

Joint Interoperability Test Command



Interoperability Process Guide

Version 1.0
10 September 2012

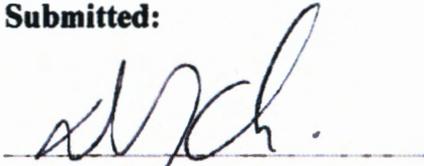
Incorporating Change 1, April 2014

(INTENTIONALLY BLANK)

Interoperability Process Guide

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

Submitted:



DOUGLAS J. ORSI
Colonel, USA
Commander
Joint Interoperability Test Command

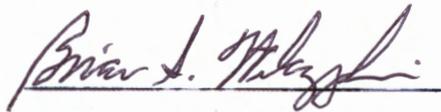
18 April 2014
Date

Approved:



Luanne Overstreet
Test and Evaluation Executive
Defense Information Systems Agency

25 April 2014
Date



Brian G. Wilczynski
Acting Principal Director
DCIO, Information Enterprise
Office of the DoD CIO

30 April 2014
Date

(INTENTIONALLY BLANK)

Summary of Changes

| Version | Sections Affected | Description of Change |
|--------------------------|-------------------|---|
| Version 1.0 | All | <ul style="list-style-type: none"> - Initial approved version. |
| Version 1.0, Change 1 | All | <ul style="list-style-type: none"> - Administrative corrections. - Fact-of-life changes - Updated waiver and ICTO sections. - Added section on Operating at Risk List processes. - 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. |

TABLE OF CONTENTS

| <u>SECTION</u> | <u>PAGE</u> |
|---|--------------------|
| 1. Purpose | 1 |
| 2. Overview of Certification Policy and Process | 1 |
| 3. Pre-Joint Interoperability Certification Procedures | 5 |
| 4. JITC Joint Interoperability Test and Certification..... | 12 |
| 5. Post-Joint Interoperability Test and Certification Process | 18 |
| 6. Interim Certificate To Operate (ICTO) Process..... | 22 |
| 7. Waivers to Policy..... | 27 |
| 8. Operating At Risk List (OARL) | 31 |
| 9. Other Evaluations and Related Information..... | 33 |
| 10. Requirements for Joint Interoperability Certification (JIC)..... | 35 |
| 11. Minimum Set of Architecture Information Required for Joint Interoperability Certification..... | 39 |
| Appendix A References | 42 |
| Appendix B Abbreviations and Acronyms..... | 43 |
| Appendix C Definitions | 48 |

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. Redefining NR KPP Policy..... | 7 |
| Figure 4-1. Representative T&E Test Phase Activities. | 12 |
| Figure 5-1. T&E Post-Test Activities. | 18 |
| Figure 5-2. Certification Testing Timeline. | 19 |
| Figure 5-3. Interoperability T&E Products. | 20 |
| Figure 5-4. JITC Interoperability Products..... | 21 |
| Figure 6-1. Procedures for Processing ICTO Requests..... | 24 |
| Figure 7-1. Waiver To Policy Process..... | 28 |
| Figure 8-1. OARL Description. | 31 |
| Figure 10-1. Joint Interoperability Certification Requirements Process Overview..... | 35 |
| Figure 10-2. Joint Interoperability Certification Requirements Process. | 37 |
| Figure 11-1. Minimum Set of Architecture Viewpoints Required for Joint Interoperability Certification. | 41 |

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. This guide 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. There are several documents governing interoperability for the DoD (listed in Appendix A). The key directives, instructions, and guides are summarized in the paragraphs below. Depicted in Figure 2-1 are the high level relationships among them.

(1) DoD Directive (DoDD) 4630.05 (reference (a)), DoD Instruction (DoDI) 4630.8 (reference (b)), and the DoD CIO memorandum, “Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS),” (reference (c)) all state 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. (DoDI 8330.aa, currently under development, will update policy and procedures for interoperability of IT, including NSS, and will incorporate and cancel DoDD 4630.05 and DoDI 4630.8 once final.)

(2) DoD CIO memorandum, “Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS),” designates the JITC as the Joint Interoperability Certification Authority for DoD. It further specifies that JITC shall certify all joint IT and NSS for interoperability, based on a Joint Staff certified NR KPP, when applicable.

(3) Joint Chiefs of Staff Instruction (CJCSI) 6212.01 and its associated NR KPP Manual prescribe the foundation and development process for the NR KPP, where the data used to develop the NR KPP is the result of the development processes for the DoD Architecture Framework (DoDAF).

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

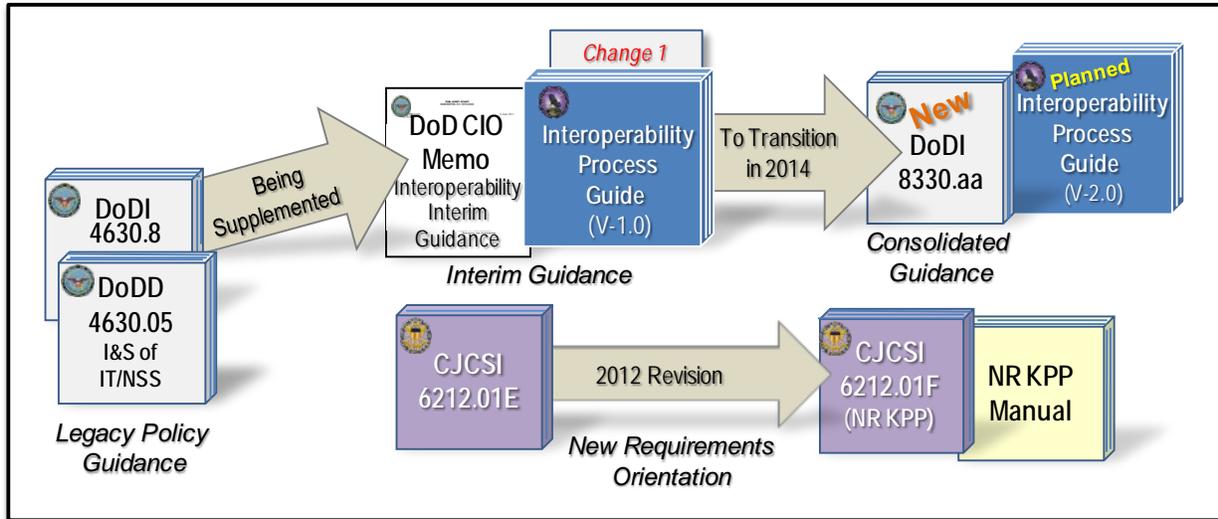


Figure 2-1. Interoperability Directives, Instructions, and Guidance.

(5) Unified Capabilities Requirements (UCR) Document (reference (f)), DoDI 8100.04 (reference (g)), and the Approved Products List (APL) Process Guide detail the interoperability certification policy and requirements for Unified Capabilities (UC). (UC capabilities are voice, video, data (collaboration), and mobile devices.) Certification processes of UC products are not readdressed in this IPG.

(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. The JITC, as the 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 also hire 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. All JITC interoperability efforts must be funded by the PMO/sponsor of the program under test. 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.

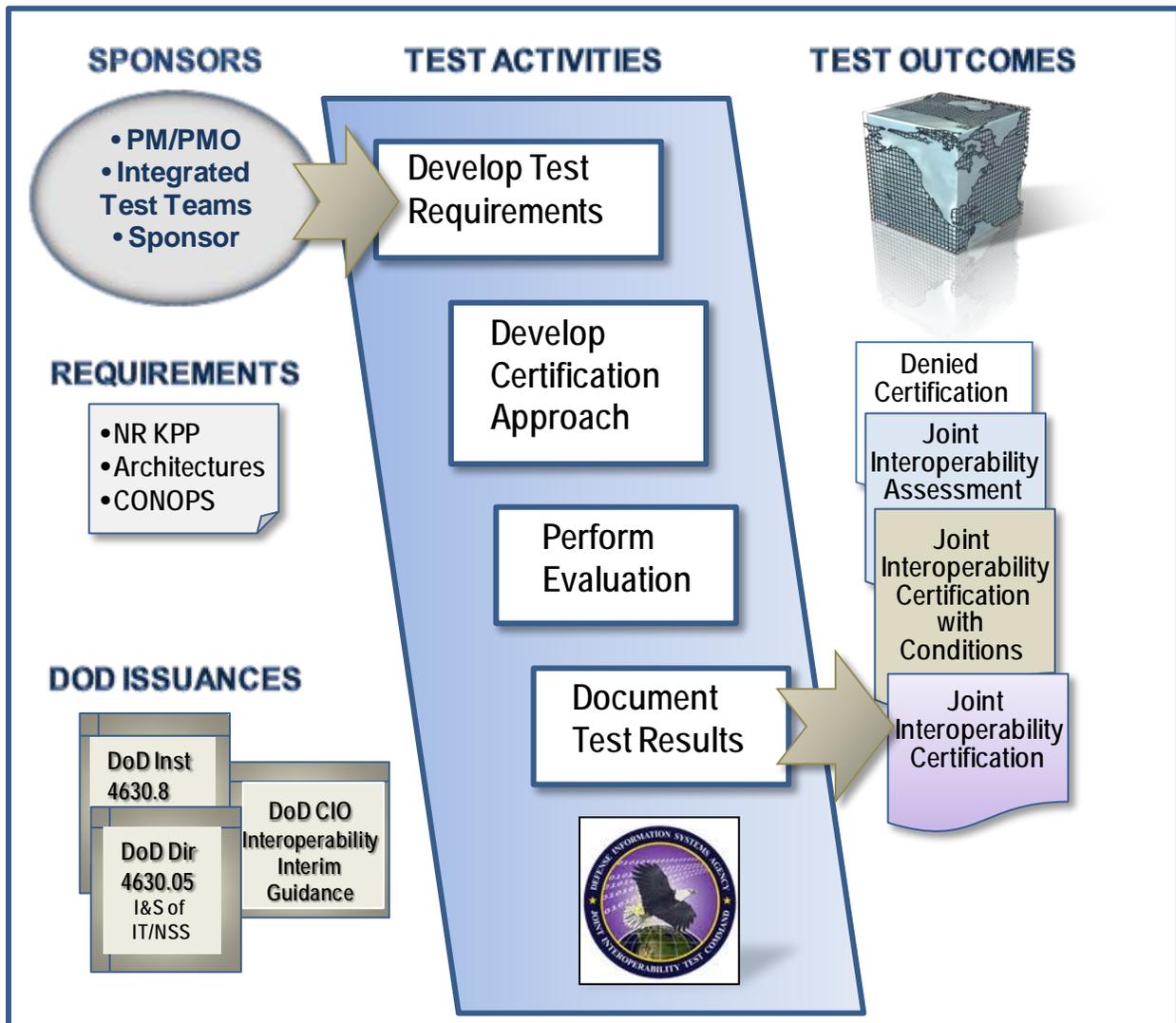


Figure 2-2. Joint Interoperability Certification T&E Overview.

(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 in accordance with these criteria. All JITC interoperability efforts will be funded by the program management office of the program under test. 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.

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 Operating at Risk List (OARL). The OARL is monitored by the DoD CIO’s Interoperability Steering Group (ISG) which is governed by specific governance. (Refer to section 8 for OARL policy and procedures.)

d. Interoperability Process Overview. The Joint Interoperability Certification preparation, test and evaluation, and certification processes are detailed in sections 3, 4, and 5. A notional process flow for a program of record is shown in Figure 2-3, therefore the steps would be applicable to most systems requiring a certification.

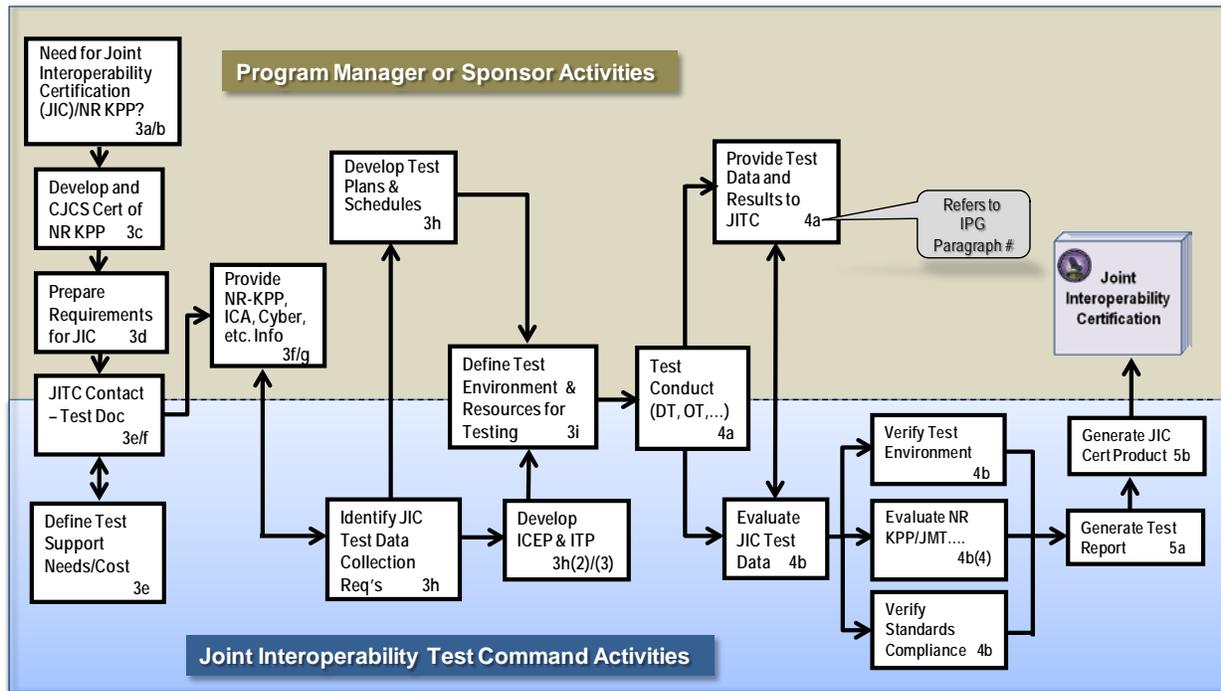


Figure 2-3. Notional Joint Interoperability Certification Process.

3. Pre-Joint Interoperability 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.

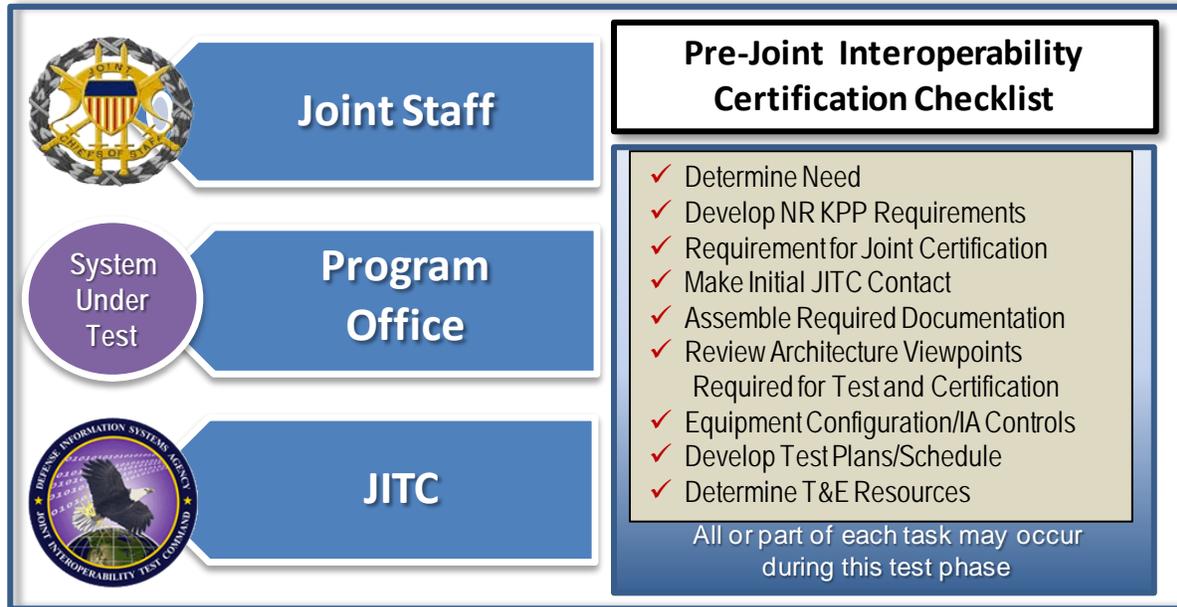


Figure 3-1. Test Preparation Activities.

a. Determine Need for Joint Interoperability Certification. Joint interoperability certification is required of all systems with joint interfaces or joint information exchanges with other systems. 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 U.S. Government Department or Agency (including federal, state, local, and tribal), Coalition partners, non-governmental organizations, as appropriate, 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).

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. If JITC 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/cgi/isgsite/index.aspx>.

NR KPPs are developed by the PMO/sponsor (see references (d) and (e) 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.

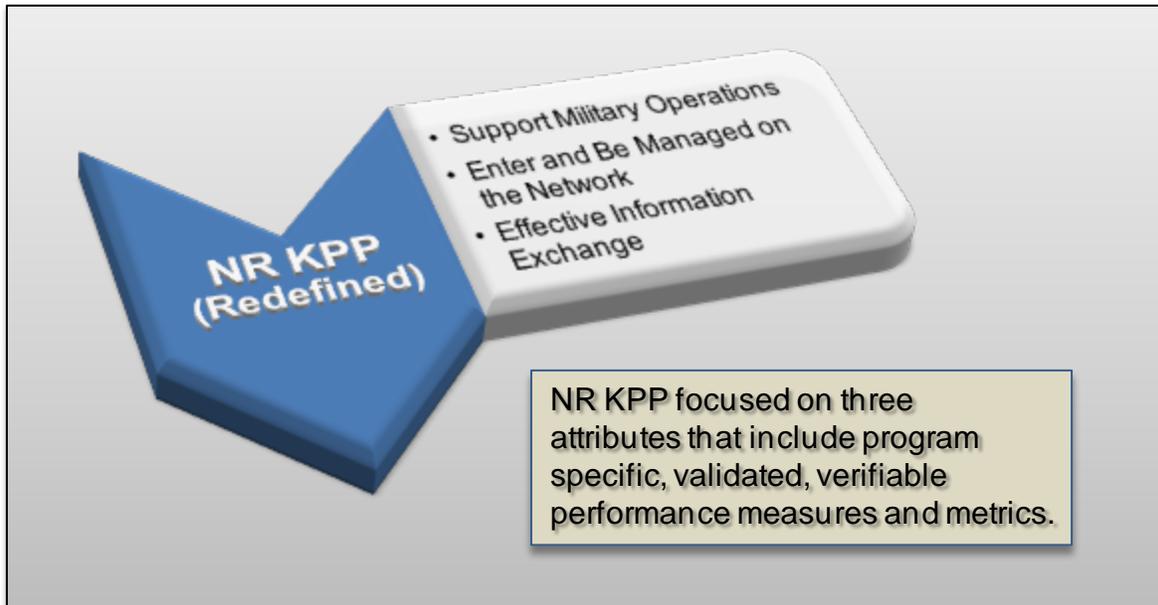


Figure 3-2. NR KPP Focus.

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 the measures of effectiveness (MOEs) and measures of performance (MOPs) associated with the three attributes of the NR KPP as described in the following paragraphs.

(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 constituting its operational mission. Test data for this attribute will normally be obtained from the test reports provided by the designated test organization responsible for the OT&E of the system.

(2) Enter and Be Managed in the Network. This attribute provides MOPs addressing the ability of the system to successfully enter into and be managed within the networks it must operate in to perform its operational mission, as well as associated technical parameters included 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. 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 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. 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.

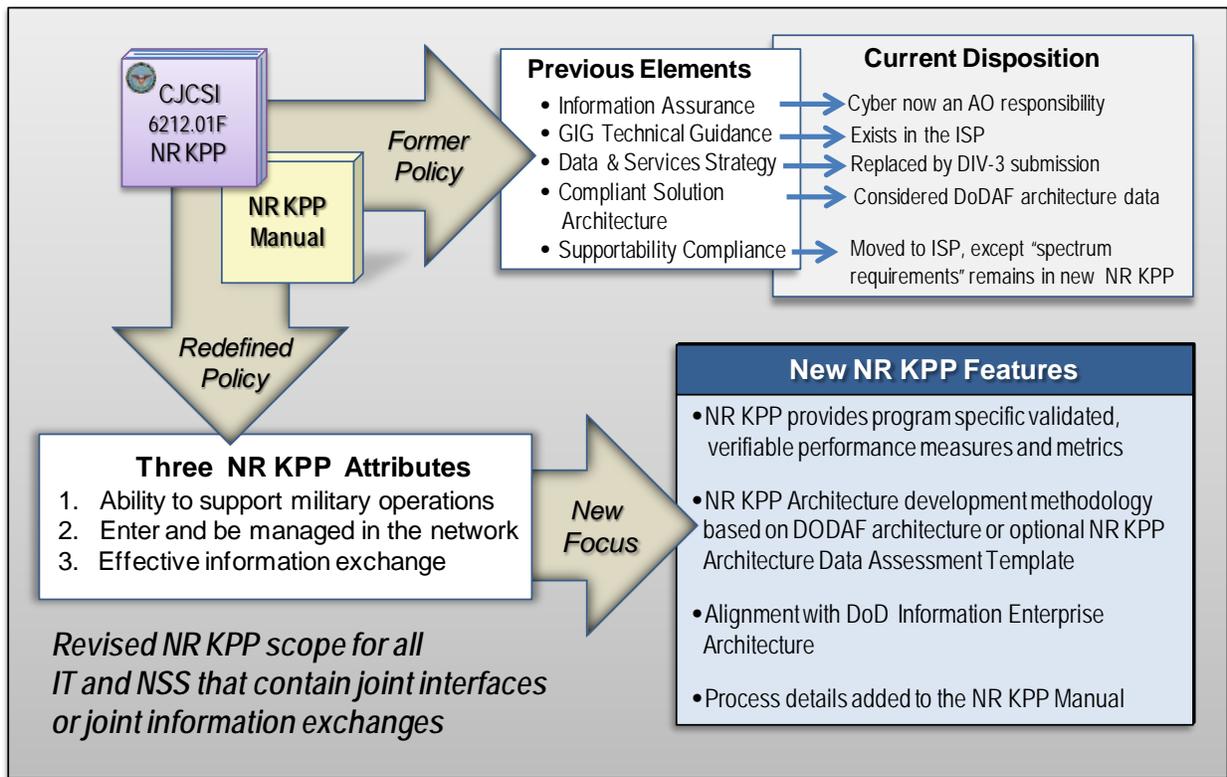


Figure 3-3. Redefining NR KPP Policy.

d. Preparing 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 what architecture viewpoints are 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, governs preparation of this documentation. (Also see Appendix A.)

(1) CJCSI 3170.01 directs Joint Capabilities Integration and Development System (JCIDS) documentation to be prepared and submitted. Format found in the CJCSI 3170.01 manual.

(2) Information Support Plans (ISPs) are governed by DoD Instruction 4630.8 and DoD CIO memorandum, “Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS). See: <https://gtg.csd.disa.mil/uam/support/userDocument/list> for user documentation.

(3) Preparation of the NR KPP, and related architecture analysis supporting its development, is detailed in references CJCSI 6212.01F and NR KPP Manual. These references also delineate the requirement for Interface Control Agreements (ICAs), and point to a descriptive ICA template on the ‘NR KPP Resource Page’ portal at: https://intellipedia.intelink.gov/wiki/Portal:NR_KPP_Resource_Page.

(4) More detailed description of the DoDAF, and its application in developing capability solution architectures, is found at the DoD CIO DoDAF web site at: <http://dodcio.defense.gov/dodaf20.aspx>.

e. Initial Contact with JITC for Scheduling Testing. 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://jitc.fhu.disa.mil/>) provides forms and contact information under the “Support” section. Funding arrangements for planning, testing, analysis, and reporting associated with interoperability certification is the responsibility of the PMO/sponsor. Funding must be in place at least 90 days prior to the start of any JITC activity. In the case of Common Data Link (CDL), testing is funded by the CDL Executive Agent.

f. Required Documentation for Test. The PMO/sponsor must provide the following information at least 120 days prior to any test and evaluation activity that will support Joint Interoperability Certification:

(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, available at: [https://intellipedia.intelink.gov/wiki/Net_Ready_-_Key_Performance_Parameter_\(NR-KPP\)_Manual](https://intellipedia.intelink.gov/wiki/Net_Ready_-_Key_Performance_Parameter_(NR-KPP)_Manual), 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, available at: [https://intellipedia.intelink.gov/wiki/Net_Ready_-_Key_Performance_Parameter_\(NR-KPP\)_Manual](https://intellipedia.intelink.gov/wiki/Net_Ready_-_Key_Performance_Parameter_(NR-KPP)_Manual).

(b) Interface control documents/specifications (as appropriate) for each interface (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 certification 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 an authorized cybersecurity configuration sufficient to ensure a realistic cybersecurity testing environment. The PMO/sponsor must provide documentation, signed by the sponsor Authorizing Official (AO) (previously a Designated Approving Authority (DAA)), when claiming exemption from any cybersecurity requirements. When a PMO/sponsor is developing 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 AO.

(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 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 all of the applicable cybersecurity controls. If the proper cybersecurity configuration is not used during testing, then the test results may be invalidated, 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. Developing Test Plans/Schedule. Joint interoperability evaluation by JITC provides a detailed assessment and determination of a system's joint interoperability. 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). The JITC may produce two types of system specific plans: the Interoperability Certification Evaluation Plan (ICEP) and 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 at each increment.

(1) TEMP.

(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 life-cycle 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 at least 120 days prior to any test event supporting interoperability evaluation. Funding must be in place at least 90 days prior to the start of any JITC activity.

(c) When test data from the PMO's/sponsor's test efforts are insufficient to perform an interoperability evaluation, or not expected to be available or sufficient for 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) shall be used to develop the TEMP measures. Established Joint Mission Threads (JMTs) shall be used to verify the operational effectiveness of information exchanges (see <https://sadie.nmci.navy.mil/jafe/default.aspx>). If established JMTs are not available, appropriate mission scripts must be approved by Joint Staff, J-6.

(e) Standards conformance testing programs serve as a foundation for overall joint interoperability evaluation and should be conducted 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 ICEP is an optional JITC test and certification strategy that 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 or SoS 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. Reference (b) describes the contents of the JITC OTRR input.

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 life-cycle 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. This evaluation strategy identifies the data necessary to support an interoperability evaluation, as well as indicate the test events/environments planned to produce that data.

4. JITC Joint Interoperability Test and Certification

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

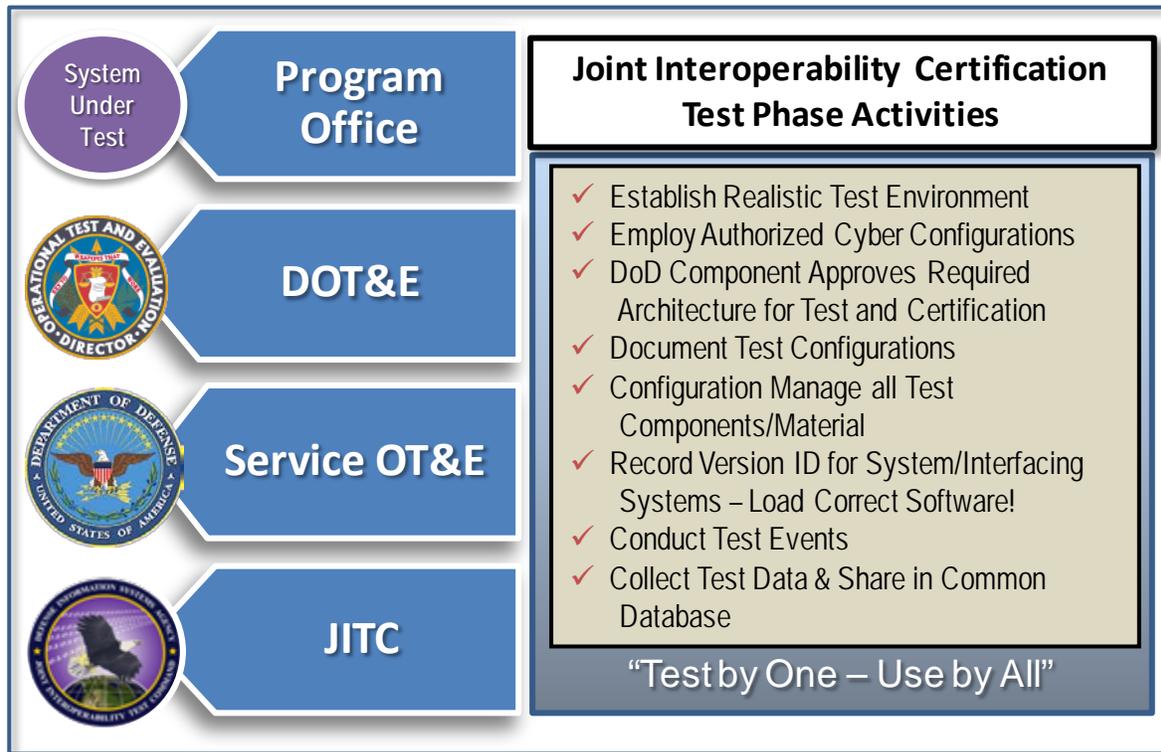


Figure 4-1. Representative T&E Test Phase Activities.

a. Test Conduct

(1) Testing provides 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, it should be realized

that 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 is usually obtained from planned OT testing, with JITC using the shared test data to provide Joint Interoperability Certification. Maximum benefit can be obtained from integrated T&E if developer 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) Preliminary interoperability status is available in the form of a Joint Interoperability Assessment. This can be particularly useful in cases where requirements documents have not been finalized, high risk areas warrant early feedback, etc.

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

(a) Joint Staff-certified NR KPP and associated architecture data, as well as any additional interoperability-related requirements that are not specified in the NR KPP or architecture products themselves, but can be derived from interface specifications or found in other parts of the requirements documents. Issues with NR KPP requirements shall be raised with the Joint Staff for resolution.

(b) Mission related data using JMTs, if provided.

(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, on technical and operational effectiveness of information exchanges over interfaces from those test events or exercises. 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 (IA) characteristics of the environment.

(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) 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 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 whether that results in a 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.

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 life-cycle. 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, and the PMO/sponsor should be aware that the NR KPP may need to be recertified.

(1) Recertification Criteria. Recertification is required when:

(a) Interoperability functionality or requirements change, as determined by the owning DoD Component. PMs will report to the ISG (or equivalent DoD Component governing body for systems without joint, multinational or interagency interoperability requirements) every 4 years to determine if recertification is required or if the existing certification will be extended for an additional 4 years.

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

(c) 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.

(d) Non-materiel changes (i.e., Doctrine, Organization, Training, Leadership and education, Personnel, Facilities and Policy (DOTLPP-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 process guide for attaining an initial certification.

(b) *Certification is scheduled to expire:*

1. Contact JITC at least 6 months prior to scheduled expiration to allow sufficient time for the recertification process to be accomplished.

2. Provide written verification that the interoperability environment (including the system and interfacing systems) has been reviewed and has not changed such that it affects system interoperability. Also, specify that system interoperability was verified through exercises, operational use, and deployments. If changes have occurred that affect interoperability, provide documentation on any changes in the interoperability environment.

3. Request the Joint Staff to review system interoperability requirements and verify that those requirements are still valid.

4. If the system interoperability environment and requirements have not changed, a new certification may be issued without additional interoperability testing when the current certification expires.

5. Alternatively, if changes to the system or its environment have impacted interoperability, or if the interoperability requirements have changed, a new joint interoperability evaluation is required. Substantive revisions in mandated DISR standards constitute a change in the interoperability environment that results in a need for recertification. 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, initiate planning for separate JITC test and certification.

(c) If 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) that could possibly impact interoperability:

1. 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 the 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), unless a new certification is required. This situation may occur because of significant changes to the requirements, such as a new interface or new mandated standards.

3. If the changes are to interfacing systems or the interoperability environment, and no impact has occurred or is expected, no action is required beyond the initial JITC evaluation of the changes.

4. If interoperability is or will be impacted, planning shall be initiated to collect data from past or planned test, exercise, 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, as for example an update to an interfacing system, it may be appropriate to obtain a Joint Interoperability Certification with Conditions.

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

1. 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.

2. If impacts to interoperability have not occurred or are not anticipated, no further action is required beyond the initial JITC evaluation of the changes.

3. If impacts to interoperability have occurred or are anticipated, initiate planning to collect data from past or planned test, exercise or operational venues with which to evaluate interoperability of the system within the changed environment for a new certification.

(3) Certification Extension Process. If a certified system is modified, but JITC determines the modifications do not affect the previously determined interoperability status, the previous certification may be extended to cover the modified version. The extended certification has the same expiration date as the existing certification. The extension only applies to the specific system versions covered, not to the expiration date. An extension request must include:

- (a) A written statement that the modification does not affect interoperability.
- (b) Sufficient information for JITC to independently determine the impact of change.

5. Post-Joint Interoperability Test and Certification Process

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.

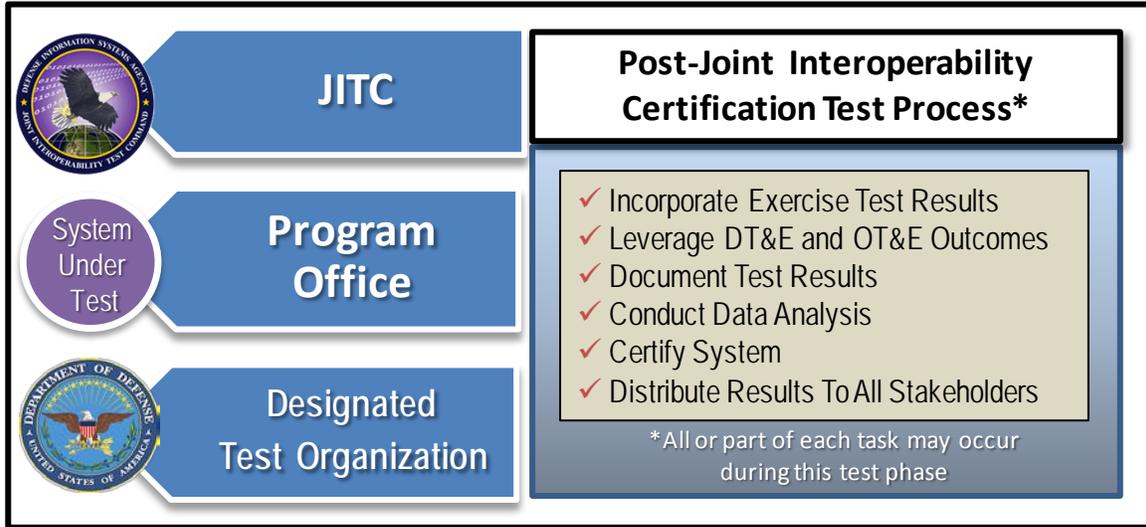


Figure 5-1. T&E Post-Test Activities.

a. Test Reports and Timelines. JITC shall provide interoperability test documentation (to the PMO/sponsor, with Joint Interoperability Certifications further being sent to ISG members) with a goal of delivery of 45 calendar days from the end of testing and receipt of all required test information. The PMO/sponsor and designated test organization provides all relevant reports, system/test configuration information, including that for interfacing systems, test data, trouble reports, analysis of any discrepancies, etc., in a timely fashion, keeping in mind the JITC processing time required after receipt of test information. Figure 5-2 below depicts the sequence of events and relative timelines integral to accomplishing this concluding phase of testing.

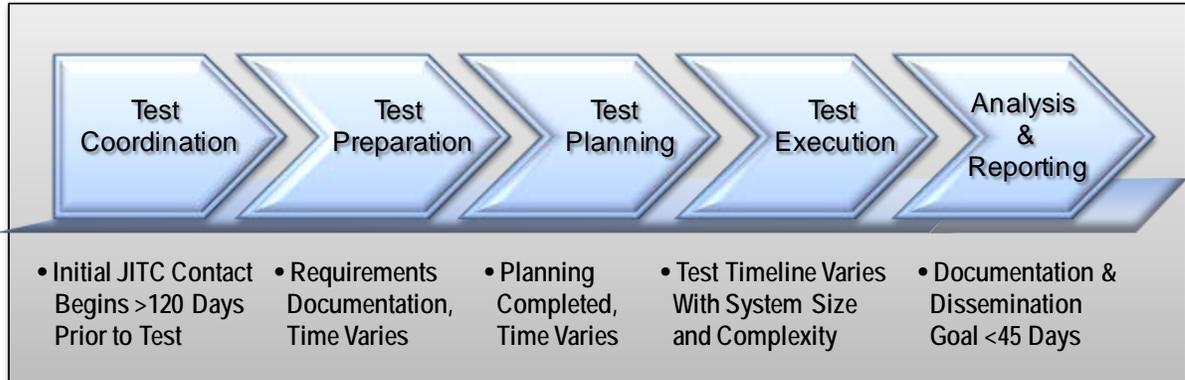


Figure 5-2. Certification Testing Timeline.

b. Certification Products. A family of reporting products has been introduced to document test and certification activities. The interoperability T&E products are described below and illustrated in Figure 5-3. The figure highlights reporting products and possible outcomes resulting from successful or failed testing. In addition, see Figure 5-4 below for a summary of current and previous reporting methods.

(1) Joint Interoperability Certification. A Joint Interoperability Certification is issued 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. Conditional certification limits the operational use of the system to only those functions and interfaces that were adequately demonstrated. The PMO must continue to work toward achieving a full Joint Interoperability Certification without conditions.

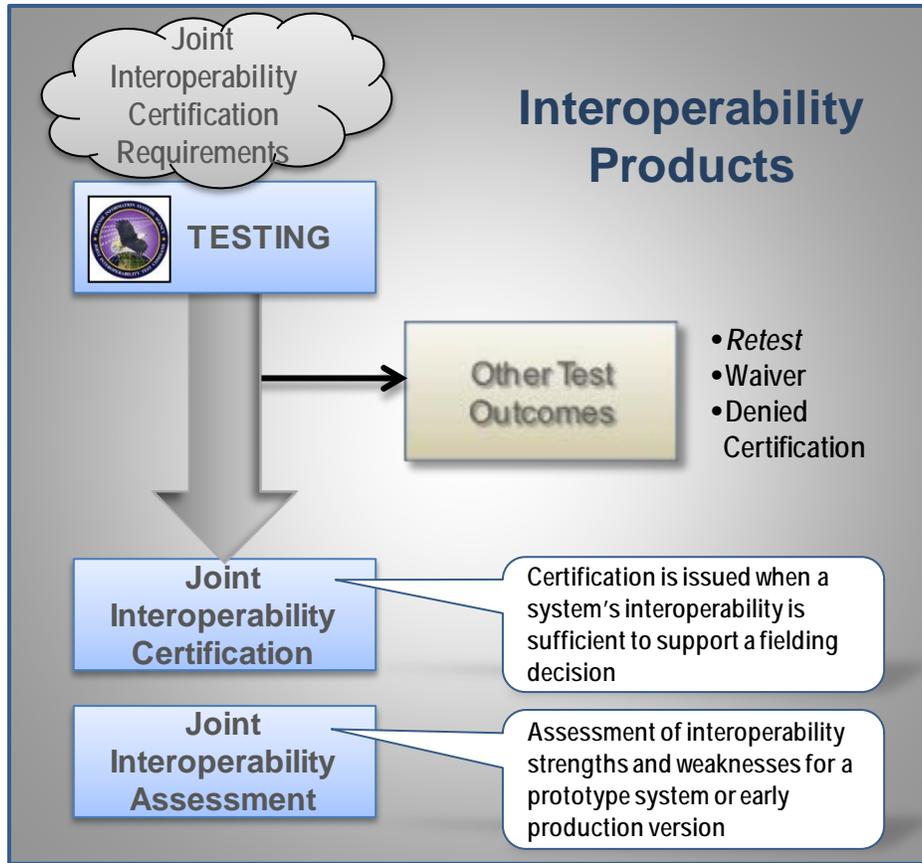


Figure 5-3. Interoperability T&E Products.

(b) Certification for Systems Developed in Increments. A Joint Interoperability Certification may be issued 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 re-certification.

(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 program manager's 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, 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.

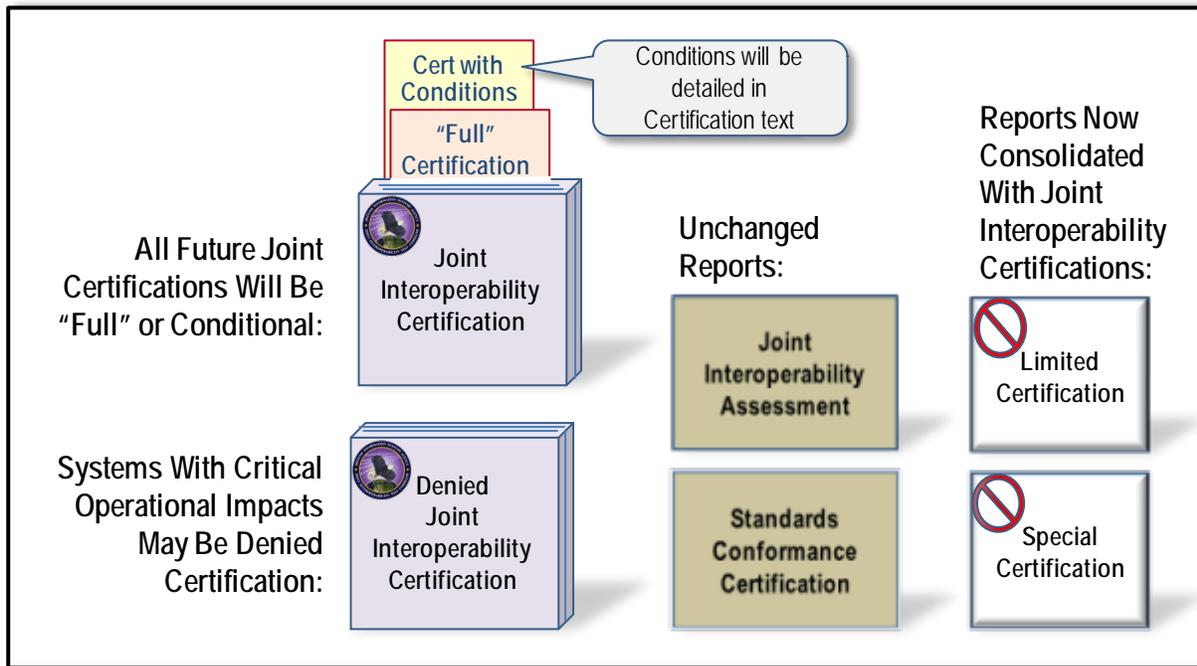


Figure 5-4. JITC Interoperability Products.

(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 test 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. These cases shall be raised to the proper authority, and all organizations that received the original certification notice shall be notified of changes in interoperability certification status pending resolution of issues.

6. Interim Certificate To Operate (ICTO) Process

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 references (b) and (c).

a. ICTO Process.

(1) The DoD CIO, in coordination with the USD(AT&L) and the Chairman of the Joint Chiefs of Staff (CJCS), 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 (c), 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) 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 Program Manger (PM) 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) Fielded systems that do not have approved interoperability requirements required for Joint Interoperability Certification must request an ICTO and pursue interoperability certification, or request a "Waiver to Policy" (see below) to continue operation. Fielded systems validated through a Joint Urgent Operational Need or Joint Emergent Operational Need, as defined in Reference (i), 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) Additional instructions regarding the ICTO procedures, templates, and ISG Points-of-Contact (POCs) are located on JITC's ISG Resource website: <http://jitc.fhu.disa.mil/cgi/isgsite/index.aspx>.

(8) All ICTO letters and status information are located in JITC's System Tracking Program (STP) (reference (m)) under the "Main Menu/Reports/ICTO Report" section (refer to <https://stp.fhu.disa.mil>).

(9) Operational systems, for which ICTO requests have expired without action by the PM/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 not normally 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. The procedures for processing ICTO requests are depicted in Figure 6-1 below.

(1) The PM/sponsor completes an ICTO request. Templates and forms for ICTO requests are on the JITC ISG Resource website <http://jitc.fhu.disa.mil/cgi/isgsite/ictoreqs.aspx>. JITC cannot submit requests for ICTOs. JITC will provide a recommendation for approval or disapproval of the ICTO request.

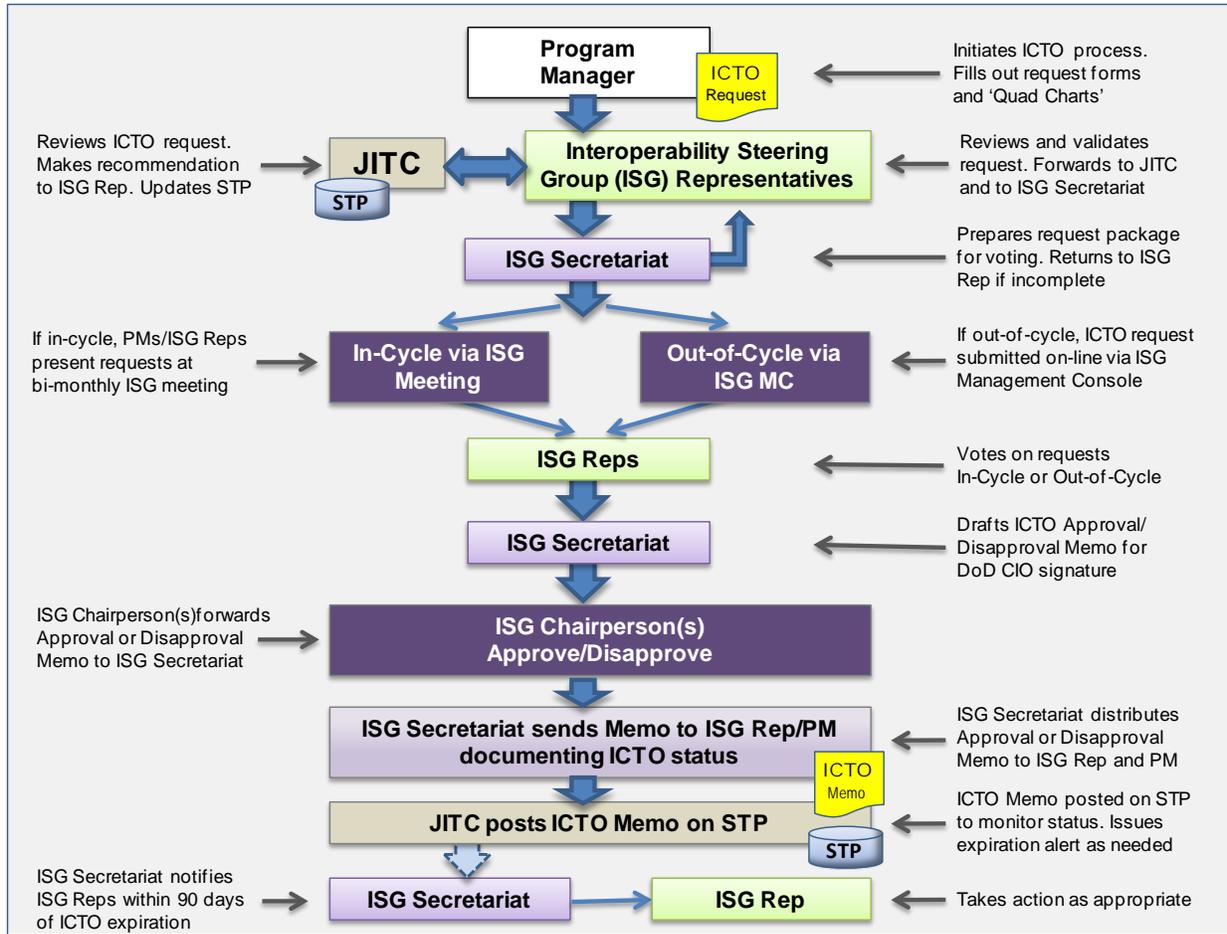


Figure 6-1. Procedures for Processing ICTO Requests.

(a) When requesting an “initial” ICTO, the PM/sponsor must submit the requisite ICTO Quad Chart and Systems Viewpoint (SV)-1 diagram through their respective Combatant Command/Service/Agency (CC/S/A) ISG representative. PMs/sponsors submitting initial ICTO requests will work with the respective ISG representative to initiate contact with JITC, and identify a JITC Action Officer (AO). The JITC AO shall assign an STP number prior to submission and gather information about the program’s capabilities and begin the cost estimating process for obtaining Joint Interoperability Certification.

(b) When requesting an ICTO “extension,” the PM/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.

(2) The PM/sponsor shall send the ICTO request to the respective ISG representative. The ISG POC List contains a complete list of ISG representatives and contact information. This list is located on JITC's ISG Resource website <http://jitic.fhu.disa.mil/cgi/isgsite/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 PM/sponsor for corrective action. Only ISG representatives can submit ICTO requests to the JITC AO.

(4) JITC AO input shall be provided either "In-Cycle" (during ISG meetings) or Out-of-Cycle (OOC) via the web-based ISG Management Console (located at <http://jitic.fhu.disa.mil/cgi/isgsite>).

(5) 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.

(6) 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.

(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 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) PMs/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) PMs/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 5 business days after receipt of the email notification.

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

(11) The ISG Secretariat 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 waivers for interoperability test and certification of DoD Component-unique (i.e., no joint, multinational, or interagency interoperability requirements) IT. 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 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 knowledge of systems supporting the warfighter. 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 DOT&E, and the CJCS, shall consider waivers to this policy 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 OSD or DoD Component head concerned.

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

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

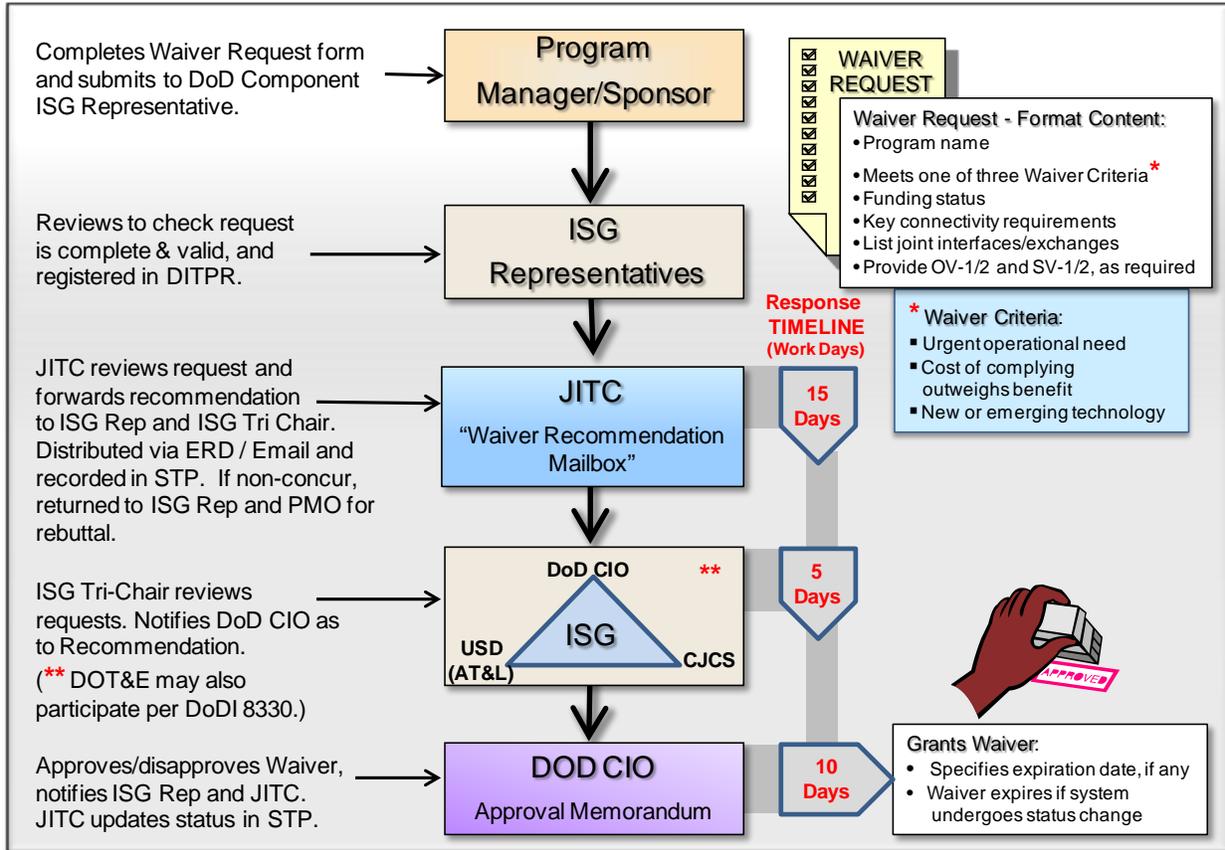


Figure 7-1. Waiver To Policy Process.

(2) 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 criteria, the rationale for the waiver, the capability it 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.

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

(4) 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.

(5) 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).

(6) 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 days of the receipt of all required information. The Joint Staff and USD(AT&L) shall have 5 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 Program Office and advise them of the opportunity to provide a rebuttal to the recommendation. Rebuttals should be addressed to the DoD CIO and returned to JITC within 7 working days from the receipt of the recommendation. 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 JS, AT&L, and DoD CIO for review and determination.

(7) DoD CIO shall approve or disapprove the waiver within 10 working days of receipt of the JITC recommendation or adjudication/resolution by the ISG. If approved, the system shall be waived from the interoperability requirements of the policy cited in the request form. 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). Recommendations for waiver rescissions shall be provided to the ISG for consideration and recommendation with a final determination from the DoD CIO.

f. Unified Capabilities (UC) Waiver Requests.

(1) In accordance with DoDI 8100.04, the DoD CIO may grant waivers to policy for UC:

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

(b) To accommodate the introduction of new or emerging technology pilot programs that have been coordinated with and recommended by the Director, DISA, and validated by the head of the OSD agency or DoD component concerned.

(2) To obtain a waiver to policy for UC products, the acquiring activity must prepare a site-specific request in memorandum format, to include the reason compliance is not possible and to identify the proposed equipment configuration. These requests shall be forwarded to the DoD CIO and DISA for review and consideration (refer to the UC APL Process Guide (reference (h))).

(3) Only in exceptional circumstances, and with DoD CIO approval, shall extensions of UC waivers be granted. The DISA Unified Capabilities Certification Office (UCCO) shall maintain a database to track the status of waivers granted for UC products.

8. Operating At Risk List (OARL)

a. Purpose. 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.

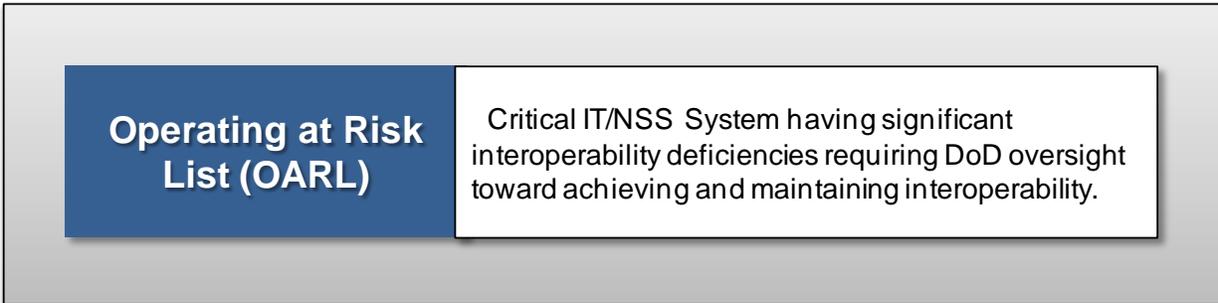


Figure 8-1. OARL Description.

b. Criteria. The OARL shall list all systems that have been denied an ICTO and/or are operating on a DoD network without having obtained a Joint Interoperability Certification, an ICTO, or a waiver to policy. Criteria for nominating programs to the OARL, described in Figure 8-1 above, 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 (TTP), 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 (OIPTs)).
- (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 (non-ACAT) IT); the CJCS; the DoD Component CIOs; the Commander, U.S. Strategic Command (USSTRATCOM); and the DISA 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>.

e. Effect. Placement on the ISG 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 and the DoD Information Network (DoDIN) (previously Defense Information Systems Network (DISN)) 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 it is determined that 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.

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. 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 life-cycle 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 (reference (b)). 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 the Joint Interoperability Certification. However, they may require accreditation if used for testing, and are not automatically exempt from cybersecurity, spectrum, network connection and similar policy.

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 (m)), 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)

a. Joint Interoperability Certification Requirements Overview. The GTG-F (reference (n)) 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.

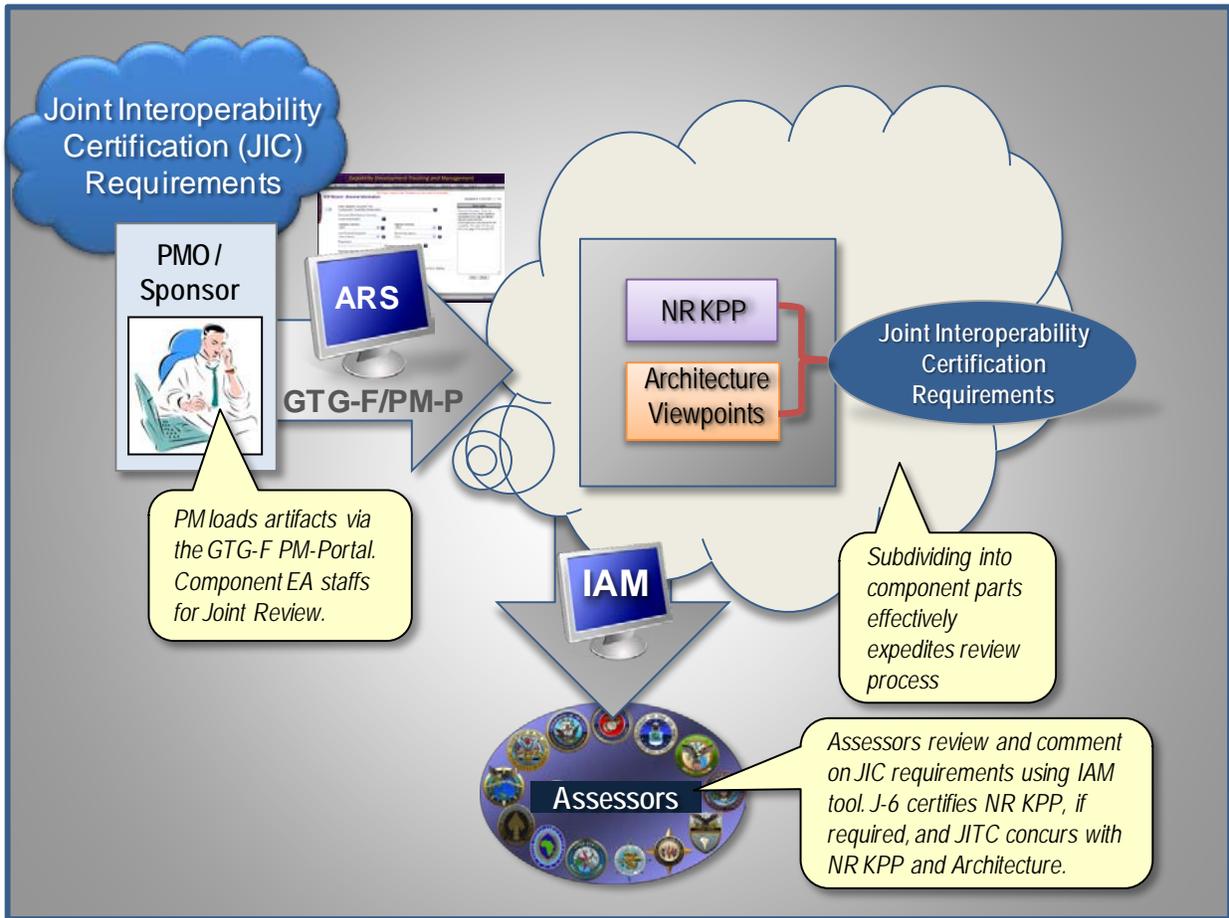


Figure 10-1. Joint Interoperability Certification Requirements Process Overview.

b. Joint Interoperability Certification Requirements Generation and Review. PMO/Sponsor development of interoperability requirements for Joint Interoperability Certification under the new paradigm uses the federated suite of tools found in the GTG-F, under the Program Management Portal (PM-P) using the Architecture Review Service (ARS) module 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 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) Unresolved issues will be addressed by the ISG.

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. The review and approval process is depicted in Figure 10-2.

(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 Capability Development Document (CDD)/Capability Production Document (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 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 has involved JITC in early development of the required architecture, the system should be ready for T&E leading to Joint Interoperability Certification.

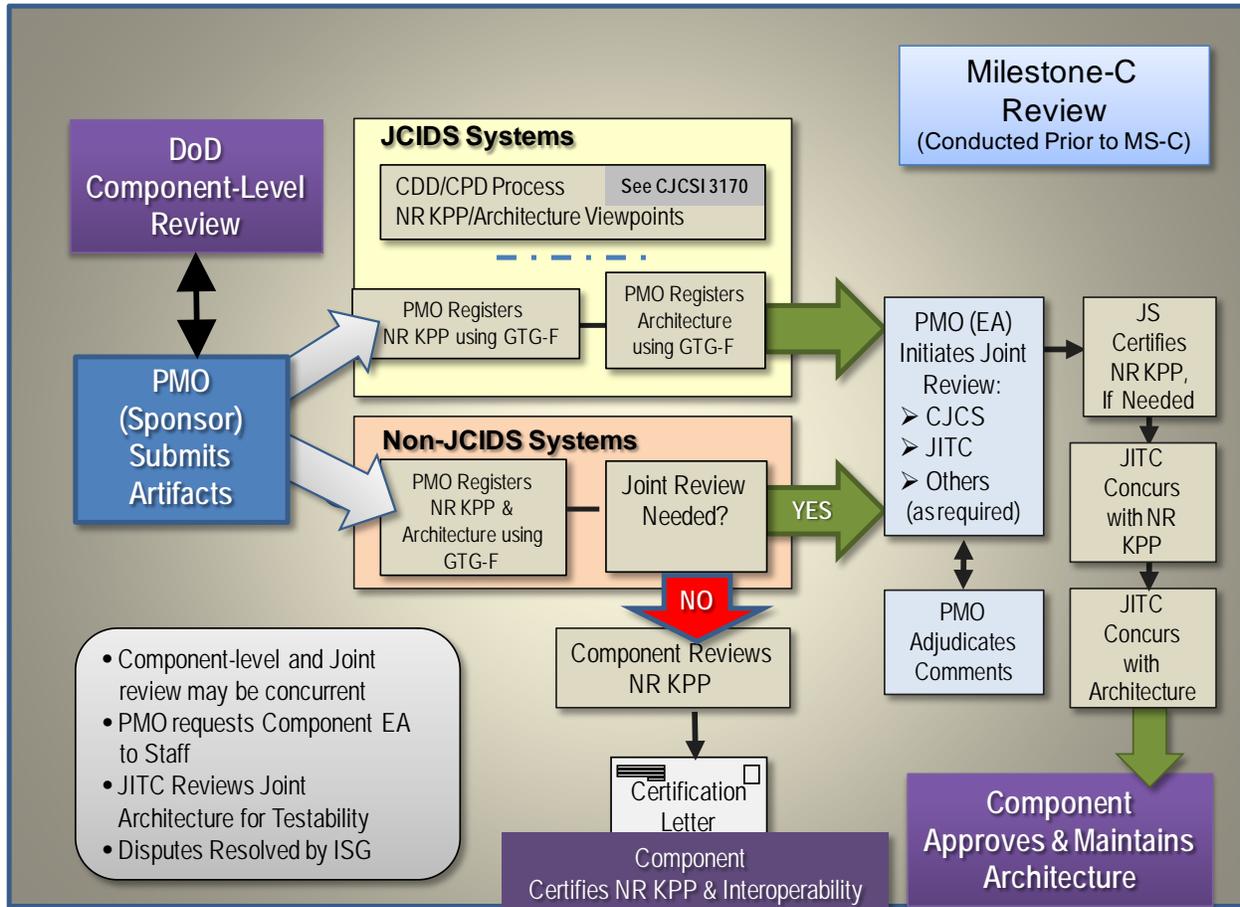


Figure 10-2. Joint Interoperability Certification Requirements Process.

d. ARS Overview. Detailed instructions for using the ARS are available on the GTG-F. Implementation of the ARS allows for early review and approval of the NR KPP and architecture required for Joint Interoperability Certification. Use of the ARS expedites the determination that the architectures contain sufficient data to support Joint Interoperability Certification. Additionally, the use of the ARS allows the program to obtain Joint Staff, J-6, certification of the NR-KPP prior to review and approval of other documentation.

e. ARS Utilization. All architecture products and the NR-KPP are registered by the developer with the GTG-F’s PM-P module under the ARS tab. The architectures and NR KPP are then staffed for review and approval.

f. 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 life-cycle of the system.
- (2) Testers and developers/reviewers of future increments will need access beyond the initial review. Changes must be tracked so that version artifacts already reviewed, certified, and approved are readily identifiable.

11. Minimum Set of Architecture Information Required for Joint Interoperability

Certification. JITC, as the Joint Interoperability Certification Authority, relies upon certain DoDAF architecture viewpoint information to perform joint interoperability evaluation and certification. These viewpoints are a subset of that required for Joint Staff NR KPP certification. PMs should coordinate with JITC early in the development of the NR KPP and architecture viewpoints to optimize the allocation of resources use for test and certification.

a. **Detailed Interoperability Architecture Requirements and Interoperability Requirements Processing.** Detailed information on the minimum set of architecture requirements and related elements is available on the ISG Resource website: <http://jitic.fhu.disa.mil/cgi/isgsite/index.aspx>. Additional architecture information is available at the Joint Staff Warfighting Mission Area (WMA) Architecture Federation and Integration Portal: <https://sadie.nmci.navy.mil/jafe/default.aspx>. 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.

b. **Minimum Set of Architecture Viewpoints Required for Joint Interoperability Certification.** Figure 11-1 is a summary of 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 architecture information that is mandatory to evaluate the interoperability of a system. “Conditional” viewpoints are those that are mandatory under certain conditions (i.e., when the conditions are met), but are otherwise not necessary for interoperability test and evaluation. “Optional” viewpoints are those that contain information potentially useful to an interoperability evaluation, but are not mandatory in all situations. PMs need to coordinate with the JITC AO to establish specific architecture viewpoint requirements, and ensure those requirements are sufficiently complete, detailed, and measurable and testable. Conditional information is required when:

(1) DIV-2 and DIV-3 are required when a system produces or consumes IT services or shared data (e.g., enterprise, cloud).

(2) StdV-1 is required when other viewpoints do not provide complete standards implementation information. The information on standards should be included when a system (whether in a separate StdV-1 or associated with other products), is dependent on other interfacing systems and services implementing compatible standards/standards profiles.

(3) SV-5b is required if the SV-5a, in conjunction with the SV-6 and other viewpoints, does not contain the elements required for interoperability evaluation. Specifically, the SV-5b is key to post-test analysis in localizing the source of failures, and potentially resulting in cost-avoidance and certification delays. The architecture viewpoint information will :

(a) Identify which systems perform which functions.

(b) Identify which system resource exchanges automate which operational resource exchanges.

(4) SvcV-1 through SvcV-7 (with the exception of SvcV-3) are mandatory when the system produces/consumes services or shared data.

| Viewpoint | Description |
|--|--|
| <u>REQUIRED</u> Architecture Viewpoints for Joint Interoperability Certification | |
| AV-1 | Overview of architecture scope and context, describes the concepts contained in the OV-1. |
| AV-2 | Integrated Dictionary – defines all terms and metadata used in the architecture. |
| OV-1 | High Level Operational Concept Graphic – describes operational concept. |
| OV-2 | Operational nodes, needlines, and activities - information exchanges between operational nodes. |
| OV-3 | Information exchanges and associated measures and metrics. |
| OV-5b | Operational Activity Model - NR KPP Missions/Tasks - activity level depiction. |
| OV-6c | Event-Trace Description - lifelines (nodes) and events. |
| SV-1 | Systems Interface Description - defines system functions and information flow among systems. |
| SV-2 | Systems Resource Flow Description - communications links, networks, and systems. |
| SV-5a | Maps system functions (activities) to operational activities. |
| SV-6 | System data exchanges & associated measures and metrics. |
| SV-7 | Complete set of system performance parameters (measures). |
| <u>CONDITIONAL</u> Architecture Viewpoints for Joint Interoperability Certification | |
| DIV-2 | Logical Data Model - architecture data definitions. |
| DIV-3 | Physical Data Model - describes how DIV-2 is implemented. |
| StdV-1 | Standards Profile - list of implemented technical standards, rules, and guidelines. |
| SV-5b | Maps systems to operational activities. |
| SvcV-1 | Services Context Description – identifies services and their interconnections. |
| SvcV-2 | Specifies resource flows exchanged between services, and may list protocol stacks. |
| SvcV-4 | Depicts allocation of service functions and data flows between service functions (activities). |
| SvcV-5 | Maps services (activities) to operational activities. |
| SvcV-6 | Maps service data exchanges with associated measures and metrics. |
| SvcV-7 | Complete set of performance parameters (measures) of the services. |
| <u>OPTIONAL</u> Architecture Viewpoints for Joint Interoperability Certification | |
| CV-all | Capability Viewpoints – taxonomy, capability evolution, etc. |
| OV-4 | Key architecture players and organizational relationships. |
| OV-5a | Describes capabilities and operational activities. |
| PV-all | Project capability delivery and dependencies. |
| StdV-2 | Emerging standards (may be conditional if emerging standards are implemented and not in StdV-1). |
| SV-4 | Defines data flow input and output by each function (activity). |

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

Appendix A References

- a. DoD Directive 4630.05, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” 5 May 2004. Certified Current as of April 23, 2007. Available at: <http://www.dtic.mil/whs/directives/index.html>
- b. DoD Instruction 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” 30 June 2004. Available at: <http://www.dtic.mil/whs/directives/index.html>
- c. DoD CIO memorandum, “Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS),” 27 March 2012.
See: <http://jitic.fhu.disa.mil/cgi/isgsite/pubs.aspx>
- d. CJCSI 6212.01F, “Net Ready Key Performance Parameter (NR KPP),” 21 March 2012. Available at: http://www.dtic.mil/cjcs_directives/
- e. Net Ready Key Performance Parameter (NR KPP) Manual. Available at: [https://intellipedia.intelink.gov/wiki/Net_Ready_-_Key_Performance_Parameter_\(NR-KPP\)_Manual](https://intellipedia.intelink.gov/wiki/Net_Ready_-_Key_Performance_Parameter_(NR-KPP)_Manual).
- f. Unified Capabilities Requirements (UCR). Available at: <http://www.disa.mil/Services/Network-Services/UCCO/>
- g. DoDI 8100.04, “DoD Unified Capabilities (UC),” 9 December 2010. Available at: <http://www.dtic.mil/whs/directives/index.html>
- h. Approved Products List (APL) Process Guide. Available at: <https://aplists.disa.mil>.
- i. CJCSI 3170.01H, “Joint Capabilities Integration and Development System,” 10 January 2012. Available at: http://www.dtic.mil/cjcs_directives/
- j. Manual for the Operation of the Joint Capabilities Integration and Development System. Available at: https://www.intelink.gov/wiki/JCIDS_Manual
- k. NR KPP Resource Page.
See: https://intellipedia.intelink.gov/wiki/Portal:NR_KPP_Resource_Page.
- l. DoD Architecture Framework (DoDAF). See: <http://dodcio.defense.gov/dodaf20.aspx>
- m. JITC System Tracking Program. See: http://jitic.fhu.disa.mil/stp_info.html.
- n. GIG Technical Guidance Federation (GTG-F).
See: <https://gtg.csd.disa.mil/uam/homepage.do>

Appendix B Abbreviations and Acronyms

| | |
|---------|---|
| ACAT | Acquisition Category |
| AO | Authorizing Official (cybersecurity) |
| AO | Action Officer (JITC) |
| APL | Approved Products List |
| ARS | Architecture Review Service |
| CAO | Connection Approval Office |
| C/S/A | Combatant Command/Service/Agency |
| 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 AO) |
| DISA | Defense Information Systems Agency |
| DISN | Defense Information Systems Network |
| DISR | DoD Information Technology Standards Registry |
| DITPR | DoD Information Technology Portfolio Repository |
| DoD CIO | Department of Defense Chief Information Officer |
| DoDAF | DoD Architecture Framework |

| | |
|----------|---|
| DoDD | Department of Defense Directive |
| DoDI | DoD Instruction |
| DoDIN | DoD Information Network |
| DOT&E | Director, Operational Test and Evaluation |
| DOTLPF | Doctrine, Organization, Training, Leadership and Education, Personnel, and Facilities |
| DOTLPF-P | DOTLPF and Policy |
| DT&E | Developmental Test and Evaluation |
| EA | Executive Agent (GTG-F) |
| GEOINT | Geospatial Intelligence |
| GIG | Global Information Grid |
| GTG-F | GIG Technical Guidance Federation |
| HF | High Frequency |
| IA | Information Assurance (now cybersecurity) |
| IAM | Interoperability & Supportability Assessment Module (GTG-F) |
| ICA | Interface Control Agreement |
| ICEP | Interoperability Certification Evaluation Plan |
| ICTO | Interim Certificate To Operate |
| IOC | Initial Operational Capability |
| 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 |
| JITC | Joint Interoperability Test Command |
| JMT | Joint Mission Thread |
| KPP | Key Performance Parameter |
| MDA | Milestone Decision Authority |
| MIB | Military Intelligence Board |
| MOE | Measure of Effectiveness |
| MOP | Measure of Performance |
| NCR | National Capital Region |
| NGA | National Geospatial-Intelligence Agency |
| NR KPP | Net-Ready Key Performance Parameter |
| NSA | National Security Agency |
| NSS | National Security Systems |
| OA | Operational Assessment |
| 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) |
| 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 |
| USD(AT&L) | Under Secretary of Defense (Acquisition, Technology, and Logistics) |
| USSTRATCOM | U.S. Strategic Command |
| VHF | Very High Frequency |
| WMA | Warfighting Mission Area |

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. [derived from CJCSI 6212.01]

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. [CJCSI 6212.01]

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. [CJCSI 6212.01]

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 and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life-cycle and must be balanced with cybersecurity. [Reference (b)]

Interoperability Certification. A formal statement of adequacy provided by the responsible Interoperability Certification Authority that a system has met its interoperability requirements. [Reference (b)]

Interoperability Certification Authority. The office with the certification authority for interoperability. Ensures that the IT or NSS has met its interoperability requirements, as demonstrated via test and evaluation. For IT or NSS with joint interoperability requirements, the Interoperability Certification Authority is JITC. For all other IT and NSS, the Interoperability Certification Authority will be determined by the owning DoD Component. [derived from Reference (c)]

Interoperability Certification Evaluation Plan (ICEP). A JITC plan, developed in conjunction with the PM/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 PM/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 CJCSI 6212.01 and other sources]

Joint Capabilities Integration and Development System (JCIDS). A Chairman of the Joint Chiefs of Staff process to identify, assess, validate, and prioritize joint military capability requirements. The JCIDS process is a collaborative effort that uses joint concepts and DoD Information Enterprise Architecture and solution architectures to identify prioritized capability gaps and integrated solutions (materiel and non-materiel) to resolve those gaps. [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 CJCSI 6212.01 and other 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 CJCSI 6212.01 and other 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.

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. [CJCSI 6212.01]

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]

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]

(INTENTIONALLY BLANK)