

# Joint Interoperability Test Command



## Interoperability Process Guide

Version 2.0  
23 March 2015

(This page intentionally left blank.)

## Interoperability Process Guide

The Interoperability Process Guide (IPG) is developed and published by the Joint Interoperability Test Command (JITC) in coordination with the Department of Defense's Chief Information Office (DoD CIO). It is effective immediately upon publication. The IPG is available at: <http://jitc.fhu.disa.mil/projects/isg/site/pubs.aspx>. Errata identified between major releases will be posted at the same location.

### Submitted:

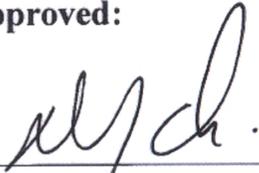


<sup>for</sup> Douglas J. Orsi  
Colonel, United States Army  
Commander, Joint Interoperability Test Command

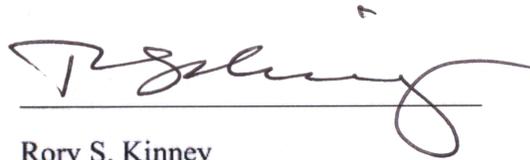
10 MAR 2015

Date

### Approved:



Douglas J. Orsi  
Acting Director  
Office of the Test and Evaluation Directorate



Rory S. Kinney  
Director, Architecture and Engineering  
Office of the DoD Chief Information Officer

10 MAR 2015

Date

23 MAR 15

Date

(This page intentionally left blank.)

**Summary of Changes**

Version	Sections Affected	Description of Change
Version 1.0	All	<ul style="list-style-type: none"> <li>- Initial approved version.</li> </ul>
Version 1.0, Change 1	All	<ul style="list-style-type: none"> <li>- Administrative corrections.</li> <li>- Fact-of-life changes</li> <li>- Updated waiver and ICTO sections.</li> <li>- Added section on Operating at Risk List processes.</li> <li>- Added Sections 10 and 11 to define the minimum DoDAF architecture requirements needed for interoperability certification. Changes in text to reflect processes associated with required architecture section.</li> </ul>
Version 2.0	All	<ul style="list-style-type: none"> <li>- Administrative corrections.</li> <li>- Updated references based on new DoDI 8330.01 and cancellation of DoDD 4630.05, DoDI 4630.8, and DoD CIO memorandum, “Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS).”</li> <li>- Added staffing guidance on requirements document review.</li> <li>- Added criticality definitions for requirements review comments.</li> <li>- Inserted Network Connection clarification.</li> <li>- Updated Operating at Risk List section.</li> <li>- Updated Recertification section.</li> <li>- Updated Waiver to Policy section.</li> <li>- Updated Architecture section.</li> </ul>

(This page intentionally left blank.)

## TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1. Purpose .....	1
2. Overview of Certification Policy and Process .....	1
3. Pre-Joint Interoperability Test and Certification Procedures .....	5
4. Joint Interoperability Test and Certification .....	12
5. Post-Joint Interoperability Test and Certification Procedures .....	15
6. Interim Certificate To Operate (ICTO) Procedures .....	23
7. Waivers to Policy.....	27
8. Operating At Risk List (OARL) .....	30
9. Other Evaluations and Related Information.....	32
10. Requirements for Joint Interoperability Certification (JIC).....	34
11. Minimum Set of Architecture Information Required for Joint Interoperability Certification .....	38
Appendix A References .....	41
Appendix B Abbreviations and Acronyms.....	43
Appendix C Definitions .....	49

## TABLE OF FIGURES

<u>FIGURE</u>	<u>PAGE</u>
Figure 2-1. Interoperability Directives, Instructions, and Guidance.....	2
Figure 2-2. Joint Interoperability Certification T&E Overview.....	3
Figure 2-3. Notional Joint Interoperability Certification Process .....	4
Figure 3-1. Test Preparation Activities.....	5
Figure 3-2. NR KPP Focus .....	6
Figure 3-3. Defining NR KPP Policy .....	7
Figure 4-1. Representative T&E Test Phase Activities .....	12
Figure 5-1. T&E Post-Test Activities .....	15
Figure 5-2. Interoperability T&E Products .....	16
Figure 5-3. JITC Interoperability Reports.....	17
Figure 5-4. Recertification Request Procedures Summary .....	20
Figure 6-1. Procedures for Processing ICTO Requests.....	25
Figure 7-1. Waiver to Policy Process .....	28
Figure 8-1. OARL Description .....	30
Figure 10-1. Joint Interoperability Certification Requirements Process Overview.....	34
Figure 10-2. Joint Interoperability Certification Requirements Process .....	36
Figure 11-1. Minimum Set of Viewpoints for Joint Interoperability Certification .....	40

## **1. Purpose**

This Interoperability Process Guide (IPG) outlines the procedures and documentation required for Joint Interoperability Test and Certification, waiver processing, and associated processes and procedures. It addresses interoperability test and certification based on the Net-Ready Key Performance Parameter (NR KPP).

- a. Section 1 provides the purpose of the IPG.
- b. Section 2 outlines the governing directives and documents that underpin interoperability testing, and identifies key organizations that participate in interoperability policy making and its implementation.
- c. Sections 3, 4, and 5 identify the processes, procedures, and guiding principles that cover preparation, evaluation, and reporting for Joint Interoperability Certification (JIC).
- d. Sections 6, 7, and 8 outline the Department of Defense, Chief Information Office (DoD CIO) processes and procedures for Interim Certificate to Operate (ICTO), Waivers to Policy, and Operating at Risk List (OARL).
- e. Section 9 provides information on other evaluations and related information.
- f. Sections 10 and 11 describe requirements for JIC, including the review process and a list of minimum required architecture information.

## **2. Overview of Certification Policy and Process**

a. **Certification Policy.** Several documents govern interoperability for DoD. The paragraphs below summarize key instructions and manuals. Figure 2-1 depicts the high level relationships among these documents.

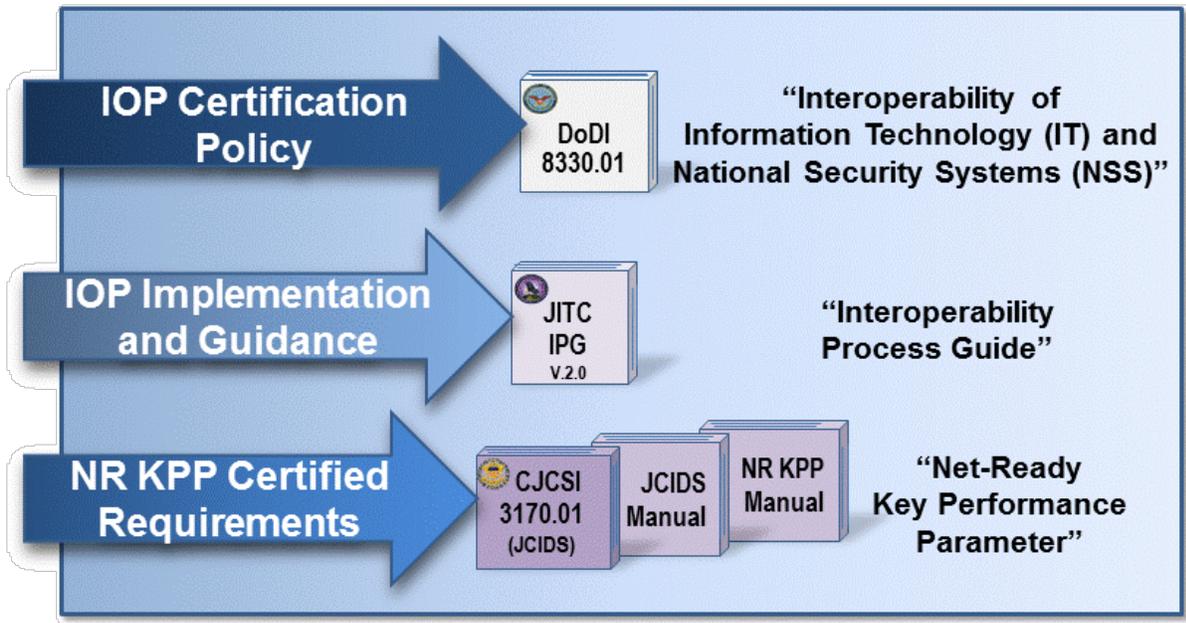
(1) DoD Instruction (DoDI) 8330.01 (reference (a)) updated policy and procedures for interoperability of Information Technology (IT) and National Security Systems (NSS). This incorporates and cancels DoD Directive (DoDD) 4630.05, DoDI 4630.8, and the DoD CIO memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)." DoDI 8330.01 states that all IT systems, including NSS, must be evaluated and certified for interoperability prior to fielding of a new system. This includes upgrades to existing systems as well as periodic interoperability evaluations during the system's life-cycle.

(2) Under the oversight and direction of the DoD CIO, JITC serves as the Joint Interoperability Certification Authority for all DoD IT with joint, multinational, and interagency interoperability requirements. DoDI 8330.01 further specifies that JITC shall certify all joint IT and NSS for interoperability, based on a Joint Staff certified NR KPP, when applicable.

(3) Although the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01 series no longer applies, NR KPP policy can be found in the Joint Capabilities Integration and

Development System (JCIDS) Manual. The NR KPP Manual (reference (b)) contains detailed information regarding the foundation and development process for the NR KPP. The DoD Architecture Framework (DoDAF) viewpoints development processes provide the data used to derive the NR KPP.

(4) This IPG describes the processes for joint interoperability testing, system certification, waiver submission, and updates required for obtaining a Joint Interoperability Certification. The IPG will be updated periodically.



**Figure 2-1. Interoperability Directives, Instructions, and Guidance**

(5) This IPG does not address certification processes for Unified Capabilities (UC). (UC capabilities are voice, video, data (collaboration), and mobile devices.) Unified Capabilities Requirements (UCR) Document (reference (c)), DoDI 8100.04 (reference (d)), and the Approved Products List (APL) Process Guide (reference (e)) detail the interoperability certification policy and requirements for UC.

(6) Some programs do not develop the NR KPP or DoDAF architecture artifacts. In these cases, the DoD CIO and Joint Staff, with technical assistance from JITC, evaluate the proposed interoperability artifacts and determine if they are acceptable as interoperability requirements. If found acceptable, all other aspects (aside from source and type of requirements) detailed in this IPG will apply.

b. Interoperability within the Acquisition Lifecycle. JITC, as DoD’s sole joint interoperability certifier, has the ability to assist designated test organizations and Program Management Offices (PMOs)/Sponsors with defining interoperability data collection requirements for Joint Interoperability Certification on a cost reimbursable basis. The actual interoperability certification event follows a traditional test and evaluation strategy as shown in Figure 2-2. Programs can use any test organization to conduct the testing, so long as they follow

the prescribed processes detailed within this IPG. Programs may engage JITC to support their testing or execute their testing in totality. Regardless of the test method, JITC must evaluate the results and make an interoperability determination.

(1) Interoperability data collection requirements can be fulfilled through the execution of other test and evaluation events. As an example, JITC can obtain data from cybersecurity (previously Information Assurance (IA)) testing, Developmental Test and Evaluation (DT&E), User Acceptance Testing (UAT), Operational Test and Evaluation (OT&E), or any combination thereof. The PMO/Sponsor of the system under test is responsible for ensuring funding for JITC efforts. Because JITC operates through a cost reimbursable model, JITC will always strive to design the most cost effective solution and work to conserve resources while achieving the greatest testing efficiencies.

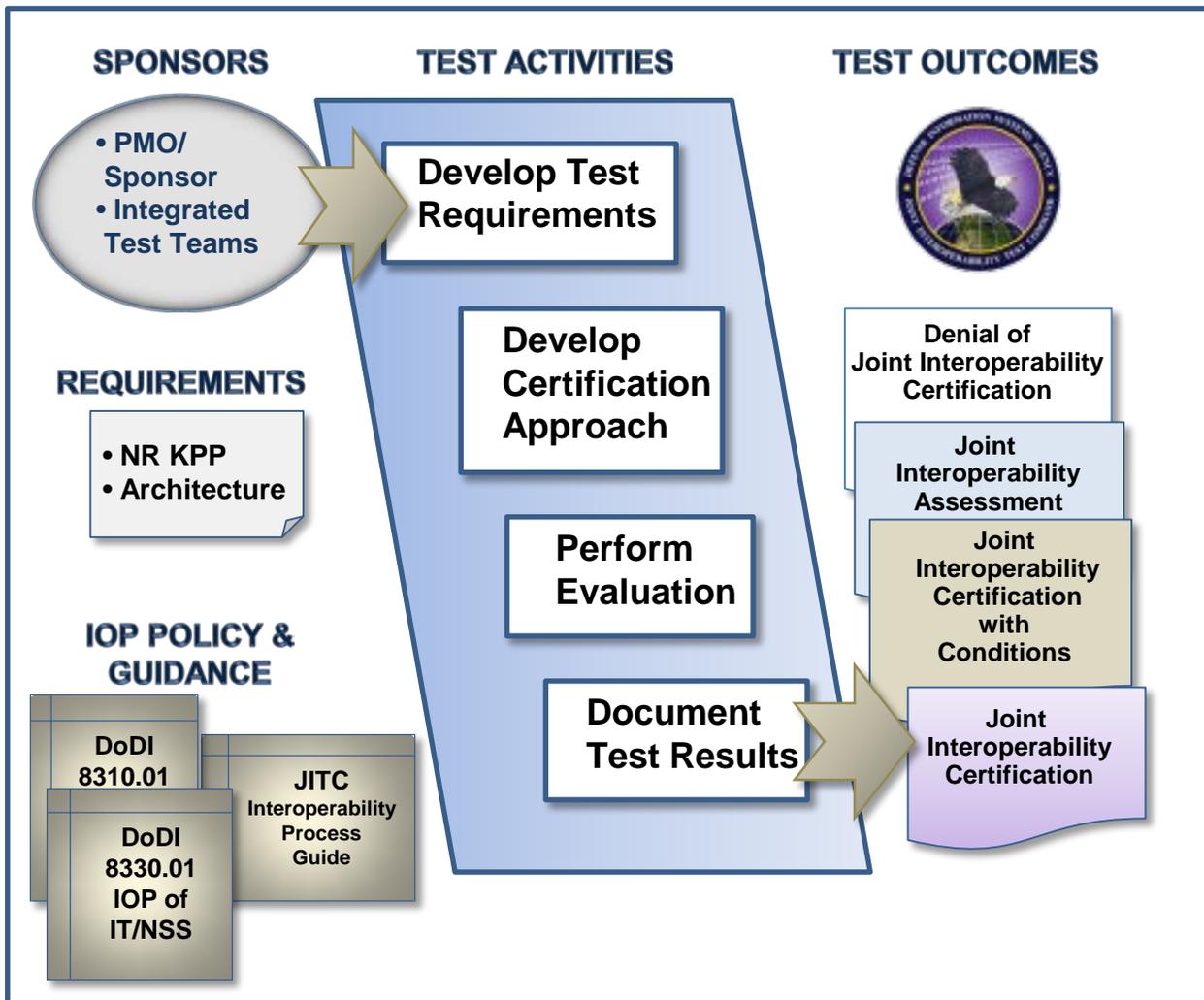


Figure 2-2. Joint Interoperability Certification T&E Overview

(2) Specific to NSS, JITC will assist National Geospatial-Intelligence Agency (NGA) and National Security Agency (NSA) with interoperability objectives and help define

interoperability test and evaluation criteria, measures, and requirements established by intelligence functional managers. JITC will assist with the test planning, data collection, and reporting to ensure systems undergo and successfully complete joint interoperability test and evaluation. As stated above, the PMO/Sponsor of the system under test is responsible for ensuring funding for JITC efforts.

c. Operating at Risk List. If a system is denied certification (due to an interoperability shortfall) or has not made significant progress toward achieving Joint Interoperability Certification, the system may be placed on the OARL. The OARL is monitored by the DoD CIO’s Interoperability Steering Group (ISG). (Refer to Section 8 for OARL policy and procedures.)

d. Network Connection. IT must be certified for interoperability, or possess an ICTO or waiver to policy before connection to any DoD network (other than for test purposes). An interoperability certification with conditions may be issued under certain circumstances. These conditions may constrain use of network interfaces that do not meet all critical requirements (threshold NR KPP), while not limiting use of other interfaces and associated information exchanges. The appropriate Connection Approval Office (CAO) determines final network connection approval, with interoperability certification being merely one of the determining factors. (This clarifies the requirement in DoDI 8330.01, Enclosure 3, paragraph 2.b(3).)

e. Interoperability Process Overview. Sections 3, 4, and 5 detail the Joint Interoperability Certification preparation, test and evaluation, and certification processes. Figure 2-3 shows a notional process flow for a program of record; therefore, the steps would be applicable to most systems requiring a certification.

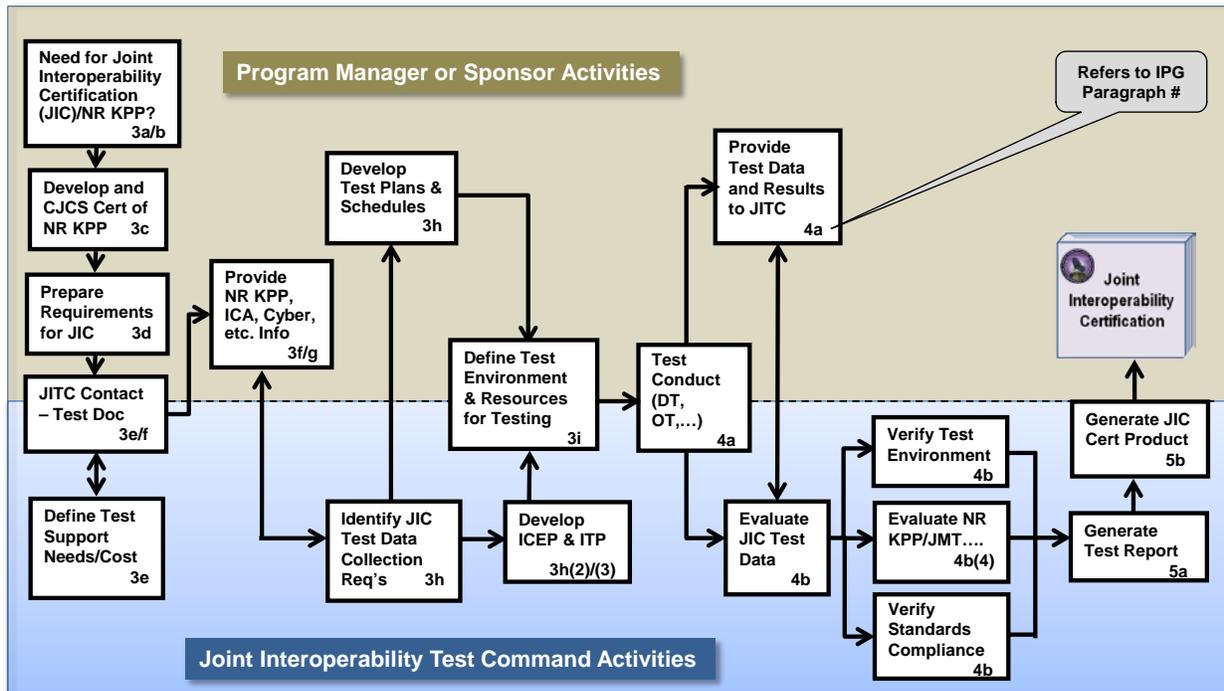
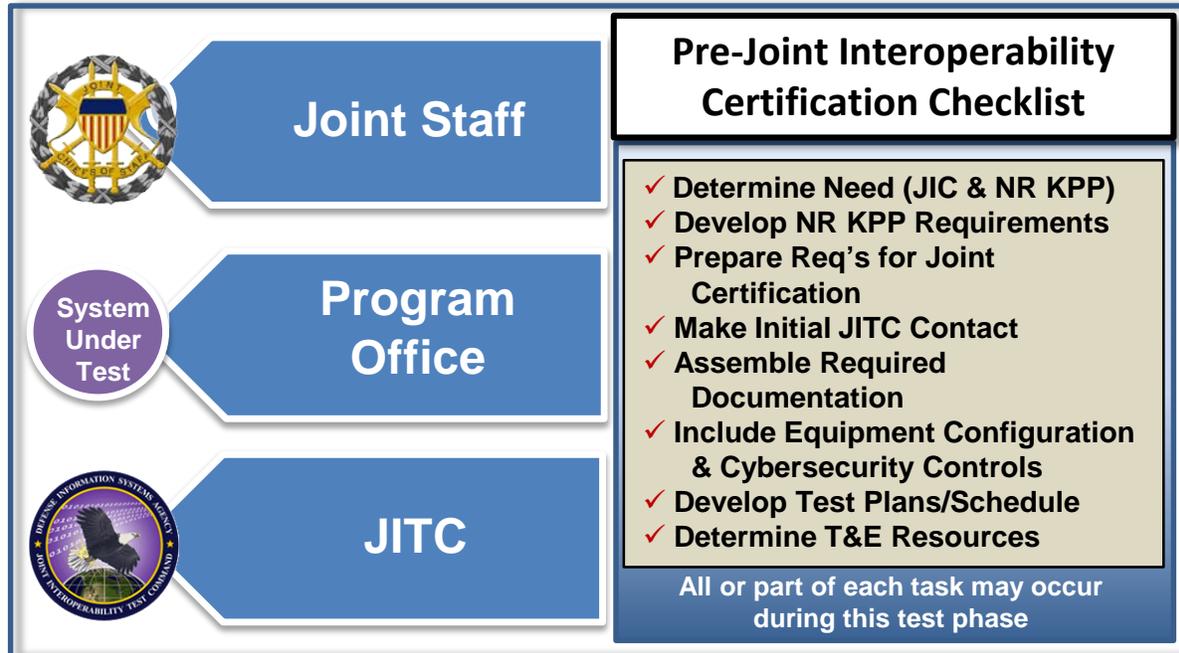


Figure 2-3. Notional Joint Interoperability Certification Process

### 3. Pre-Joint Interoperability Test and Certification Procedures

The Test and Evaluation (T&E) checklist shown in Figure 3-1 below typifies the range of test preparation activities that routinely occur during the pre-joint certification phase.



**Figure 3-1. Test Preparation Activities**

a. Determine Need for Joint Interoperability Certification. All systems with joint interfaces or joint information exchanges with other systems require joint interoperability certification. A joint interface occurs when any system whose mission is joined through a logical connection with a system(s) or data sources from an external partner for the purpose of exchanging common data, sharing situational awareness, or partnering to perform a single mission. An external partner is defined as another DoD Component, U.S. Government Department or Agency (including federal, state, local, and tribal), Coalition partners, non-governmental organizations, or any combination thereof that utilize the same interfaces and/or exchange information produced/consumed/shared or distributed by the system under test. Interfaces and/or information exchanges include all the data products and waveforms used or produced by the system (including sensor platforms). If Joint Interoperability Certification applicability is in doubt, the PMO/Sponsor should contact JITC for assistance with a determination or work through their respective ISG representatives for resolution. A list of Service/Agency ISG representatives can be found on JITC's ISG Resource website: <http://jitic.fhu.disa.mil/projects/isgsite/index.aspx>.

b. Determine Need for NR KPP Certification. The Joint Staff is responsible for confirming whether a system has joint interfaces or joint information exchanges and requires a Joint Staff NR KPP certification. The PMO/Sponsor develops the NR KPPs (see reference (b) for policy and procedures on developing the NR KPP and supporting documentation). Generally, certification of interoperability involves evaluating three (3) attributes with the NR KPP (see

Figures 3-2 and 3-3), and associated technical requirements defined in, or derived from, the solution architecture data.



**Figure 3-2. NR KPP Focus**

c. Develop NR KPP Requirements. An early step in preparation for joint interoperability certification is a Joint Staff requirements review, which includes Joint Staff certification of the NR KPP (or equivalent documentation). The NR KPP defines measures of effectiveness (MOEs) and measures of performance (MOPs) with threshold and, if applicable, objective criteria associated with three attributes: support military operations, enter and be managed on the network, and effective information exchange. Early coordination between the PMO/Sponsor and JITC is essential to ensure collection of the required data as part of the testing planned by the PMO/Sponsor.

(1) Support Military Operations. This attribute involves the MOEs and MOPs used in evaluating interoperability aspects of the system being tested within the operational context in achieving the tasks to fulfill its operational mission. Test data for this attribute will normally be obtained from the designated test organization responsible for the OT&E of the system.

(2) Enter and Be Managed on the Network. This attribute provides MOPs addressing the system's ability to successfully enter into and be managed within the networks it must operate on to perform its operational mission (includes the means for information transport). This also addresses associated technical parameters in or derived from architecture data for the system and the associated networks. Evaluating these details involves addressing both operational and technical requirements associated with the system's interaction with the specified networks. This evaluation may make use of data collected from DT&E for some technical requirements and OT&E for the operational requirements. Note: Careful review of assertions that a program does not enter or is not managed in a network is critical here, particularly with sensor programs, payloads, or platforms (manned or unmanned).

(3) Effective Information Exchange. This attribute provides MOPs associated with specific interfaces and information exchanges (resource flows) supporting the operational mission. It also considers interface and exchange technical parameters included in, or derived from, architecture data. As with the previous attribute, evaluation of this attribute must address both operational and technical requirements associated with each interface or exchange. Data to evaluate satisfaction of these requirements may be obtained from DT&E for some technical requirements or OT&E.

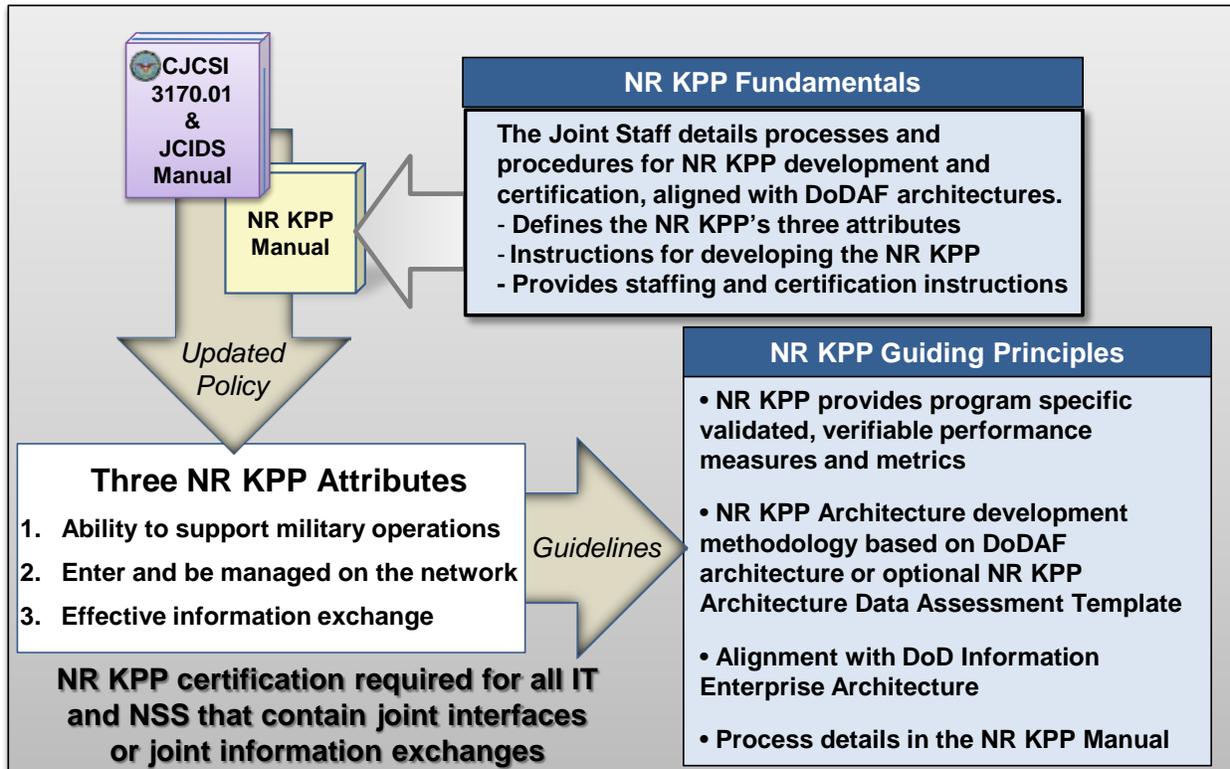


Figure 3-3. Defining NR KPP Policy

d. Prepare Requirements for Joint Interoperability Certification. PMO/Sponsor has the responsibility for developing the requisite interoperability requirements documents and associated architecture data. The PMO/Sponsor-JITC coordination on architecture viewpoints needed for interoperability testing and certification should happen early in the architecture development process. The following policy and guidance, as well as appropriate DoD Component requirements, govern preparation of this documentation. (Also see Appendix A for additional references.)

(1) CJCSI 3170.01 (reference (f)) directs JCIDS documentation to be prepared and submitted. Format found in the JCIDS manual (reference (g)).

(2) DoDI 8330.01 (reference (a)) governs Information Support Plans (ISPs).

(3) The NR KPP manual (reference (b)) details preparation of the NR KPP, and related architecture analysis supporting its development.

(4) The above references also delineate the requirement for Interface Control Agreements (ICAs), and reference (b) also points to a descriptive ICA template.

(5) The DoD CIO DoDAF web site (reference (h)) contains a detailed description of the DoDAF, and its application in developing capability solution architectures.

e. Initial Contact with JITC to Schedule Support. To shorten test timelines, the PMO/Sponsor must work with their respective ISG representative to establish contact with JITC as early as possible (during initial development phases) to begin coordination for interoperability evaluation. The JITC public website (<http://jitic.fhu.disa.mil/>) provides forms and contact information under the “Support” section. The PMO/Sponsor is responsible for arranging funding for planning, testing, analysis, and reporting associated with interoperability certification. Funding must be in place prior to the start of any JITC activity (typically 120 days before). In the case of Common Data Link (CDL), the CDL Executive Agent funds testing.

f. Required Documentation for Test. The PMO/Sponsor must provide JITC the following information prior to any test and evaluation activity that will support Joint Interoperability Certification (typically 120 days before):

(1) Approved requirements documents (or requirements for Joint Interoperability Certification) with certified NR KPP. Information must include:

(a) A Joint Staff-certified NR KPP. The NR KPP will describe a set of performance measures, to include MOEs and MOPs.

(b) Appropriate supporting solution architecture data, as indicated in the NR KPP Manual (reference b) or the minimum essential architecture information required for Joint Interoperability Certification, as described in Section 11 of this document.

(2) Interface Documentation

(a) ICAs for each external interface of the system to be certified, as defined in the NR KPP Manual.

(b) Interface control documents/specifications (as appropriate) for each external interface of the system to be certified (made available to JITC and other participating test organizations).

(3) For systems employing technology governed by policy mandating specific standards conformance requirements (e.g., specified by DoD Information Technology Standards Registry (DISR)), documentation of appropriate standards conformance shall be provided or cited. For example, Radio Frequency (RF) communications often require over-the-air-interoperability, which involves the ability of two or more radios to process the waveforms generated by the other device. Such policies, for example, include those governing:

(a) DoD Ultra-High Frequency (UHF) Satellite Communications (SATCOM).

(b) Geospatial Intelligence (GEOINT) standardization for Still Imagery, Motion Imagery, and Geospatial Intelligence.

(c) Selected High Frequency (HF) and Very High Frequency (VHF) communications capabilities.

(4) Documentation of the cybersecurity configuration sufficient to ensure a realistic cybersecurity testing environment. The PMO/Sponsor must provide documentation, signed by the sponsor Authorizing Official (previously a Designated Approving Authority (DAA)), when claiming exemption from any cybersecurity requirements. When a PMO/Sponsor develops an enterprise application or service that is wholly dependent upon the enterprise infrastructure for security and access control, the requirements for security certification may be waived by the cybersecurity Authorizing Official.

(5) Version identification information for the system or system components (both services and data) to be certified, and for any interfacing capabilities and enterprise components.

(6) Approved PMO/Sponsor and designated test organization test plans and planning documents (see paragraph 3.h below).

(7) A Program Security Classification Guide.

g. Equipment Configuration/Application of Required Cybersecurity Controls.

Interoperability evaluation will be based on testing of production representative systems in as realistic an operational environment as practicable, to include the expected joint operating environment. Testing includes the use of test scenarios with a typical message mix, loading that reflects normal and wartime modes, and benign and hostile environments. System test configurations will represent realistic cybersecurity aspects of the operational environment to include application of the cybersecurity controls. If testing does not use the proper cybersecurity configuration, then the test results may be rejected, requiring additional testing. It is important in the planning stages to recognize the need for a suitable interoperability environment (for the system under test and interfacing systems), including cybersecurity considerations.

h. Develop Test Plans/Schedule. The PMO/Sponsor shall coordinate with JITC to integrate interoperability test requirements and resources into the system's T&E documents (e.g., Test and Evaluation Master Plan (TEMP), test plans). JITC may produce an interoperability assessment strategy, which may be incorporated into an Interoperability Certification Evaluation Plan (ICEP) or an Interoperability Test Plan (ITP). The plan(s) used will depend on several factors: the complexity of the system (e.g., single item, number of external interfaces); development approach (e.g., commercial-off-the-shelf (COTS), evolutionary with numerous increments); and the anticipated number of JITC and non-JITC conducted test events. Changes in requirements, architecture, concept of operations, or the developmental/operational testing program may require changes in the overall plans. When a program is being developed in increments (phases, blocks, spirals, major releases, etc.), the plans must specify which requirements the system must meet for each increment to be certified.

(1) Test Plan Strategy

(a) Whenever possible, interoperability test data (including standards conformance) shall be obtained from the test program developed by the PMO/Sponsor and designated test organization, with input from JITC regarding data collection required to satisfy interoperability evaluation requirements. JITC shall provide these interoperability data collection requirements to the PMO/Sponsor and designated test organization as early in the lifecycle as possible (after receipt of funding) to be included in TEMPs and test plans. JITC interoperability certification is based on results from events that are as operationally realistic as feasible. This normally entails collection of data obtained from operational testing, operationally realistic exercise events, or from actual operational use.

(b) PMO/Sponsor and designated test organizations shall coordinate test plans with JITC prior to any test event supporting interoperability evaluation.

(c) When test data from the PMO's/Sponsor's test efforts are insufficient to perform an interoperability evaluation, JITC (when funded, and in coordination with the responsible PMO/Sponsor and designated test organization) shall develop and execute a plan for interoperability testing for collection and evaluation of the necessary data.

(d) NR KPP MOEs/MOPs (or equivalent requirements) are used to develop the TEMP. Established Joint Mission Threads (JMTs) shall be used to verify the operational effectiveness of information exchanges (reference (i)). If established JMTs are not available, appropriate mission operational tasks (activities) are derived from the Joint Staff certified NR KPP and approved architecture viewpoints (i.e., as in OV-5B and OV-6C).

(e) Standards conformance serves as a foundation for interoperability. If applicable, standards conformance should be assessed prior to joint interoperability testing. The PMO/Sponsor shall coordinate with JITC during the planning of standards conformance testing to ensure interoperability evaluation needs are adequately addressed. This will allow JITC to leverage planned testing for the system's Joint Interoperability Certification process and minimize additional testing.

(f) Coordination and scheduling considerations should be negotiated by the PMO/Sponsor and designated test organization with proponents of interfacing systems (e.g., the certification process requires interfacing systems be available during interoperability testing).

(2) Interoperability Certification Evaluation Plan (ICEP). An optional JITC test and certification strategy, an ICEP identifies a series of test events at which data collection in support of interoperability evaluation is planned. It is normally developed in coordination with the PMO/Sponsor using the TEMP to identify suitable events for interoperability data collection. Also, it is used to coordinate development of data collection requirements and procedures with the PMO/Sponsor and associated designated test organizations. An ICEP establishes an overall plan on how a system will be evaluated. An ICEP will usually point to individual test plans for the details on testing component systems.

(3) Interoperability Test Plan (ITP). An ITP describes a system to be tested, test objectives, and detailed test procedures for an interoperability test. JITC develops an ITP when

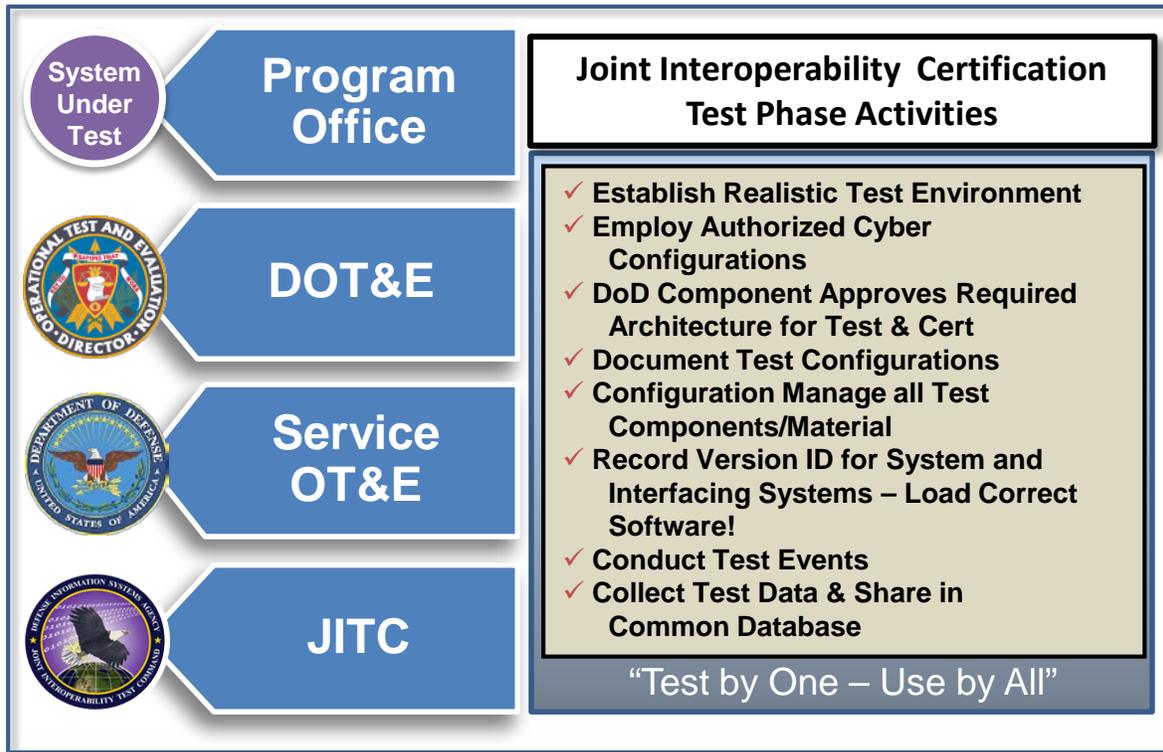
no previous or planned testing will produce the data needed to evaluate interoperability, where programmatic or other constraints preclude inclusion of suitable data collection in planned testing. ITPs are written for individual test or data collection events. These plans detail the testing and data collection and analysis procedures that apply to that event. A variant of an ITP, 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).

(4) Operational Test Readiness Review (OTRR) Interoperability Statement. JITC evaluates whether a system is ready for OT&E from an interoperability perspective and provides an appropriate recommendation with regard to proceeding to OT&E based on that evaluation. The statement addresses:

- (a) Status of IT interoperability and standards conformance issues.
- (b) Confirmation that all required developmental testing relating to IT interoperability has been successfully completed and passed.
- (c) Details of any interoperability issues that must be resolved before the start of OT&E.
  - i. Determining Required Resources for Test & Certification. To be cost effective, the PMO/Sponsor must integrate the evaluation of a system's interoperability into the overall test, evaluation, and development processes as early in the developmental lifecycle as possible. The PMO/Sponsor and JITC shall jointly establish a strategy for evaluating interoperability requirements in the most efficient and cost effective manner, in an operationally realistic environment, including cybersecurity considerations. This evaluation strategy identifies the data necessary to support an interoperability evaluation, as well as indicates the test events/environments planned to produce that data.

#### 4. Joint Interoperability Test and Certification

During testing, a variety of structured events surround successful interoperability test and certification. Figure 4-1 summarizes the range of activities that typically occur during this key phase.



**Figure 4-1. Representative T&E Test Phase Activities**

##### a. Test Conduct

(1) The PMO/Sponsor is responsible for providing the data for interoperability evaluation and follows the plans developed during pre-test activities. While test data is an essential element for analysis, it is critical to pay sufficient attention to the basic tenets of testing. The test environment must be properly configured, including cybersecurity controls, and the correct version of the software and operating system must be loaded and configuration managed. Version identification is equally important, not merely for the system under test, but for interfacing systems. Documenting this information during testing is critical to a successful test, as often it is unavailable afterwards. Results – good or bad – are meaningless if there are uncertainties about how components were configured (both hardware and software) and what version of a system interoperated with what interfacing system versions.

(2) Integrated T&E (“Test by one, use by all.”) is encouraged to leverage test events to make the most effective and efficient use of scarce resources. However, integrated testing does not result in a single test event that answers all questions. Nor does integrated testing mean that a single organization performs all of the evaluation and reporting. What integrated testing does

do is allow independent evaluators to share the data from a test, with each performing the appropriate analysis to address their specific test issues and measures. For example, data to support interoperability evaluation should include results from OT testing, with JITC using the shared test data to provide Joint Interoperability Certification. Maximum benefit can be obtained from integrated T&E if developers and test teams collaborate on test planning and execution, and establish common databases to share data.

b. Initial Joint Interoperability Test and Certification Process

(1) Joint interoperability certification is based on test and evaluation of production representative systems (hardware/software) in as realistic an operational joint environment as practicable, including use of authorized cybersecurity configurations.

(2) Joint interoperability certifications provide input to the Milestone Decision Authority (MDA) (post Milestone C), or cognizant fielding authority, for a fielding decision. The Joint Interoperability Certification does not satisfy any other certifications that may be required (e.g., spectrum certifications, network manager approval to connect, and/or other validations/approvals).

(3) A Joint Interoperability Assessment provides preliminary interoperability status. This can be particularly useful in cases where requirements documents have not been finalized, high risk areas warranting early feedback, etc.

(4) JITC shall evaluate interoperability test results using a variety of resources including:

(a) Joint Staff-certified NR KPP and information prescribed in Section 11 as required for Joint Interoperability Certification. Issues with NR KPP requirements shall be raised with the Joint Staff for resolution.

(b) Mission-related information.

(c) Data from DT&E, OT&E, acceptance testing, exercise venues, or other demonstrations, consistent with any approved TEMP, or other interoperability data collection requirements. The potential operational impacts of all unresolved interoperability deficiencies noted during evaluation must be determined by the appropriate users or user representatives and be reported by JITC in any resulting certification.

(d) Interoperability test and evaluation criteria, measures, and requirements established by intelligence functional managers (e.g., NGA and NSA).

(5) Pre-test activities by JITC include verifying that system and network configurations used in testing are representative of a realistic operational environment, to include cybersecurity (formerly IA) characteristics.

(6) JITC has the capability to evaluate cybersecurity (or portions of cybersecurity requirements) when requested, and shall document any known cybersecurity status as part of reporting the interoperability status. However, some portions of cybersecurity requirements may not be (or able to be) assessed until after JITC interoperability certification, and as such cannot

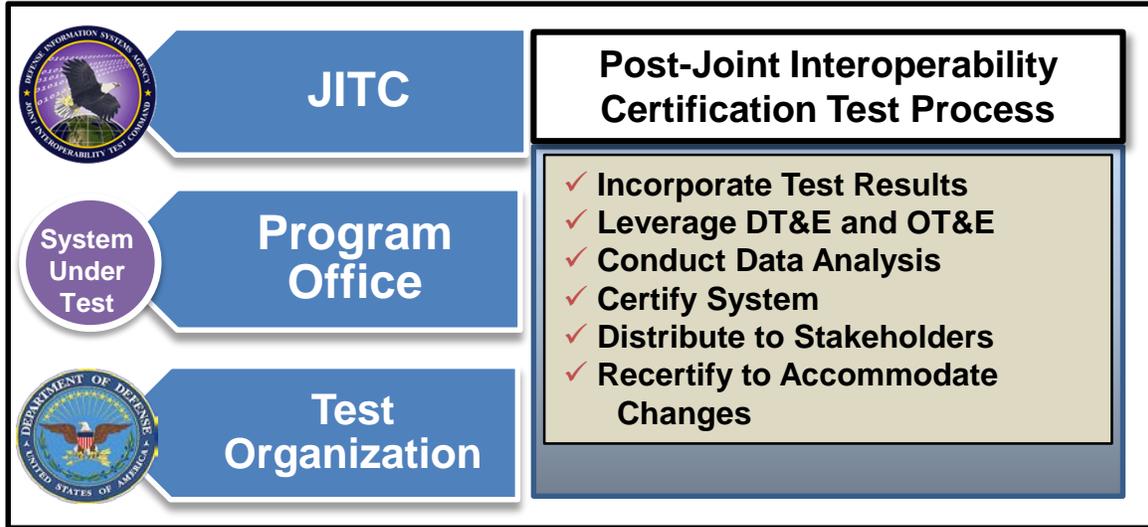
be reported in the certification. Significant cybersecurity issues shall be reported in the Joint Interoperability Certification for systems with an NR KPP, and any deficiency which has a potential critical operational impact, may result in JITC being unable to certify the system.

(7) JITC shall also determine whether any necessary standards conformance certifications have been obtained. This is usually accomplished in DT&E venues because of the nature of standards conformance testing. JITC shall consider test results from previous standards conformance testing conducted during system development.

(8) JITC evaluation of interoperability is not merely an assessment of functional performance, but of the effectiveness of information exchange within the operational environment. Interoperability of a system depends on many factors that the PMO/Sponsor may influence, but not directly control. Interfacing systems, operational network access and loading, atmospheric conditions, satellite transponder or channel availability, ambient electromagnetic conditions, etc., are among the factors that may impact interoperability, and the resulting certification, independent of the performance of the system under test. For this reason, unlike most other forms of testing, deficiencies in interoperability may occur that are not attributable to the system being tested, but may influence the interoperability evaluation and subsequent certification. If a system has no requirement to operate under some set of conditions, failing to do so may be noted but shall not be considered as an interoperability failure. For example, atmospheric dust in excess of specified requirements prevents closing of a link.

**5. Post-Joint Interoperability Test and Certification Procedures**

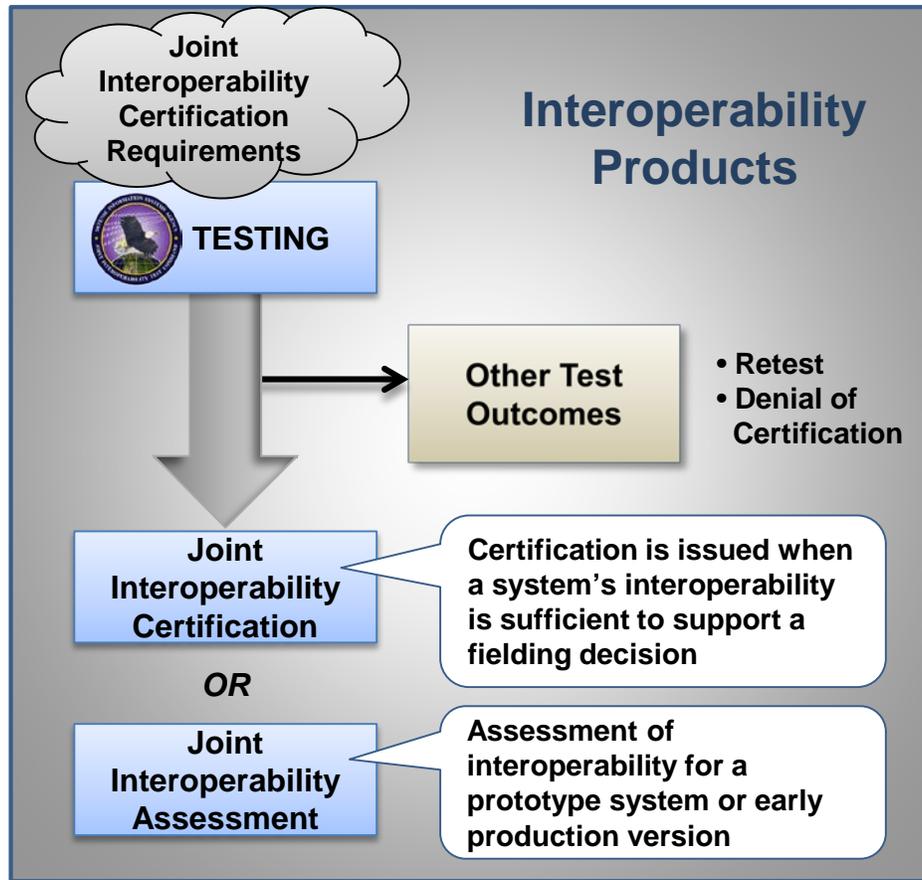
This section describes the principal post-test actions required by stakeholders to accomplish interoperability certification. The processes summarized in Figure 5-1 below typify the range of post-test activities that routinely occur during this final phase of the process.



**Figure 5-1. T&E Post-Test Activities**

a. Reporting. JITC shall provide interoperability test documentation to the PMO/Sponsor, with Joint Interoperability Certifications being sent to ISG members, with a delivery goal of 60 calendar days from the end of testing and receipt of all required test information. The PMO/Sponsor and designated test organization should provide all relevant reports, system/test configuration information (including for interfacing systems), test data, trouble reports, analysis of any discrepancies, etc., in a timely fashion. All parties should keep in mind the JITC processing time required after receipt of test information – the sooner organizations provide the required information, the sooner they can receive their certification.

b. Certification Products. A family of reporting products has been introduced to document test and certification activities. Figure 5-2 and the paragraphs below describe the interoperability T&E products and possible outcomes resulting from successful or failed testing. In addition, see Figure 5-3 for a summary of current reports.



**Figure 5-2. Interoperability T&E Products**

(1) Joint Interoperability Certification. JITC issues a Joint Interoperability Certification when a system has been evaluated against its joint interoperability requirements and the system's interoperability status is sufficient to support a fielding decision.

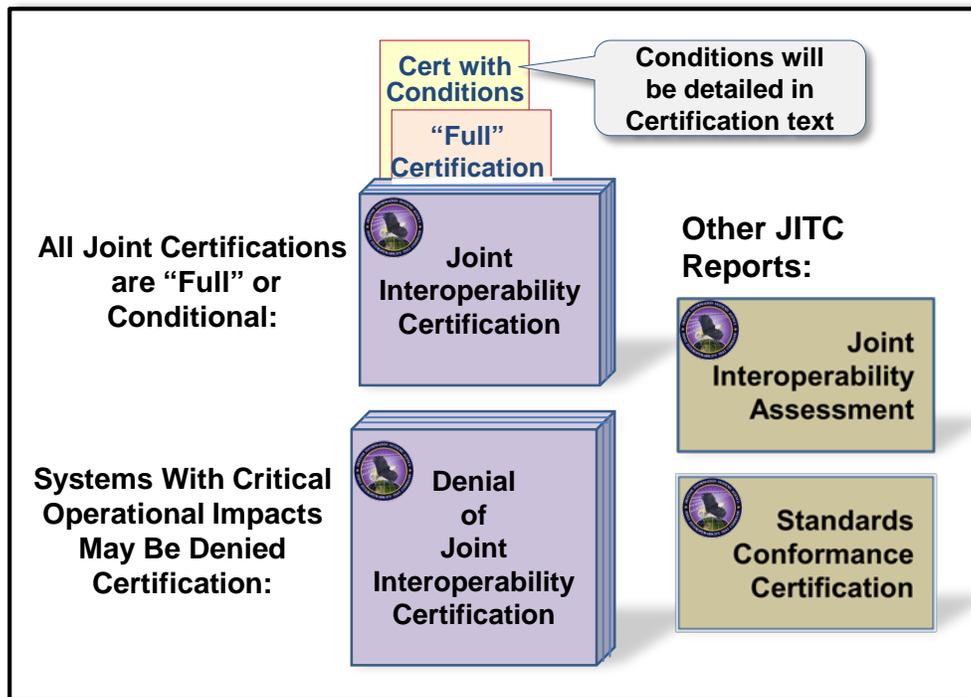
(a) Joint Interoperability Certification with Conditions. When appropriate, JITC may issue certifications with conditions (limitations) when only subsets of the requirements are met. Conditional certifications provide the system/interface interoperability status for cases where useful capabilities are provided, despite not meeting all threshold requirements, and there are no expected critical operational impacts or adverse effects on the joint interoperability environment. Conditions to certification are based on assessment of operational impact and limit the operational use of the system to only those functions and interfaces that were adequately demonstrated. A PMO/Sponsor must submit the system for additional interoperability testing in order to have these conditions (restrictions) removed.

(b) Certification for Systems Developed in Increments. JITC may issue a Joint Interoperability Certification for each increment of a system. All joint interoperability requirements for a given increment shall be used for evaluation and reporting the status, not just those requirements implemented. If requirements for the system were not delineated by increment (phase, spiral, block, etc.) in the Joint Staff certified NR KPP, all requirements will

apply to the current increment. Changing the increment or criticality of a requirement is a modification to the requirements that may require Joint Staff recertification.

(2) Denial of Joint Interoperability Certification. When interoperability deficiencies are identified that critically impact joint interoperability or joint mission accomplishment, JITC may issue a denial of certification memorandum. This provides CIOs, Joint Staff, MDAs, and PMOs notification of problems that warrant immediate attention.

(3) Joint Interoperability Assessment. A joint interoperability assessment can be issued to assess a system’s interoperability strengths and weaknesses. Assessments are typically provided when a certification is not appropriate (i.e., when there is no certified NR KPP, but the PMO requests an early assessment). Interoperability assessments can be conducted during DT&E or OT&E events, acceptance testing, interoperability exercises, or other test venues. The PMO/Sponsor shall coordinate with and fund JITC to establish the exact assessment needs and identify documentation requirements.



**Figure 5-3. JITC Interoperability Reports**

(4) Revocation and Reissuance of Joint Interoperability Certifications. Joint interoperability certifications may be rescinded, revoked, or reissued by JITC. This would occur if an issue has been detected due to a change between a fielded configuration and a tested configuration. This would include a change in data exchange partners as well as a change in system configuration, or any interoperability deficiency discovered post test. All organizations that received the original certification notice shall be notified of changes in interoperability certification status.

(5) Certification Extension Process. JITC grants a certification extension to extend coverage of an existing certification to include modifications not affecting interoperability made before the certification has expired. Since certifications are given for specific version numbers, a certification extension would be granted to expand the certification to cover a follow-on version that does not change the original certification – just a new version. The “extended” certification has the same expiration date as the existing certification. The PMO/Sponsor will follow the guidance for "Certification is Scheduled to Expire" in cases where only the period of certification needs to be renewed and no additional testing is required. PMOs/Sponsors will contact their JITC AO to establish required information and cost. At a minimum, certification extension requests must include:

(a) A written statement by the PMO/Sponsor (submitted with the request package) that the modification does not affect interoperability.

(b) Sufficient information for JITC to independently determine the impact of change.

c. Recertification Process. Interoperability can degrade over time. Changes to standards, interfacing systems, and cumulative minor upgrades impact the ability of systems to interoperate and must be carefully monitored throughout the system’s lifecycle. Joint interoperability certifications for a specific increment must be renewed periodically or when system, operating environment, or requirements changes occur that affect joint interoperability. The PMO/Sponsor is responsible for notifying JITC regarding incremental upgrades and other changes affecting interoperability. Coordination with JITC will identify funding requirements for test and certification. The PMO/Sponsor should be aware that the NR KPP may need to be recertified.

(1) Recertification Criteria. Recertification is required when:

(a) The Joint Interoperability Certification is revoked (e.g., critical operational deficiencies are reported after fielding in a given environment).

(b) The system certification expires at the end of 4 years.

(c) Changes to the interoperability environment, including the system, interfacing systems, system requirements have been made or are anticipated to occur (e.g., new increment to be fielded, or other materiel changes) impact interoperability.

(d) A new increment is released, materiel changes (e.g., hardware or software modifications, including firmware) occur to the system that affect interoperability, or materiel changes occur to interfacing systems that affect interoperability. Also, substantive revisions in mandated DISR standards may constitute a change in the interoperability environment that results in a need for recertification.

(e) Non-materiel changes (i.e., Doctrine, Organization, Training, Leadership and education, Personnel, and Facilities – Policy (DOTLPF-P)) occur that affect joint interoperability.

(2) Recertification Procedures. The PMO/Sponsor shall perform the following activities depending upon the specific situation.

(a) *If certification is revoked:*

1. Make changes to the system, the requirements, or both, to correct discrepancies or operational interoperability issues that were responsible for the revocation.

2. Obtain new certification by following the processes outlined in this guide for attaining an initial certification.

(b) *If certification is scheduled to expire and PMO/Sponsor desires recertification without additional testing (procedures summarized in Figure 5-4):*

1. The PMO/Sponsor should contact JITC through the applicable DoD Component ISG representative early enough to allow sufficient time for the recertification process to be accomplished. It is recommended this process be started as early as 12 months but no later than 6 months prior to certification expiration.

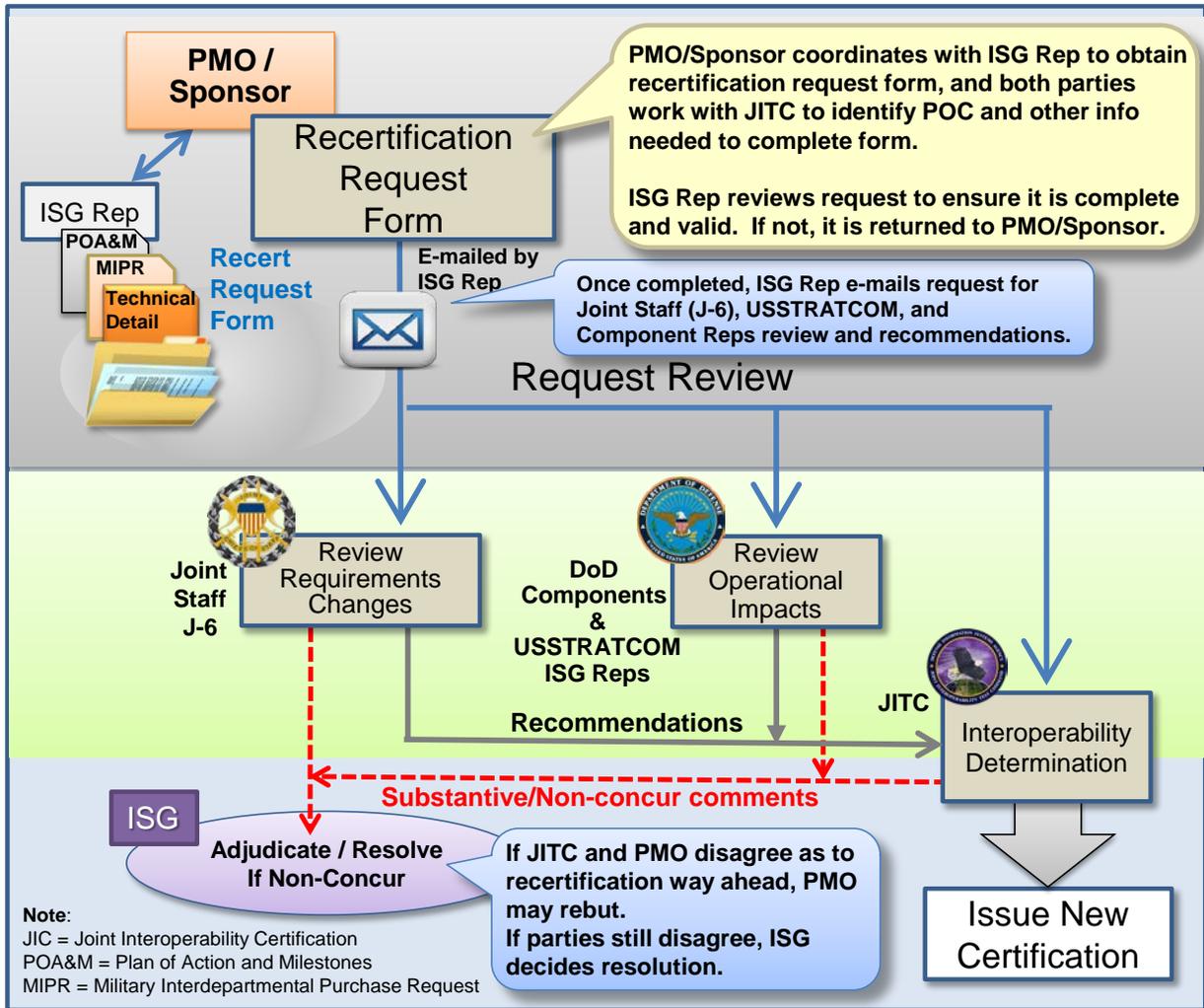
2. The ISG representative will provide the PMO/Sponsor with the recertification request form, which identifies required technical and funding information. The PMO/Sponsor will work with the respective JITC Action Officer (AO) to complete the recertification request form, which can be found on the ISG Resource website, along with a listing of the ISG representatives, at: <http://jitic.fhu.disa.mil/projects/igsite/index.aspx>.

3. The PMO's/Sponsor's recertification request will provide written verification that the interoperability environment (including the system and interfacing systems) and joint interoperability requirements (in certified NR KPP and approved architectures) have been reviewed and have not changed such that they affect interoperability. Operation of the system has been verified through exercises, operational use, and deployments (i.e., all moderate or greater operational impacts identified as conditions in the existing Joint Interoperability Certification). If changes have occurred, the written verification will outline the deltas from the prior certified version.

4. The PMO/Sponsor will send the recertification request to the applicable DoD Component ISG representative for review and concurrence.

5. ISG representatives shall ensure requests are complete and valid. If the request is not complete and valid, the ISG representative shall return it to the PMO/Sponsor.

6. Once completed and validated by the ISG representative, the ISG representative shall send the request via e-mail to JITC ([disa.huachuca.jt.mbx.jitc-iop-recertification-requests@mail.mil](mailto:disa.huachuca.jt.mbx.jitc-iop-recertification-requests@mail.mil)), Joint Staff J-6, U.S. Strategic Command (USSTRATCOM), and other Components for recommendation.



**Figure 5-4. Recertification Request Procedures Summary**

7. Joint Staff J-6, USSTRATCOM, and other Components will provide recommendation to requesting ISG representative, JITC, Joint Staff J-6, USSTRATCOM, and other Components within 30 days of the receipt of all required information. Joint Staff J-6, will verify that requirements (certified NR KPP and approved architectures) are current and changes (from the last certification), if any, do not impact joint interoperability. USSTRATCOM, in coordination with other Components, will review the system for any new operational impacts in the field.

8. JITC shall review all requests and provide an interoperability determination to the PMO/Sponsor and ISG representative within 30 days of receiving recommendations from Joint Staff J-6, USSTRATCOM, and other Components.

9. JITC may issue a new certification (the goal being to do so within 30 days of making the determination) without additional interoperability testing if the joint interoperability requirements, system configuration, and operational environment of the system are current and

have not changed in a manner that impacts joint interoperability, and no new operational impacts have been identified.

10. Alternatively, if JITC determines that changes to the system or its environment have impacted interoperability, or if the interoperability requirements have changed, JITC will determine whether a desktop assessment will suffice to issue a new certification or if a new joint interoperability evaluation/test is required. Substantive revisions in mandated DISR standards constitute a change in the interoperability environment that can result in a need for recertification. The PMO/Sponsor will coordinate with JITC to integrate Joint Interoperability Certification requirements into the program's existing test activities (e.g., DT&E, OT&E, acceptance testing, exercise venues, or other demonstrations). If that is not feasible, the PMO/Sponsor will initiate planning for separate JITC test and certification.

11. In the case of disagreement between JITC and the PMO/Sponsor regarding the determination for recertification way ahead, the PMO/Sponsor will have the opportunity to provide a rebuttal to JITC.

12. If after the PMO/Sponsor rebuttal is submitted and reviewed there is still a disagreement whether a recertification test is required, the matter will be brought to the ISG for resolution. The ISG decision will be provided in writing to the PMO/Sponsor and JITC.

13. The PMO/Sponsor recertification request identifies the information and documentation needed for timely procurement of JITC support in a "Recertification Request" Plan of Action and Milestones (POA&M) and Military Interdepartmental Purchase Request (MIPR). The Recertification Request POA&M contains standardized verbiage and cost for JITC to review the recertification package and issue a Joint Interoperability Certification memorandum if all criteria are met to issue a certification without additional testing (or analyzing additional test results) in accordance with this section.

14. JITC supports recertification requests as a fee for service. The recertification timeline starts when a complete recertification request, with funding, is received. The JITC AO will coordinate with the PMO/Sponsor to return unused funding.

***(c) If changes to the interoperability environment (including the system, interfacing systems, and system requirements) have been made or are anticipated to occur (e.g., new increment to be fielded, or other materiel changes) that could possibly impact interoperability:***

1. The PMO/Sponsor will coordinate with JITC to determine whether the changes have impacted, or may be expected to impact, interoperability of the system as documented through previous certification or assessment efforts.

2. If changes have been made to the system, or its requirements, and no impact to interoperability has occurred or is anticipated, JITC should consider issuing an extension to the existing certification (see below).

3. If the changes are to the interoperability environment or interfacing systems, and no impact has occurred or is expected, no action is required beyond the initial JITC evaluation of the changes. JITC will notify the PMO/Sponsor and respective ISG representative of its determination of “no further action required,” and will document this finding in the System Tracking Program (STP).

4. If interoperability is or will be impacted, the PMO/Sponsor and JITC will initiate planning to collect data from past or planned tests, exercises, or operational venues, or to plan test events to obtain such data. Such data is essential to evaluate interoperability of the changes to support a new certification. If not all changes can be tested, such as an update to an interfacing system, it may be appropriate to obtain a Joint Interoperability Certification with Conditions.

5. When there is disagreement between the PMO/Sponsor and JITC as to the need for additional testing, the matter will be brought to the ISG for resolution. The ISG decision will be provided in writing to the PMO/Sponsor and JITC.

**(d) *If DOTLPF-P changes related to the previously certified system have occurred or are anticipated:***

1. The PMO/Sponsor will coordinate with JITC to determine whether the changes have impacted, or are anticipated to impact, interoperability of the system as documented through previous certification or assessment efforts.

a. If impacts to interoperability have not occurred or are not anticipated, no further action is required beyond the initial JITC evaluation of the changes. JITC will notify the PMO/Sponsor and respective ISG representative of its determination of “no further action required,” and will document this finding in the STP.

b. If impacts to interoperability have occurred or are anticipated, the PMO/Sponsor and JITC shall initiate planning to collect data from past or planned tests, exercises, or operational venues with which to evaluate interoperability of the system within the changed environment for a new certification.

2. When there is disagreement between the PMO/Sponsor and JITC as to the need for additional testing, the matter will be brought to the ISG for resolution. The ISG decision will be provided in writing to the PMO/Sponsor and JITC.

## **6. Interim Certificate To Operate (ICTO) Procedures**

An ICTO permits a system to be fielded for operational use without a Joint Interoperability Certification. An ICTO is the authority to operate new systems for a limited time (less than one year) to allow operational use while pursuing Joint Interoperability Certification per reference (a).

### a. ICTO Process

(1) The DoD CIO, in coordination with the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) and the Chairman of the Joint Chiefs of Staff (CJCS), through the ISG, adjudicates and grants ICTOs for systems with joint, multinational, and interagency interoperability requirements. The DoD Component heads grant ICTOs for all other systems. ICTOs may only be granted when the system is undergoing interoperability certification testing and there is a documented need to operate the system before completing interoperability test and certification.

(2) Per reference (a), the DoD CIO shall only grant an ICTO when:

(a) The operational chain of command and the CJCS have validated an urgent operational need requiring fielding of the IT or NSS prior to Joint Interoperability Certification.

(b) Defense Information Systems Agency (DISA) (JITC) or other DoD Component test labs are unable to assess all required interfaces for the IT or NSS undergoing joint interoperability testing.

(c) In either case, the PMO/Sponsor of the IT or NSS must engage with JITC and pursue full Joint Interoperability Certification.

(3) Factors impacting ICTO decision include:

(a) Urgent operational need.

(b) Existing test results/artifacts.

(c) Assessed impact on the operational systems/networks.

(d) Plan of action to complete Joint Interoperability Certification.

(e) Have no pre-existing critical interoperability deficiencies identified by JITC.

(4) ICTO requests must include recommendations from JITC, and must include sufficient information to substantiate the request.

(5) An ICTO is not appropriate for systems that fail to meet identified interoperability requirements during joint interoperability testing, and are not progressing towards a full Joint Interoperability Certification.

(6) An ICTO is not appropriate for fielded systems that do not have approved interoperability requirements. These systems can pursue Joint Interoperability Certification or request a "Waiver to Policy" (see Section 7) to continue operation. Fielded systems validated through a Joint Urgent Operational Need or Joint Emergent Operational Need, as defined in reference (f), do not require an ICTO, Joint Interoperability Certification, or Waiver to Policy unless the capability meets the threshold for a Major Defense Acquisition Program or Major Automated Information System.

(7) JITC's ISG Resource website contains additional instructions regarding the ICTO procedures, templates, and ISG Points-of-Contact (POCs):  
<http://jitic.fhu.disa.mil/projects/isgsite/index.aspx>.

(8) JITC's STP (reference (j)) contains all ICTO letters and status information under the drop down menu "Reports/Document Reports/ICTO Report" section (refer to <https://stp.fhu.disa.mil>).

(9) Operational systems, for which ICTO requests have expired without action by the PMO/Sponsor or have been disapproved by the ISG, shall be placed on the OARL for monitoring and tracking purposes.

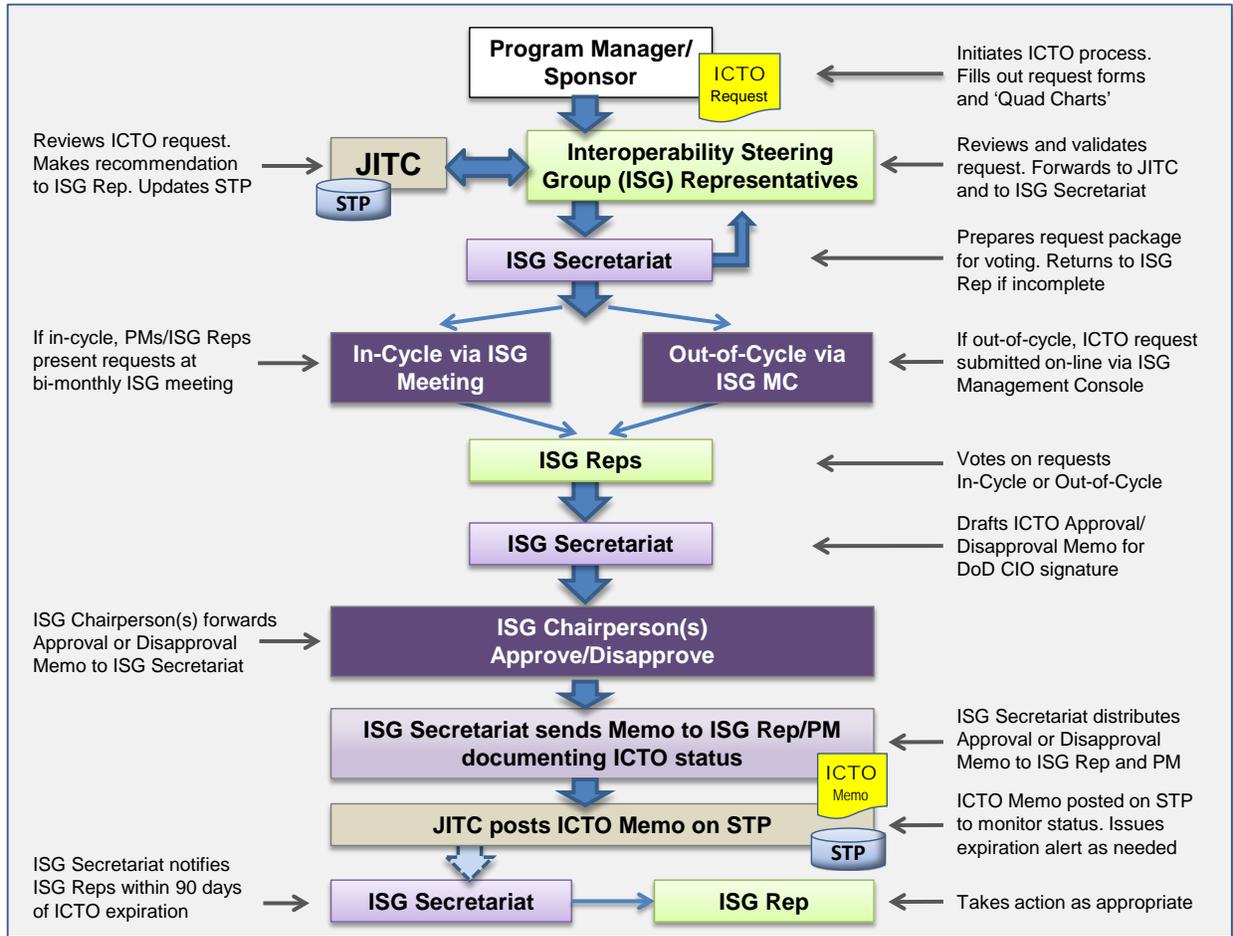
(10) Total duration of an ICTO shall normally not exceed one (1) year; however, the ISG may consider an extension if, and only if, progress is made towards interoperability certification. Each request shall be reviewed on a case-by-case basis.

b. ICTO Procedures. Figure 6-1 depicts the procedures for processing ICTO requests.

(1) The PMO/Sponsor completes an ICTO request; JITC cannot submit requests for ICTOs. The JITC ISG Resource website contains templates and forms for ICTO requests: <http://jitic.fhu.disa.mil/projects/isgsite/ictoreqs.aspx>. JITC will provide a recommendation for approval or disapproval of the ICTO request.

(a) When requesting an "initial" ICTO, the PMO/Sponsor must submit the requisite ICTO Quad Chart and Systems Viewpoint (SV)-1 diagram through their respective Component ISG representative. PMOs/Sponsors submitting initial ICTO requests will work with the respective ISG representative to initiate contact with JITC; JITC will then identify an AO.

(b) When requesting an ICTO "extension," the PMO/Sponsor is required to submit a Quad Chart and SV-1. The ISG shall not grant extension requests for upgraded capabilities. If a specified version of the system has been replaced with another (e.g., Version 7.1 replaced by Version 7.2), a new "initial" ICTO should be requested. The ISG shall track the new system version ICTO and its complete history throughout previous version ICTOs.



**Figure 6-1. Procedures for Processing ICTO Requests**

(2) The PMO/Sponsor shall send the ICTO request to the respective ISG representative. The ISG POC List on JITC’s ISG Resource website contains a complete list of ISG representatives and contact information: <http://jitic.fhu.disa.mil/projects/igsite/poclist.aspx>.

(3) The ISG representative shall review and validate the ICTO request. If the ISG representative concurs with the request, the ISG representative shall forward the request to the JITC AO. If the ISG representative does not concur, the request shall be sent back to the PMO/Sponsor for corrective action. Only ISG representatives can submit ICTO requests to the JITC AO.

(4) The JITC AO shall review the ICTO request and research the system to determine if an ICTO should be recommended. The JITC AO shall use JITC’s STP to determine previous testing and certification status.

(5) The JITC AO shall coordinate with respective JITC POCs if the ICTO topic crosses other Divisions/Portfolios, or if additional expertise is required to review the ICTO request.

(6) JITC AO input shall be provided via the web-based ISG Management Console (located at <http://jitic.fhu.disa.mil/projects/isgsite/index.aspx>).

(7) If the mandatory sections of the ICTO Quad Chart are not filled out properly, the request shall be returned to the ISG representative for corrective action. Once the forms/charts have been completed, the ISG representative shall send the ICTO request, including JITC input and recommendation, to the ISG Secretariat. The ISG Secretariat shall coordinate with the JITC AO regarding outstanding programmatic issues, interoperability testing status, and recommendations pertaining to the ICTO request.

(8) If processed In-Cycle, the ICTO request shall be added to the next scheduled meeting agenda. JITC AO's input is required for the ISG voting members to determine if a system obtains an ICTO during the ISG meeting.

(9) If processed Out-of-Cycle (OOC), the ISG representative shall forward the ICTO request to the ISG Secretariat for input in the ISG Management Console. The tool will send an e-mail notification to the appropriate JITC AO for comments/recommendations. Once comments/recommendations are received, the ISG members will receive an e-mail notification advising them that a request is ready for polling. The following rules apply to those requests forwarded for OOC processing:

(a) All initial ICTO requests for OOC processing shall be approved for a maximum of six (6) months.

(b) PMOs/Sponsors submitting initial ICTO requests for OOC processing must brief the panel at the next scheduled ISG meeting if significant progress has not been made towards Joint Interoperability Certification.

(c) PMOs/Sponsors that submit initial ICTOs for OOC processing must provide rationale detailing the urgency of the request (e.g., urgent deployment schedule). This will assist in determining the criticality of the request and allow members to make an informed decision.

(d) ISG members should complete their review and provide input within five (5) business days after receipt of the e-mail notification.

(10) The ISG Secretariat shall forward signed/approved ICTO letters to the PMO/Sponsor and the ISG members documenting the ICTO status.

(11) JITC shall post all ICTO letters (including disapproval letters) in the STP and monitor the expiration dates. The STP will generate an "Expiring ICTO Alert." This alert provides a list of ICTOs that have expired or will expire within 90 days.

(12) When an ICTO has expired, or is within 90 days of expiration, the ISG Secretariat shall notify the ISG representative that action is needed. It is the responsibility of the ISG representatives to ensure resolution of all expiring or expired ICTOs.

## **7. Waivers to Policy**

a. DoD Component heads may approve requests to waive the requirement for interoperability testing or interoperability certification of DoD Component-unique IT (i.e., no joint, multinational, or interagency interoperability requirements). Upon approval, the DoD Component shall provide the DoD CIO with copies of the waiver request and approval memorandums.

b. For other (not Component-unique) IT, DoD joint interoperability policy may be waived using the procedures below. The waiver process will identify low risk systems connected to DoD's network infrastructure and increase visibility of systems supporting the warfighter. These waivers do not apply to other DoD CIO requirements, such as system survivability, cybersecurity, or ISP development. Waivers may be either permanent or have an expiration date, at the discretion of the DoD CIO.

### **c. Waiver Process**

(1) The DoD CIO, in coordination with the USD(AT&L), the Director, Operational Test and Evaluation (DOT&E), and the CJCS, shall consider policy waivers only if one of the following criteria are met:

(a) When the operational chain of command and the CJCS have validated an urgent operational need.

(b) To accommodate the introduction of new or emerging technology pilot programs that have been coordinated with, and validated by, the Office of the Secretary of Defense (OSD) or DoD Component head concerned.

(c) When the requesting DoD Component can demonstrate that the cost of complying with the policy outweighs the benefit to DoD.

(2) Statutory requirements may be waived only if the statute specifically provides for doing so.

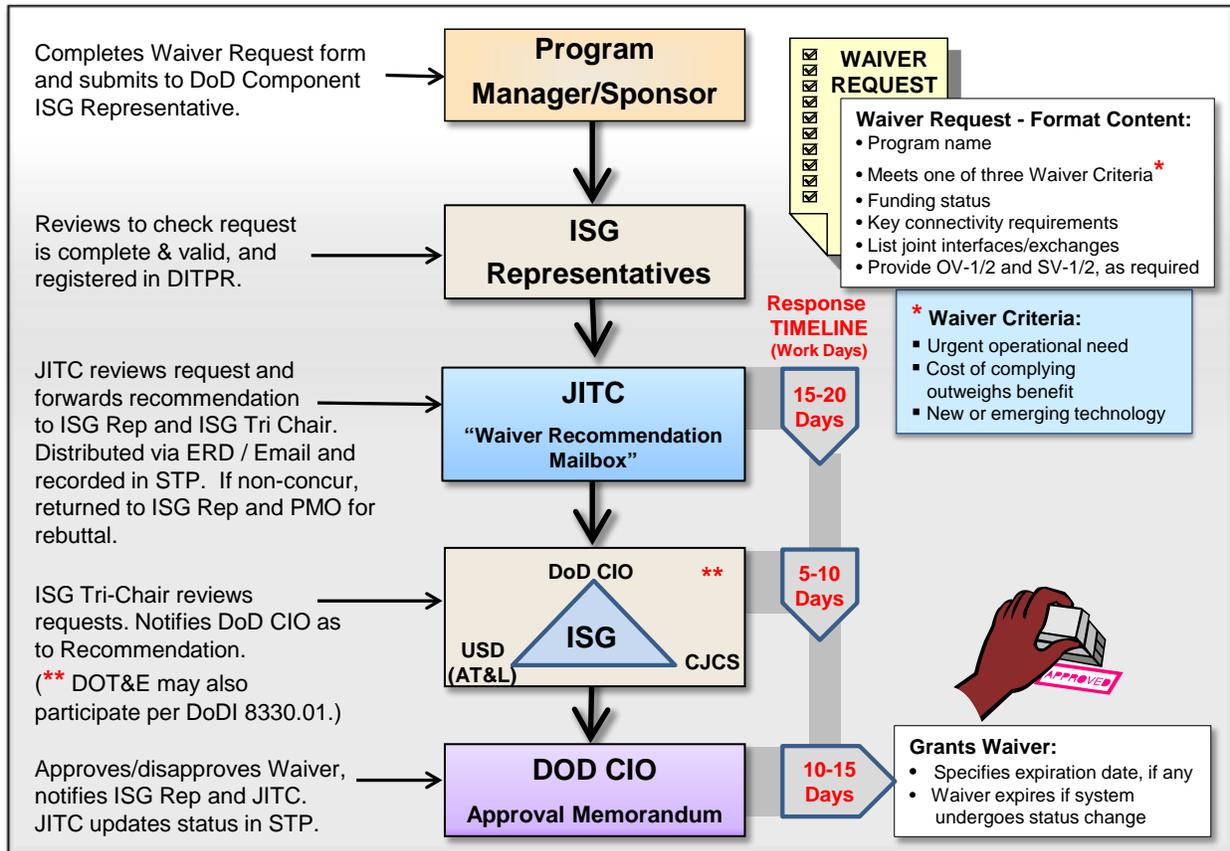
(3) The DoD CIO, in coordination with the USD(AT&L) and the CJCS, grants waivers to policy for systems with joint, multinational, and interagency interoperability requirements. The DoD Component heads grant waivers to policy for all other systems.

(4) Each time a Connection Approval Office (CAO) decision is made, including renewals, the CAO must verify that any ICTOs or waivers have not expired.

(5) JITC shall review and provide a recommendation on the waiver request to the DoD CIO, assessing risk to the network and DoD operations.

(6) The final decision on the waiver request shall be made by the DoD CIO. If approved, the system shall be waived from the interoperability policy requirements cited in the request.

d. Waiver Procedures. The PMO/Sponsor is responsible for generating the waiver request, using the request form available at: <http://jitic.fhu.disa.mil/projects/isgsite/testwaiver.aspx>. Figure 7-1 summarizes these procedures.



**Figure 7-1. Waiver to Policy Process**

(1) The request shall include: the program’s name, the portion of the policy requested to be waived, proof of meeting one or more of the waiver criteria, the rationale for the waiver, the capability the program provides, the existing program funding, the identification of key connectivity requirements, joint interfaces/joint information exchanges, and OV-1/2 and SV-1/2 architecture data, as needed.

(2) Requests should be sent to the applicable DoD Component ISG representative for review and concurrence. Refer to: <http://jitic.fhu.disa.mil/projects/isgsite/index.aspx> for a listing of the ISG representatives.

(3) ISG representatives shall ensure requests are complete and valid, to include verifying the system is registered in the DoD Information Technology Portfolio Repository (DITPR). If the request is not complete and valid, the ISG representative shall return it to the PMO/Sponsor.

(4) Once completed and validated by the ISG representative, the ISG representative shall send the request via e-mail to the JITC waiver recommendation mailbox ([disa.huachuca.jitic.mbx.waiver-recommendation@mail.mil](mailto:disa.huachuca.jitic.mbx.waiver-recommendation@mail.mil)).

(5) JITC shall review all waiver requests received in the JITC waiver recommendation mailbox and provide a recommendation to the ISG representative, Joint Staff, USD(AT&L), and DoD CIO. The goal is to provide waiver recommendations within 15 to 20 working days of receipt of all required information. The Joint Staff and USD(AT&L) shall have 5 to 10 working days to review and provide comments to the DoD CIO. Lack of a response by the deadline indicates concurrence with the JITC recommendation.

(a) For those systems identified by JITC as having no joint interfaces/information exchanges (i.e., DoD Component-unique), JITC will return the request to the requesting PMO/Sponsor and ISG representative for adjudication. No further action will be taken for these requests by JITC or the DoD CIO.

(b) In the case of a negative JITC recommendation, JITC will provide the recommendation to the requesting Component ISG representative and the PMO/Sponsor advising them of the opportunity to provide a rebuttal to the recommendation. The PMO/Sponsor through their ISG representative will provide e-mail notification to JITC of their intention to provide a rebuttal within 10 working days of receipt of JITC's recommendation. Rebuttals should be addressed to the DoD CIO and returned to JITC normally within 30 days. Lack of a response by the deadline indicates concurrence with the JITC recommendation.

(c) Rebuttals should address the points raised by JITC and any other mitigating circumstances supporting a waiver. JITC will submit the request, recommendation, other reference documentation, and rebuttal to the Joint Staff, USD(AT&L), and DoD CIO for review and determination.

(6) DoD CIO, coordinating with DOT&E as necessary, shall approve or disapprove the waiver within 10 to 15 working days of receipt of the waiver request package which included the request, JITC recommendation, and PMO/Sponsor rebuttal if provided. If approved, the system shall be waived from the interoperability requirements of the policy cited in the request form. If disapproved, the PMO/Sponsor will be expected to comply with the interoperability policy as written.

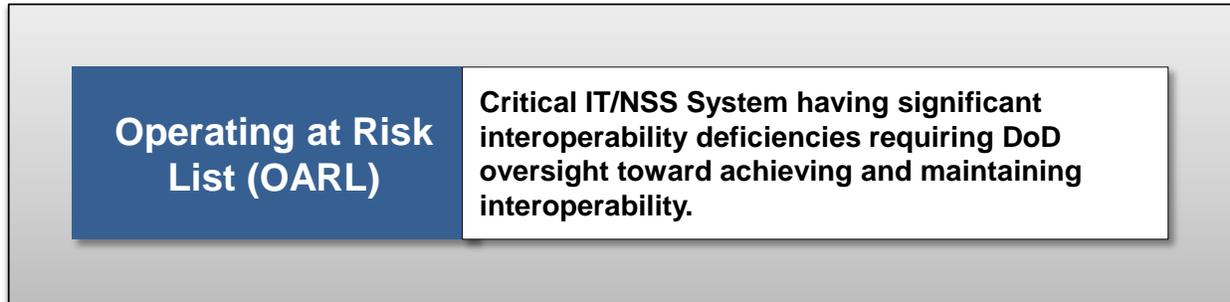
(7) A waiver to policy memorandum shall be issued following the initial e-mail approval verifying the system and version that has been granted a waiver, and noting any specific expiration date if one has been determined. The waiver expires if the specific version(s) of the system undergoes changes that affect interoperability. Status, recommendations, and memoranda for waiver requests are stored in the JITC STP at <https://stp.fhu.disa.mil>.

e. Rescission of Waivers. Policy waivers granted by the DoD CIO may be rescinded when circumstances warrant (e.g., when significant interoperability issues are identified). ISG members may provide recommendations for waiver rescissions to the ISG for consideration and recommendation with a final determination from the DoD CIO.

f. Unified Capabilities (UC) Waiver Requests. For waivers on UC components refer to DoDI 8100.04 (reference (d)).

## 8. Operating At Risk List (OARL)

a. Purpose. As described in Figure 8-1, systems with significant interoperability deficiencies, or not actively progressing toward certification, shall be placed on the OARL to ensure that sufficient attention is given to achieving and maintaining interoperability objectives.



**Figure 8-1. OARL Description**

b. Criteria. The OARL shall list all systems that have been denied an ICTO, are operating on a DoD network without a Joint Interoperability Certification, an ICTO, or a waiver to policy. Criteria for nominating programs to the OARL include, but are not limited to:

- (1) Joint interoperability deficiencies observed during operational exercises or real world operations.
- (2) Operational problems noted with Tactics, Techniques, and Procedures (TTPs), and training that impact joint interoperability for fielded (legacy) systems.
- (3) No plans for JITC Joint Interoperability Certification testing (when it is required).
- (4) Failed JITC Joint Interoperability Certification test and no plans for addressing the identified deficiencies.
- (5) Lack of JCIDS or test documentation.
- (6) Joint interoperability certification issues.
- (7) Unresolved issues from other activities concerned with interoperability (e.g., Overarching Integrated Product Teams (OIPs)).
- (8) Non-compliance with approved integrated architectures.
- (9) No plans to address interoperability test and evaluation criteria, measures, and requirements established by intelligence functional managers (e.g., NGA and NSA).
- (10) No plans to upgrade to changed mandated standards.

c. Nomination Process. The ISG may nominate systems for inclusion on the OARL. The DoD CIO is ultimately responsible for OARL determination.

d. Distribution. The OARL is updated, verified, and distributed at least quarterly to all DoD MDAs; affected system fielding authorities (for non-Acquisition Category (ACAT) IT); the CJCS; the DoD Component CIOs; the Commander, USSTRATCOM; and the DISA Connection Approval Office (CAO). The USD(AT&L) and DoD Component heads assist DISA to distribute the OARL to all DoD Component MDAs and affected systems' fielding authorities. It is available through the ISG Management Console at: <https://nit-jitc.nit.disa.mil/cgi/isg/oarl/oarl.aspx>.

(1) The DoD CIO will send a "Memorandum of Notification" to the responsible Service Component or Agency (ATTN: ISG Representative) upon the ISG'S initial decision to place a system on the OARL.

(2) On a recurring basis, the DoD CIO will send a "Quarterly Distribution of the Interoperability OARL" memo to all appropriate authorities and organizations (referenced in paragraph 8.d. above). This memo will include updated information pertaining to the joint interoperability status of all systems on the OARL.

e. Effect. Placement on the OARL may require the applicable PMO/Sponsor to appear before the ISG for status updates as required. If the ISG is not satisfied with the program's progress towards Joint Interoperability Certification, the ISG shall notify the appropriate MDA or affected fielding authority and the DISA CAO for further action.

f. Removal from the OARL. Programs shall be removed from the OARL if they successfully obtain an ICTO, receive a waiver to policy, achieve Joint Interoperability Certification, or the system is no longer in operational use. Final approval to remove a program from the OARL is the responsibility of the ISG Tri-Chairs. The DoD CIO will send a "Removal from the Interoperability OARL" memo to the respective Service/Agency ISG representative once the IT system has met the specified criteria.

## **9. Other Evaluations and Related Information**

a. **Standards Conformance Certification.** Standards Conformance Certifications are issued at the conclusion of technical testing against a standard/standards profile to describe the degree of conformance to that standard/profile (reference (k)). A standards conformance certification is the first step towards verifying interoperability, and is not sufficient by itself to support a fielding decision.

(1) Standards conformance testing will be conducted at multiple points in the development and integration process to ensure that a conformance certified system has not been corrupted by additional software or system integration activities.

(2) Additional testing beyond basic standards conformance may be required to determine conformance with multi-standard profiles, or compliance with additional technical requirements mandated by other policies or procedures.

(3) A system's standards profile must be monitored throughout the lifecycle to identify any necessary system updates and retesting requirements caused by changes in the interoperability environment.

b. **Foreign Systems Interoperability Evaluation.** A foreign system's interoperability evaluation is used to report interoperability testing results for foreign systems with U.S. defined requirements. Systems having such requirements must also have a DoD Component sponsor. A Joint Interoperability Certification or assessment can be received. Standards conformance certification may be performed for foreign systems that affect joint interoperability.

c. **Homeland Defense Systems Interoperability Evaluation.** Homeland Security-related systems may be tested by JITC when there are interfaces to DoD systems. As with any systems without Joint Staff NR KPP certification, JITC may not issue a Joint Interoperability Certification; however, JITC may provide joint interoperability assessments or standards conformance certifications.

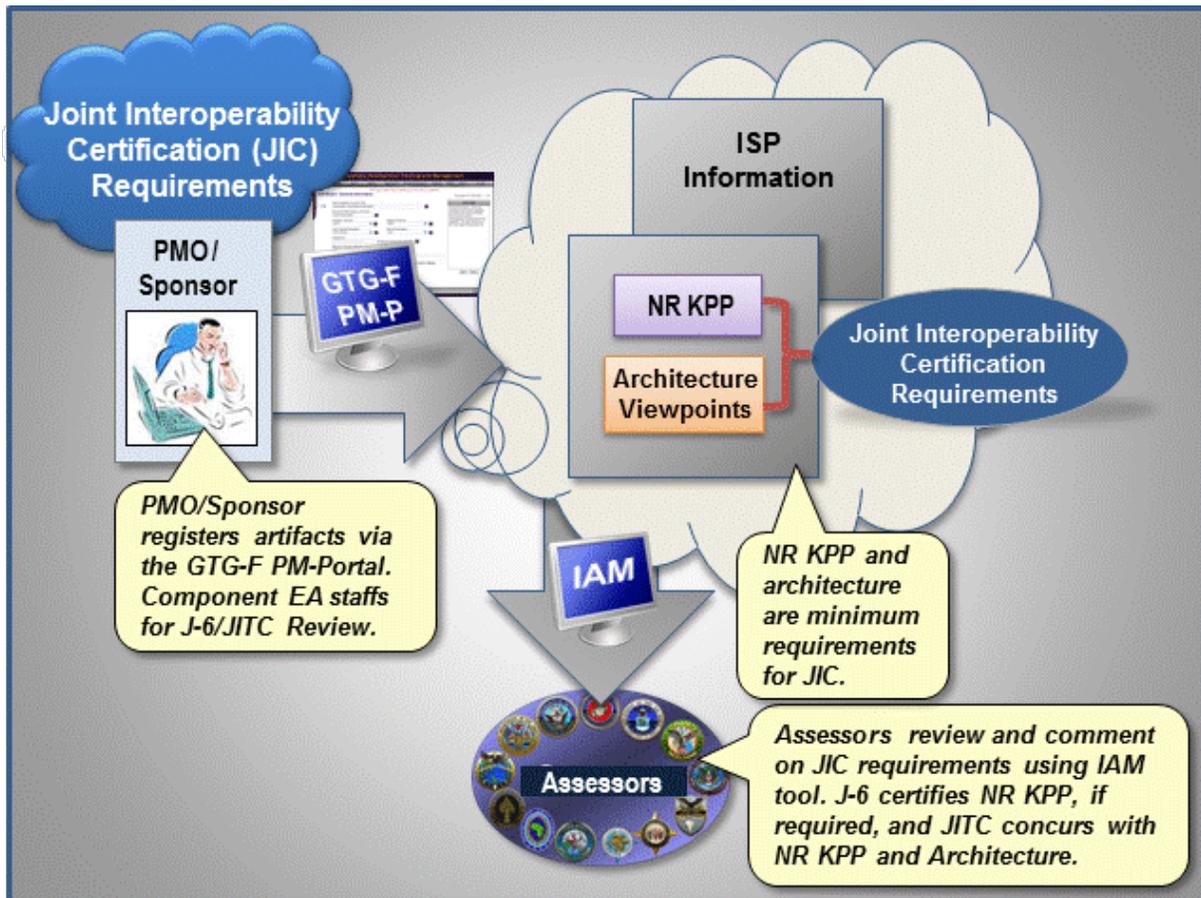
d. **Stimulators/Simulators and Training Systems.** Stimulators/simulators and training systems, separate from operational systems, may be used in the testing of systems and to support exercises. These devices may interface with other systems in the testing environment. Using these systems in a testing environment may not negate operationally realistic requirements. Potential differences and risks between the test environment and the operational environment will be considered and documented in accordance with applicable policy. Stimulator/simulator and training systems that only perform the function of simulation or training and only store, process, or exchange simulated (i.e., not operational) data do not require a Joint Interoperability Certification. However, they may require accreditation if used for testing, and are not automatically exempt from cybersecurity, spectrum, network connection, and similar policies.

e. IPG Related Information. The JITC public web site at <http://jitc.fhu.disa.mil/> provides information and JITC POCs. JITC maintains online information such as basic policy and procedures, descriptions of test programs, registers, and an interoperability database. JITC also tracks interoperability information for programs and systems in the STP (reference (j)), which includes (unclassified) information on ICTOs, and certification status. Authorized users (.mil/.gov) may refer to the STP website (<https://stp.fhu.disa.mil/>) for access instructions.

**10. Requirements for Joint Interoperability Certification (JIC)**

The primary sources for approved joint interoperability requirements are typically the Information Support Plan (ISP) and Capability Production Document (CPD), and, in some cases, the Capability Development Document (CDD). These documents, when approved, should contain the information needed to support a Joint Interoperability Certification (i.e., a certified NR KPP and the required architecture viewpoints).

a. Joint Interoperability Certification Requirements Overview. The Global Information Grid (GIG) Technical Guidance Federation (GTG-F) (reference (1)) contains the NR KPP and associated architecture viewpoints required for documenting system requirements and evaluating joint interoperability (see Figure 10-1). To streamline the approval and use of architectures used for joint test and certification, the NR KPP and required architecture viewpoints may be processed separately within the GTG-F tool suite. This approach allows joint test and interoperability certification as soon as the NR KPP and architecture have been approved. (Section 11 identifies the minimum set of architecture information.)



**Figure 10-1. Joint Interoperability Certification Requirements Process Overview**

b. Joint Interoperability Certification Requirements Generation and Review. PMO/Sponsor development of interoperability requirements for Joint Interoperability Certification uses the

federated suite of tools found in the GTG-F, under the Program Management Portal (PM-P) located at: <https://gtg.csd.disa.mil/uam/homepage.do>. Detailed instructions for creating and tasking the components for review are available on the GTG-F. The PMO/Sponsor may request a review of partial requirements – those meeting the minimum needs for Joint Interoperability Certification – before the full set of documentation has been produced. This allows for expedited certification. The following highlights the Joint Interoperability Certification architecture review and approval process:

(1) Joint Staff J-6, will determine the need for Joint reviews.

(2) NR KPP certification is documented within the GTG-F tool suite for NR KPPs that are not certified within the JCIDS process. NR KPP certifications occur at, or before, the Milestone C final review, and post Milestone C review when requested by the sponsoring GTG-F Executive Agent (EA) to support Joint Interoperability Certification.

(a) Components approve the NR KPP for non-Joint NR KPP certifications.

(b) JITC reviews and validates that the NR KPP and required architecture are testable and sufficient for Joint Interoperability Certification.

(3) JITC will comment on the architecture for testability prior to Component approval.

(4) The ISG will address unresolved issues.

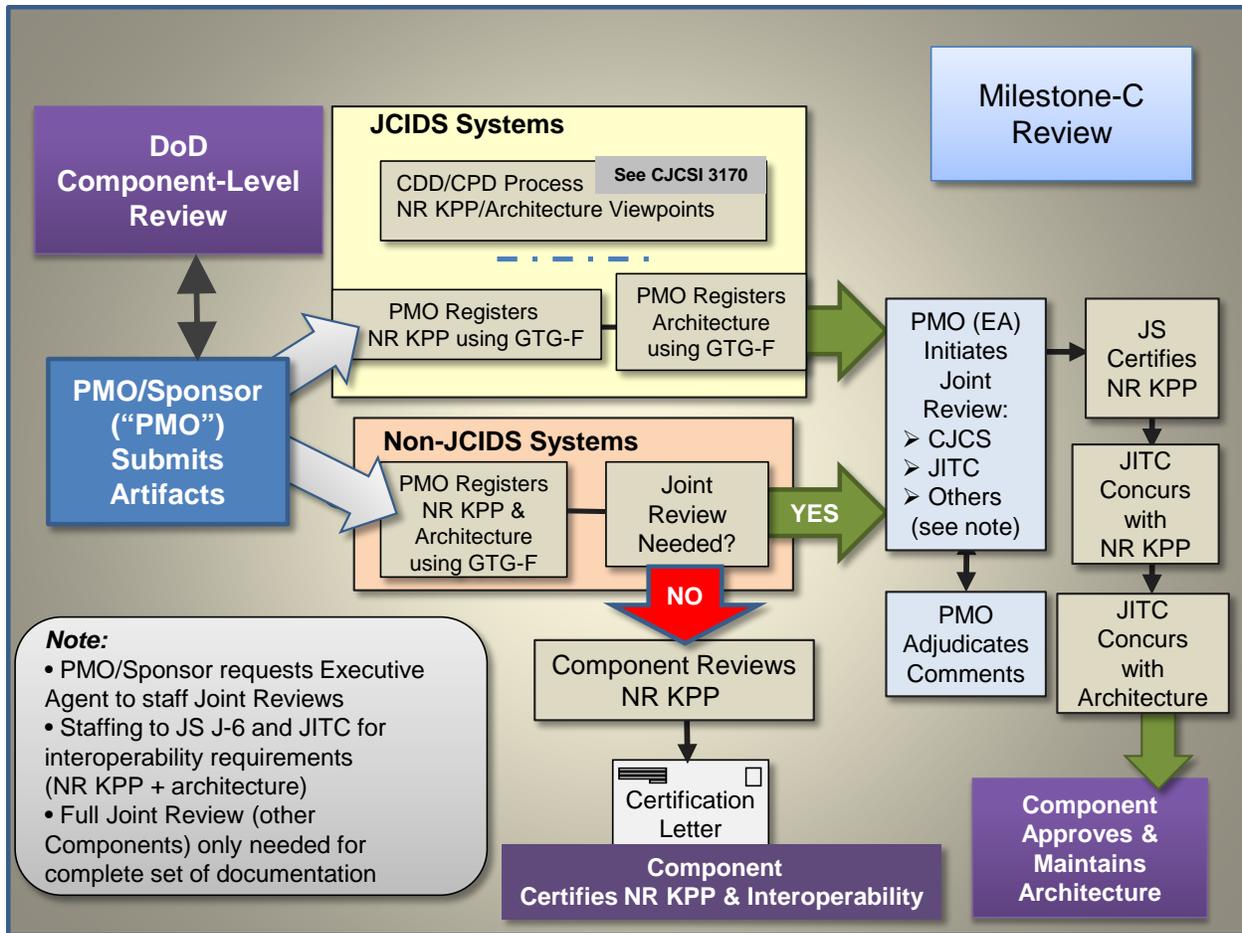
c. Joint Interoperability Certification Additional Considerations. The review process includes internal Component-level and joint-level reviews/approvals, with the PMO/Sponsor submitting artifacts via the GTG-F. Figure 10-2 depicts the review and approval process.

(1) For JCIDS systems, the requirements for Joint Interoperability Certification may include an NR KPP already certified by the Joint Staff as part of the CDD/CPD processes. If so, the Joint Staff will verify that no major changes have occurred since NR KPP certification.

(2) For non-JCIDS acquisitions, the PMO/Sponsor will request a joint review and Joint Staff certification of the NR KPP. If a joint review is not required (i.e., no joint interfaces), the PMO/Sponsor should have an NR KPP N/A letter from the Joint Staff and the Component will certify the NR KPP.

(3) For joint reviews, the Joint Staff certifies the NR KPP, if needed, and JITC will review and validate that the NR KPP and the associated architecture are testable and sufficient for Joint Interoperability Certification.

(4) The Component approves and maintains the architecture after Joint Staff and JITC review. If the system is sufficiently mature, and the PMO/Sponsor has involved JITC in early development of the required architecture, the system should be ready for T&E leading to Joint Interoperability Certification.



**Figure 10-2. Joint Interoperability Certification Requirements Process**

d. Requirements Document Review Staffing Guidance

(1) All organizations supporting the Requirements Document Review process must provide their best support to this important function (e.g., knowledgeable reviewers, adequate time to perform the review). Each reviewer (assessor) needs to thoroughly examine the document, NR KPP, and associated architecture information. Documents and related information (collectively, interoperability requirements) can go through several stages of review depending upon the comments and comment adjudications. For all stages of review, reviewers/assessors must assign their comments a criticality level (Critical, Substantive, or Administrative) according to the "requirements review comment criticality" entries in Appendix C, Definitions. Every comment must also: 1) identify the deficiency; 2) provide a specific recommendation; and 3) provide rationale for the comment/recommendation.

(2) The goal is to identify all critical comments early, so they can be resolved before the final review stages. Critical comments provided during a final review can affect a Milestone C/fielding decision. If an issue will prevent the system from achieving interoperability certification, then the comment should be marked "critical." All other concerns should be marked "substantive" or "administrative," as appropriate. Reviewers/assessors should contact

the PMO/Sponsor about critical questions or concerns to avoid misunderstandings that may cause unnecessary delays. PMOs/Sponsors also need to work closely with the reviewers/assessors to provide any additional requested input or clarification. Adequately addressing the issues to improve the accuracy and completeness of the document will help move it through the review process in a timely manner. Reviewers/assessors must contact the PMO/Sponsor about any critical comments during final reviews to allow for proper coordination and timely resolution of the critical issue.

e. Joint Interoperability Certification Requirements Data Repository

(1) Artifacts associated with requirements for Joint Interoperability Certification (e.g., NR KPP, NR KPP certification memorandum, architecture viewpoints) may be uploaded directly into the GTG-F, or a “link” may be provided to this information residing in another repository. If a link is used, the PMO/Sponsor shall:

- (a) Provide access (e.g., accounts and use of any special tools) to reviewers/testers.
- (b) Maintain configuration management of all items.
- (c) Provide version identification of all items with unambiguous references synchronizing items among the repositories (including GTG-F).
- (d) Maintain storage of the information throughout the system life-cycle.

(2) Testers and developers/reviewers of future increments will need access beyond the initial review. Changes must be tracked to readily identify version artifacts already reviewed, certified, and approved.

## **11. Minimum Set of Architecture Information Required for Joint Interoperability Certification**

JITC, as the Joint Interoperability Certification Authority, uses information from certain DoDAF architecture viewpoints to test and evaluate DoD IT for Joint Interoperability Certification. These viewpoints are a subset of those required for Joint Staff NR KPP certification and are contained in a complete CPD, ISP, or other approved requirements document. PMOs/Sponsors need to coordinate with JITC early to address joint interoperability requirements in the NR KPP and architecture viewpoints.

a. Architecture Viewpoints Required for Joint Interoperability Certification. Figure 11-1 summarizes the architecture information by DoDAF viewpoints that are the focus for Joint Interoperability Certification. The architecture viewpoints must be complete, accurate representations of the system, and information in each product should represent the underlying integrated set of architecture data. “Required” viewpoints represent mandatory architecture information to evaluate the interoperability of a system. “Conditional” viewpoints are mandatory under certain conditions (i.e., when the conditions described below are met), but are otherwise not necessary for interoperability test and certification. Additional architecture information is often useful, and will be needed for the final Joint Staff NR KPP review. The PMO/Sponsor must coordinate with the JITC AO to establish specific architecture viewpoint requirements, and ensure those requirements are sufficiently complete, detailed, measurable, and testable.

b. Conditional Architecture Information. Conditional architecture requirements continue to evolve; many of the conditional viewpoints address IT services/enterprise services. In the following circumstances, conditional information becomes required information.

(1) Data and Information Viewpoints (DIV)-2 and DIV-3 are required when the Standards Viewpoint (StdV)-1 does not clearly define critical Operational/System Resources (respectively), or when a standard Resource is used in a non-standard way.

(2) Services Viewpoints (SvcV)-1 through SvcV-7 (with the exception of SvcV-3/5) are required when the system produces or consumes services or information stored in a shared space (i.e., “joint” services in the context of the IPG). The PMO/Sponsor needs to coordinate with their JITC AO when determining requirements for service viewpoints. The system design and how the architecture is documented will determine what viewpoints are needed, making coordination between the PMO/Sponsor and JITC critical. For some systems, the SvcV viewpoints will replace the Required SVs. In other situations, both SV and SvcV (or “hybrid”) viewpoints may be required. In all cases, the actual requirement is that the necessary architecture information must be provided, no matter where it appears.

- c. Detailed Interoperability Architecture Requirements and Interoperability Requirements Processing. The ISG Resource website contains detailed information (the “Notional Guide”) on the minimum set of architecture requirements and data elements used for certification: <http://jite.fhu.disa.mil/projects/isgsite/index.aspx>. The Joint Staff Warfighting Mission Area (WMA) Architecture Federation and Integration Portal: <https://wmaafip.csd.disa.mil/> contains additional architecture information. This portal provides essential architecture information, including information on specific programs/systems, reference architecture material such as the Joint Information Environment (JIE) architectures, JMTs, Integrated Dictionary information, and links to related sites.

Viewpoint	Description
<b><u>REQUIRED Architecture Viewpoints for Joint Interoperability Certification</u></b>	
<b>AV-1</b>	"Executive Summary" of the architecture. It will describe the Purpose, Scope, Perspective, etc. of the effort. It is not precisely tied to the architecture's data elements, as are the other views.
<b>AV-2</b>	Data Dictionary. Purpose is to expand on the brief description of data elements used throughout the architecture.
<b>OV-1</b>	A graphical depiction of what the architecture is about and an idea of the performers and operations involved.
<b>OV-2</b>	Describes the Operational Performers within the scope of the architecture, and their need to communicate.
<b>OV-3</b>	Resource exchange between the Operational Performers.
<b>OV-5b</b>	Describes the Operational Activities within the scope of the architecture, the Operational Resources those Activities require, and what Operational Resources are created by the Activities.
<b>OV-6c</b>	Provides a time-ordered examination of the Resource Flows as a result of a particular scenario.
<b>SV-1</b>	Addresses the composition and interaction of System Performers. The SV-1 links together the operational and systems architecture models.
<b>SV-2</b>	Describes the precise specification of physical connections between systems. In network-centric environments, this will also describe the networks utilized by the systems.
<b>SV-5a</b>	Maps system functions (activities) to operational activities.
<b>SV-6</b>	Definition of the Resource exchanges between the System Performers. The SV-6 specifies the characteristics of the System Resource Flows with emphasis on resources crossing the system boundary.
<b>SV-7</b>	Set of system performance parameters (measures).
<b>StdV-1</b>	Standards Profile - list of implemented technical standards, rules, and guidelines. <i>Note: If implemented standards appear in the StdV-2 and not the StdV-1 (e.g., as some have done for emerging standards that are currently implemented), then this information is also required.</i>
<b><u>CONDITIONAL Architecture Viewpoints for Joint Interoperability Certification</u></b> Note: PMO/Sponsor needs to coordinate with their JITC AO when determining requirements for service viewpoints	
<b>DIV-2</b>	Logical Data Model. Documentation of the data requirements and structural business process (activity) rules. <i>CONDITION: REQUIRED when critical Operational Resources are not clearly defined in the StdV-1, or when a standard Resource is used in a non-standard way.</i>
<b>DIV-3</b>	Physical Data Model. Physical implementation format of the Logical Data Model entities, e.g., message formats, file structures, physical schema. <i>CONDITION: REQUIRED when critical System Resources are not clearly defined in the StdV-1, or when a standard Resource is used in a non-standard way.</i>
<b>SvcV-1</b>	Services Context Description – identifies services and their interconnections. <i>CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.</i>
<b>SvcV-2</b>	Specifies resource flows exchanged between services, and may list protocol stacks. <i>CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.</i>
<b>SvcV-4</b>	Depicts allocation of service functions and data flows between service functions (activities). <i>CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.</i>
<b>SvcV-5</b>	Maps services (activities) to operational activities. <i>CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.</i>
<b>SvcV-6</b>	Maps service data exchanges with associated measures and metrics. <i>CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.</i>
<b>SvcV-7</b>	Complete set of performance parameters (measures) of the services. <i>CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.</i>

**Figure 11-1. Minimum Set of Viewpoints for Joint Interoperability Certification**

## **Appendix A References**

- a. DoD Instruction 8330.01, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” May 21, 2014. Available at: <http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf>
- b. Net Ready Key Performance Parameter (NR KPP) Manual on the NR KPP Resource Page. Available at: [https://intellipedia.intelink.gov/wiki/Portal:NR\\_KPP\\_Resource\\_Page](https://intellipedia.intelink.gov/wiki/Portal:NR_KPP_Resource_Page)
- c. Unified Capabilities Requirements (UCR). Available at: <http://www.disa.mil/Services/Network-Services/UCCO/>
- d. DoDI 8100.04, “DoD Unified Capabilities (UC),” 9 December 2010. Available at: <http://www.dtic.mil/whs/directives/index.html>
- e. Approved Products List (APL) Process Guide. Available at: <https://aplits.disa.mil>.
- f. CJCSI 3170.01I, “Joint Capabilities Integration and Development System (JCIDS),” 23 January 2015. Available at: [http://www.dtic.mil/cjcs\\_directives/](http://www.dtic.mil/cjcs_directives/)
- g. Manual for the Operation of the Joint Capabilities Integration and Development System. Available at: [https://www.intelink.gov/wiki/JCIDS\\_Manual](https://www.intelink.gov/wiki/JCIDS_Manual)
- h. DoD Architecture Framework (DoDAF). See: <http://dodcio.defense.gov/dodaf20.aspx>
- i. Joint Mission Thread (JMT) information on Joint Staff J-6, Warfighting Mission Area Architectures tab. Available at: <https://wmaafip.csd.disa.mil/>
- j. JITC System Tracking Program. See: <https://stp.fhu.disa.mil>
- k. DoDI 8310.01, “Information Technology Standards in the DoD,” February 2, 2015. Available at: <http://www.dtic.mil/whs/directives>
- l. GIG Technical Guidance Federation (GTG-F). See: <https://gtg.csd.disa.mil/uam/homepage.do>

(This page intentionally left blank.)

**Appendix B Abbreviations and Acronyms**

ACAT	Acquisition Category
AO	Action Officer (JITC)
APL	Approved Products List
CAO	Connection Approval Office
CDD	Capability Development Document
CDL	Common Data Link
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COTS	Commercial-Off-the-Shelf
CPD	Capability Production Document
DAA	Designated Approving Authority (now Authorizing Official)
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DITPR	DoD Information Technology Portfolio Repository
DIV	Data and Information Viewpoint
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoDAF	DoD Architecture Framework
DoDD	Department of Defense Directive
DoDI	DoD Instruction
DOT&E	Director, Operational Test and Evaluation

DOTLPPF-P	Doctrine, Organization, Training, Leadership and education, Personnel, and Facilities – Policy
DT&E	Developmental Test and Evaluation
EA	Executive Agent (GTG-F)
ERD	Electronic Report Distribution (tool)
GEOINT	Geospatial Intelligence
GIG	Global Information Grid
GTG-F	GIG Technical Guidance Federation
HF	High Frequency
IA	Information Assurance (now cybersecurity)
ID	Identification
IAM	Interoperability & Supportability Assessment Module (GTG-F)
ICA	Interface Control Agreement
ICEP	Interoperability Certification Evaluation Plan
ICTO	Interim Certificate To Operate
IPG	Interoperability Process Guide
ISG	Interoperability Steering Group
ISP	Information Support Plan
IT	Information Technology
ITP	Interoperability Test Plan

JCIDS	Joint Capabilities Integration and Development System
JIC	Joint Interoperability Certification
JIE	Joint Information Environment
JS	Joint Staff
JITC	Joint Interoperability Test Command
JMT	Joint Mission Thread
KPP	Key Performance Parameter
MDA	Milestone Decision Authority
MIPR	Military Interdepartmental Purchase Request
MOE	Measure of Effectiveness
MOP	Measure of Performance
NGA	National Geospatial-Intelligence Agency
NR KPP	Net-Ready Key Performance Parameter
NSA	National Security Agency
NSS	National Security Systems
OARL	Operating at Risk List
OIPT	Overarching Integrated Product Team
OOC	Out-of-Cycle
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review

OV	Operational Viewpoint
PM	Program Manager
PMO	Program Management Office
PM-P	Program Management Portal (GTG-F)
POA&M	Plan of Action and Milestones
POC	Point Of Contact
RF	Radio Frequency
SATCOM	Satellite Communications
StdV	Standards Viewpoint
STP	System Tracking Program
SV	Systems Viewpoint
SvcV	Services Viewpoint
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TTP	Tactics, Techniques, and Procedures
UAT	User Acceptance Testing
UC	Unified Capabilities
UCCO	Unified Capabilities Certification Office
UCR	Unified Capabilities Requirements
UHF	Ultra-High Frequency

U.S.	United States
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology, and Logistics)
USSTRATCOM	U.S. Strategic Command
VHF	Very High Frequency
WMA	Warfighting Mission Area

(This page intentionally left blank.)

## **Appendix C Definitions**

**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. [JITC]

**Cybersecurity.** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. [Defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23.]

**External IT.** A system that resides or operates outside the intrinsic and defined boundaries of an IT (i.e., with information flowing from and/or to the boundary). The system boundary is described in the system's architecture data model. As an example, an external system to a DoD space system is the widely shared communications backbone or data network that a space system might interface with for communications or data services.

**Information Assurance (IA).** See Cybersecurity.

**Interface Control Agreement (ICA).** ICAs are interface agreements established for each external interface to the IT. ICA templates are defined in the NR KPP Manual.

**Interim Certificate to Operate (ICTO).** Authority to field systems for a limited time to allow operational use while pursuing Joint Interoperability Certification. The decision to grant an ICTO is made by the ISG.

**Increment.** Whether an evolutionary, incremental, or spiral acquisition, an increment is a militarily useful, logistically supportable, and technically mature increase in operational capability that can be developed, produced, deployed, and sustained. Each increment will have its own set of threshold and objective values set by the user. Increments include block upgrades, pre-planned product improvement, and similar efforts providing an increase in operational capability.

**Information Support Plan (ISP).** The ISP is a key document in achieving interoperability certification. The ISP describes IT and information needs, dependencies, and interfaces for programs. It focuses on the efficient and effective exchange of information that, if not properly managed, could limit or restrict the operation of the program in accordance with its defined capability. Entered through the GTG-F portal, the ISP contains or links to the NR KPP along with supporting architectural data. Instructions for completion of the ISP are found on the portal. [DoDI 8330.01]

**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 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). [US Code]

***Interface Control Document.*** An interface control document communicates all possible inputs to and all potential outputs from a system for potential or actual IT users. The internal interfaces of a system or subsystem are typically not documented in an interface control document, but are documented in a system design document (such as a software design document). An interface control document may describe:

- The inputs and outputs of a single system,
- The interface between two systems or subsystems,
- The complete interface protocol from the lowest physical elements (e.g., the mating plugs, the electrical signal voltage levels) to the highest logical levels (e.g., the application layer of a model), or some subset thereof.

Interface control documents are a key element of systems engineering as they define and control the interfaces of a system, and thereby bound its requirements. [Software systems engineering sources]

***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. IT 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 cybersecurity. [DoDI 8330.01]

***Interoperability Certification.*** A formal statement of adequacy provided by the responsible Interoperability Certification Authority agency that a system has met its interoperability requirements. [DoDI 8330.01]

***Interoperability Certification Authority.*** The office with the certification authority for interoperability. Verifies that the IT has met its interoperability requirements, as proven through test and evaluation. For IT with joint, multinational, and interagency interoperability requirements, the Interoperability Certification Authority is JITC. For all other IT, the owning DoD Component designates the Interoperability Certification Authority. [DoDI 8330.01]

***Interoperability Certification Evaluation Plan (ICEP).*** A JITC plan, developed in conjunction with the PMO/Sponsor, that establishes 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 PMO/Sponsor should coordinate with JITC to integrate interoperability into the system's T&E documents (e.g., Test and Evaluation Master Plan (TEMP), test plans). Complex systems that depend on multiple evaluation events will require JITC to develop an ICEP, in addition to interoperability test plans (ITP). Separate from any ICEP, 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). [JITC]

**Interoperability Environment.** The communications environment of a system, with interfaces described by SV-1/2 information and information exchanges over the interfaces defined by OV-3/SV-6 information, including protocol and data standards, RF waveforms and other spectrum considerations, etc., to include aspects of the electromagnetic environment that affect information exchange. Connections to the DoD's network infrastructure and enterprise services (including shared data spaces) may form part of a system's interoperability environment.

**Joint.** Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. Used in information interoperability policy to include these and external mission partners: joint, combined, and coalition forces, other U.S. Government Departments and Agencies (including federal, state, local and tribal), and non-governmental organizations, as appropriate. [derived from DoDI 8330.01 and other sources]

**Joint Capabilities Integration and Development System (JCIDS).** A Chairman of the Joint Chiefs of Staff process including but not limited to identifying, assessing, validating, and prioritizing joint military capability requirements. The JCIDS process is a collaborative effort between requirements and acquisition communities to set achievable risk-informed capability requirements, and make effective cost, performance, schedule, and quantity trade-offs. [CJCSI 3170.01]

**Joint Interface.** A "Joint" interface is an interface (as defined in DoDAF models for systems and services, such as the SV-1, SV-3, and the various service models) between or among systems or services that is considered "Joint" per the definition above. Used in information interoperability policy meaning an interface between/among external mission partners: joint, combined, and coalition forces, other U.S. Government Departments and Agencies (including federal, state, local and tribal), and non-governmental organizations, as appropriate. Coalition partners, non-governmental organizations, etc., which share the same physical/logical interfaces will also make an interface "joint." Not all information exchanges over an interface need to be joint for it to be considered a joint interface. [derived from multiple sources]

**Joint Information Exchange.** An exchange of information/data between/among systems when any system whose mission is joined through a logical connection with a system(s) or data sources from an external partner for the purpose of exchanging common data, sharing situational awareness, or partnering to perform a single mission (i.e., when one program such as Identity Management is consumed as part of data reuse efficiencies). Coalition partners, non-governmental organizations, etc., that exchange information produced/consumed/shared or distributed by the system under test will result in "joint" exchanges. Information exchanges

include all the data products and waveforms used or produced by the system (including sensor platforms). [derived from multiple sources]

**Joint Interoperability Certification.** Joint Interoperability Certification (issued only by JITC) involves an evaluation of information interoperability with respect to interoperability requirements at the joint level. JITC updates interoperability certifications throughout a system's life-cycle to reflect changes in the system, status, and joint interoperability environment. [DoDI 8330.01]

**Joint Mission Thread.** An operational and technical description of the end-to-end set of activities and systems that accomplish the execution of a joint mission.

**Milestone Decision Authority (MDA).** The designated individual with overall responsibility for a program. The MDA shall have the authority to approve entry of an acquisition program into the next phase of the acquisition process and shall be accountable for cost, schedule, and performance reporting to higher authority, including Congressional reporting. [DoDD 5000.01]

**National Security System (NSS).** Information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which: (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). NSS include any information system (including any telecommunications system) protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [US Code]

### **Requirements Review Comment Criticality**

***Critical Comment.*** Critical comments must identify violations of law or contradictions of Executive Branch or DoD policy; unnecessary risks to safety, life, limb, or DoD materiel; waste or abuse of DoD appropriations; or imposition of an unreasonable burden on a Component's resources; an information-related issue that would prevent the program's ability to provide a required operational/functional capability; or missing integrated architectural product content needed to provide or validate measurable/testable requirements. Any critical comments result in an automatic non-concur. [derived from SD 818]

***Substantive Comment.*** A substantive comment identifies unnecessary, incorrect, misleading, confusing, or inconsistent information with other sections; disagreement with the proposed responsibilities, requirements, or procedures; or an issue that would significantly impact the program's ability to provide a required operational and/or functional capability. One substantive comment is usually not sufficient justification for a non-concur, however, multiple substantive comments may be grounds for a non-concur. [derived from SD 818]

***Administrative Comment.*** An administrative comment concerns non-substantive aspects, such as dates of references, format, typographical, and grammar errors. Administrative comments will never warrant a non-concur. [derived from SD 818]

***Service (DoDAF).*** A service, in its broadest sense, is a well-defined way to provide a unit of work, through which a provider provides a useful result to a consumer. Services do not necessarily equate to web-based technology or functions, although their use in the net-centric environment generally involves the use of web-based, or network-based, resources. [DoDAF]

***Unified Capabilities Requirements (UCR).*** The document that specifies the functional requirements, performance objectives, and technical specifications for certification of approved products to be used in DoD networks to provide end-to-end Unified Capabilities (UC). [derived from DoDI 8100.04]

(This page intentionally left blank.)