Joint Staff (JS) logo on the briefing slide template (i.e., do not replace the JS logo with the DISA or JITC logo)
- Number all charts in lower left corner
- Do not use font size less than 20 point to ensure readability
- Briefings should be concise and to the point. Do not get bogged down in technical details, keep detail charts as backups

4.4 When preparing a status of interoperability briefing, use JITC's System Tracking Program (STP) <https://stp.fhu.disa.mil> to determine the testing/certification status of the systems, and then contact the JITC System POC to verify the status.

4.5 Use the following color-codes to depict a system's status on the briefing slides:

4.5.1 Green systems have a full or specified interfaces joint system interoperability test certification/recertification memorandum. JITC has certified some or all of their critical interfaces. Fielding these systems' certified interfaces may be of value to the Warfighter, even though further testing may be warranted/planned or the system has known limitations.

4.5.2 Yellow systems are actively participating in the testing process (engaged in or scheduled for joint system interoperability test certification/recertifications) but have not yet been certified/recertified for joint interoperability.

4.5.3 Red systems need to be certified/recertified but are not progressing toward obtaining certification/recertification. These systems have either been unable to schedule a joint system

interoperability test (due to CC/S/A limitations) or have tested and were unable to obtain a joint system interoperability test certification.

4.5.4 White systems are legacy systems that are successfully operating in the field and are of such a low interoperability risk that there is limited benefit in testing and certifying them. Many of these systems have participated in other interoperability tests but have but not themselves been under evaluation or certified.

4.6 The Action Officer (AO) will ensure the briefing and information paper go through the proper review and staffing procedures before presentation to the MCEB. During this process, the AO will incorporate comments, as appropriate. The AO will ensure coordination with respective JITC POC(s) if briefing topic crosses into other divisions.

4.6.1 AO develops the briefing and information paper.

4.6.2 AO sends the briefing/information paper to the Branch Chief for review/approval.

4.6.3 Upon Branch Chief approval, briefing/information paper is sent to the Division Chief for review/approval.

4.6.4 Upon Division Chief approval, briefing/information paper is sent to the Chief, Plans and Policies Branch (C, P&PB) for review/approval.

4.6.5 Once the Branch/Division Chief and C, P&PB approve the briefing/information paper, the AO shall present the briefing to JITC's Corporate Board.

4.6.6 Incorporate changes from the Corporate Board and staff them through the Branch/Division Chief and C, P&PB.

4.6.7 Upon approval from the Branch/Division Chief and C, P&PB, the AO shall present the briefing to the MCEB ITP. The ITP is one of seven panels that support the MCEB. All MCEB briefings must be coordinated through the ITP before presentation to the MCEB. Contact the ITP Executive Agent (EA) to schedule the MCEB briefing at: ITP_EA@ncr.disa.mil

4.6.8 Incorporate changes from the ITP members, and staff them through the Branch/Division Chief and C, P&PB. Upon approval, resubmit to the ITP EA for ITP approval.

4.6.9 Upon approval from the ITP, e-mail the briefing/information paper to DISA's Director for Testing for review/approval (copy the JITC Commander, Deputy Commander, Staff Director, C, PP&WSD, and C, P&PB).

4.6.10 Incorporate changes from DISA's Director for Testing, and staff them through the Branch/Division Chief and C, P&PB.

4.6.11 Upon approval from the Branch/Division Chief and C, P&PB, the briefing must be e-mailed to DISA's MCEB Coordinator for staffing and approval. If the briefing contains contentious material, the MCEB Coordinator will staff the briefing through DISA's Senior

Strategy Session (SSS) for review/approval. DISA's MCEB Coordinator contact information is: Strategic Planning and Information Directorate, (703) 681-1646, McCulloch@ncr.disa.mil.

4.6.12 Incorporate changes from DISA's MCEB Coordinator, and staff the revised briefing through the Branch/Division Chief and C, P&PB.

4.6.13 Upon approval from the Branch/Division Chief and C, P&PB, provide the revised briefing to DISA's MCEB Coordinator. DISA's MCEB Coordinator must be kept informed of any changes/issues throughout the entire MCEB briefing cycle.

4.6.14 The briefing must be staffed through the following MCEB cycle with coordination from the designated JS J-6 POC. The same briefer shall brief throughout the entire MCEB briefing cycle if the topic requires a decision/action from the MCEB Principals. These meetings are usually one week apart. A quick turnaround is necessary if changes are required between meetings.

- MCEB Coordinators' Meeting
- MCEB C4 Deputies' Meeting
- MCEB Principals' Meeting (Executive Session)

4.7 Ensure final MCEB briefing is sent to the ITP Executive Agent ITP_EA@ncr.disa.mil for posting on JITC's ITP website <http://jitic.fhu.disa.mil/itp/tstatus.htm>.