Department of Defense

Interoperability Process Guide

Version 3.0
July 2023

(This page intentionally left blank.)

Interoperability Process Guide

The Interoperability Process Guide (IPG) is developed and published by the Joint Interoperability Test Command (JITC) in coordination with the Interoperability Steering Group (ISG) Tri-Chairs. It is effective immediately upon publication. The IPG is available at: https://jitc.fhu.disa.mil/projects/isgsite. Errata identified between major releases will be posted at the same location.

Submitted:

MORALES.MICH
AEL.1249906235
Digitally signed by
MORALES.MICHAEL.1249906235
Date: 2023.06.22 14:18:19 -07'00'

Mr. John LeCompte
Chief, Strategy, Plans, and Automations Division
Joint Interoperability Test Command (JITC)

Approved:

MATTHIAS.ROBERT.
DENNIS.114825077
0
Digitally signed by
MATTHIAS.ROBERT.DENNIS.1148
250770
Date: 2023.06.22 17:17:18 -07'00'

Robert D. Matthias
Captain, USN
Commander, Joint Interoperability Test Command

ZAMBERLAN.MARK.
ALBERT.107695838
2
Digitally signed by
ZAMBERLAN.MARK.ALBERT.107695
8382
Date: 2023.06.23 08:22:46 -04'00'

Mr. Mark Zamberlan
Tri-Chair, ISG (DoD CIO)

MCROBIE.ROBERT
.W.JR.1043359122
Digitally signed by
MCROBIE.ROBERT.W.JR.104335912
2
Date: 2023.06.23 09:59:17 -04'00'

Mr. Robert McRobie, Jr.
Tri-Chair, ISG (JS J6)

PETERSON.KEVIN.B
RYAN.1047219732
Digitally signed by
PETERSON.KEVIN.BRYAN.104721
9732
Date: 2023.06.23 10:23:54 -04'00'

Mr. Kevin Peterson
Tri-Chair, ISG (OSD A&S)

(This page intentionally left blank.)

Summary of Changes

Version	Sections Affected	Description of Change
Version 1.0 (10 September 2012)	All	Initial approved version.
Version 1.0, Change 1 (April 2014)	All	- 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.
Version 2.0 (23 March 2015)	All	- Administrative corrections. - Updated references based on new DoDI 8330.01 and cancellation of DoDD 4630.05, DoDI 4630.8, and DoD CIO memorandum, “Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS).” - Added staffing guidance on requirements document review. - Added criticality definitions for requirements review comments. - Inserted Network Connection clarification. - Updated Operating at Risk List section. - Updated Recertification section. - Updated Waiver to Policy section. - Updated Architecture section.
Version 2.0 Change 1 (30 October 2018)	All	- Added Appendix D to address TE-21 Reform Initiative and JITC Automation. - Removed references to USSTRATCOM in Recertification Procedures section and OARL section.

Summary of Changes (continued)

Version	Sections Affected	Description of Change
Version 3.0 (July 2023)	All	- Administrative corrections. - Updated title of guide to DoD IPG; guide approval is now by ISG Tri-Chairs and JITC Commander. - General: Updated content to align with new DoDI 8330.01, CJCSI 5123.01I, 2021 JCIDS Manual, DoDD 5000.01, DoDI 5000.02 and the supporting acquisition pathway issuances. - Updated Pre-T&E and T&E sections to include initial conditions/assumptions. - Added JIEP and TSP and removed ICEP. - Updated Post-T&E Procedures sections to include updated Recertification procedures. - Updated Waiver to Policy section. - Updated Operating at Risk List section. - Updated Supporting Evaluations and Resources section. - Updated Architecture section (required and conditional viewpoints). - Added definitions for End-to-End Testing, GTG-F, Net-Ready, Net-Ready Certification Authority, Net-Ready performance attribute, and Test and Evaluation. - Added Appendices E and F to address ISP and (non-ISP) AAF requirements processes, respectively.

TABLE OF CONTENTS

SECTION **PAGE**

1. Purpose 1
2. Overview of Interoperability Policy and Certification Process 2
3. Pre-Test and Evaluation Procedures (planning) 7
4. Test and Evaluation Procedures (execution) 17
5. Post-Test and Evaluation Procedures (reporting) 21
6. Interim Certificate to Operate Procedures 31
7. Waivers to IT Interoperability Policy 36
8. Operating At Risk List 40
9. Supporting Evaluations and Resources 42
10. Requirements for Joint Interoperability Certification 44
11. Minimum Set of Architecture Information Required for Joint Interoperability Evaluation 49
Appendix A References 52
Appendix B Abbreviations & Acronyms 54
Appendix C Definitions 59
Appendix D Process Improvement Through Automation 66
Appendix E ISP Process 68
Appendix F Requirements Process for Other Acquisition Pathways 72

TABLE OF FIGURES

FIGURE **PAGE**

Figure 2-1. Interoperability Policies and Guidance 2

Figure 2-2. Joint Interoperability Certification T&E Overview 4

Figure 2-3. Notional Joint Interoperability Certification Process 6

Figure 3-1. Pre-T&E Activities 7

Figure 3-2. NR KPP Focus 8

Figure 3-3. Policies Governing Requirements Preparation 10

Figure 4-1. T&E Activities 17

Figure 5-1. Post-T&E Activities 21

Figure 5-2. T&E Products 22

Figure 5-3. Recertification Request Procedures Summary 26

Figure 6-1. Procedures for Processing ICTO Requests 33

Figure 7-1. Waivers to IT Interoperability Policy Process 37

Figure 8-1. OARL Description 40

Figure 10-1. Joint Interoperability Requirements Process Overview (Non-JCIDS) 44

Figure 10-2. Joint Interoperability Requirements Review and Approval Process 46

Figure 11-1. Required Architecture Viewpoints for Joint Interoperability Certification .. 50

Figure 11-2. Conditional Architecture Viewpoints for Joint Interoperability Certification 51

1. Purpose

The Interoperability Process Guide (IPG) provides implementing guidance for Department of Defense (DoD) Instruction (DoDI) 8330.01.

The IPG outlines the policy, process, and procedures required for Joint Interoperability Test, Evaluation, and Certification (TE&C), waiver to policy requests, and other related interoperability test and evaluation (T&E) activities. It addresses interoperability test and certification based on the Net-Ready Key Performance Parameter (NR KPP).

The IPG is intended for use by Program Managers (PMs)/Sponsors for the joint interoperability TE&C of information technology (IT) and national security systems (NSS) (referred to in this guide as “IT”) in accordance with DoDI 8330.01. The following describes the sections and appendices of the IPG:

a. Section 1 provides the purpose of the IPG.

b. Section 2 outlines the publications that govern joint interoperability TE&C, identifies key organizations that participate in drafting and implementing interoperability policy, and provides an overview of the joint interoperability TE&C process.

c. Sections 3 through 5 identify the processes, procedures, and guiding principles that cover planning, execution, and reporting for Joint Interoperability Certification (JIC).

d. Sections 6 through 8 outline the DoD, Chief Information Officer (CIO) processes and procedures for Interim Certificate to Operate (ICTO), Waivers to IT Interoperability Policy, and Operating at Risk List (OARL).

e. Section 9 provides information on supporting evaluations and related resources.

f. Sections 10 and 11 describe requirements for JIC, including the review process and a list of minimum required architecture information.

g. Appendices A through C cover references, abbreviations & acronyms, and definitions (respectively).

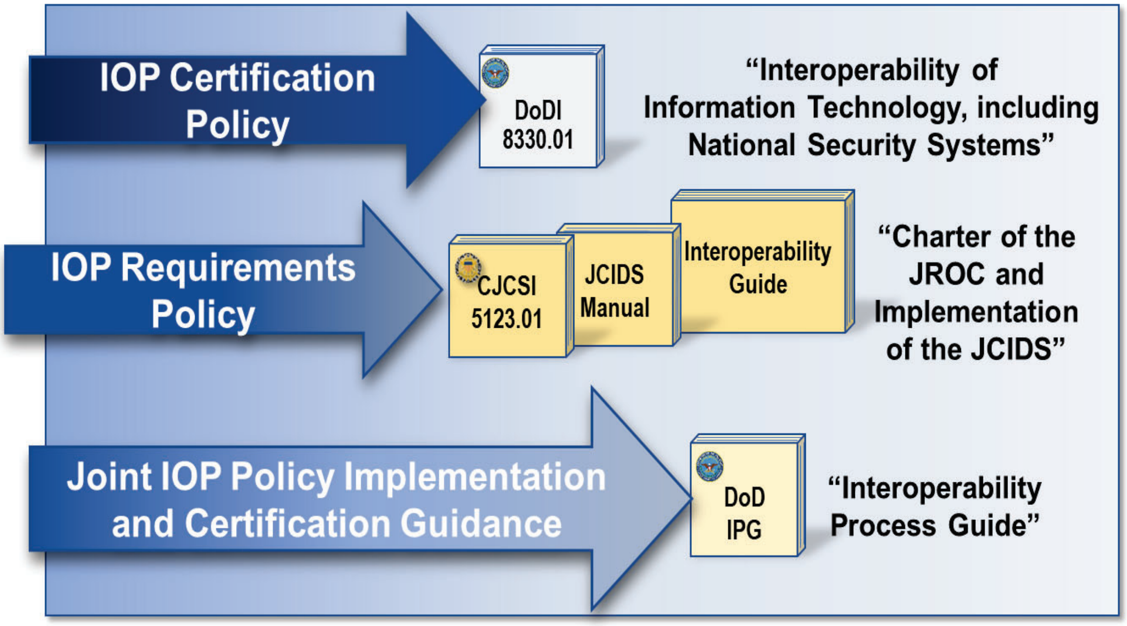
h. Appendix D outlines the framework to enable T&E process improvement through automation.

i. Appendix E outlines the Information Support Plan (ISP) process.

j. Appendix F outlines the processes for Component review of joint interoperability requirements products (non-Joint Capabilities Integration and Development System (non-JCIDS) for acquisition pathways that are not required to produce an ISP.

2. Overview of Interoperability Policy and Certification Process

a. Interoperability Policy. Several documents govern interoperability for the DoD. This section summarizes key instructions, manuals, and guides. Figure 2-1 depicts the high-level relationships among these documents.


IOP Certification Policy
DoDI 8330.01
"Interoperability of Information Technology, including National Security Systems"
IOP Requirements Policy
CJCSI 5123.01
JCIDS Manual
Interoperability Guide
"Charter of the JROC and Implementation of the JCIDS"
Joint IOP Policy Implementation and Certification Guidance
DoD IPG
"Interoperability Process Guide"

LEGEND:

CJCSI	Chairman of the Joint Chiefs of Staff Instruction	IPG	Interoperability Process Guide
DoD	Department of Defense	JCIDS	Joint Capabilities Integration and Development System
DoDI	Department of Defense Instruction		
IOP	Interoperability	JROC	Joint Requirements Oversight Council

Figure 2-1. Interoperability Policies and Guidance

(1) DoDI 8330.01 updated policy and procedures for interoperability of IT. DoDI 8330.01 states that IT capability must be evaluated and certified for interoperability prior to fielding of a new IT (system) or upgrading an existing IT. IT with a joint performance requirement (JPR) (e.g., joint interfaces or joint information exchanges with other IT) requires JIC.

(a) A joint interface is an interface between/among external partners. A joint interface occurs when any IT is joined through a logical connection with IT or data sources from an external partner for the purpose of exchanging data, sharing situational awareness, or partnering to perform a joint mission.

(b) A joint information exchange is an exchange of information/data between/among IT when any IT whose mission is joined through a logical connection with an IT or data sources from an external partner for the purpose of exchanging common data, sharing situational awareness, or partnering to perform a single mission (e.g., when one program such as Identity Management is consumed as part of data reuse efficiencies).

(2) The PM/Sponsor is required to develop Net-Ready performance attributes to define IT requirements in accordance with DoDI 8330.01 and the "Manual for the Operation of the Joint Capabilities Integration and Development System" (JCIDS Manual).

(a) Joint Staff determines whether the Net-Ready performance attribute should be designated a JPR. If designated a JPR, then the Net-Ready performance attribute is elevated to a key performance parameter (i.e., an NR KPP). If the Joint Staff determines that the IT has no JPR, then the Component will be responsible for the interoperability evaluation (i.e., no NR KPP).

(b) The Interoperability Guide (JCIDS Manual: Annex A, Appendix G, to Enclosure B) contains detailed information regarding the content and development process for the NR KPP. The DoD Architecture Framework (DoDAF) viewpoints provide the data used to populate the NR KPP.

(c) The term "Net-Ready content," when used in this guide, refers to the NR KPP and supporting architecture information. The Net-Ready content establishes the requirements the Joint Interoperability Test Command (JITC) uses to evaluate joint interoperability (i.e., assess the technical exchange of information, data, and services, and the end-to-end operational effectiveness of those exchanges through test and evaluation).

(3) Under the oversight and direction of the DoD CIO, JITC serves as the joint interoperability certification authority for all DoD IT with joint interoperability requirements. DoDI 8330.01 further specifies that JITC must certify IT for joint interoperability, based on a Joint Staff certified Net-Ready performance attribute.

(4) The Interoperability Steering Group (ISG) is established by DoDI 8330.01 for the general oversight of interoperability policy execution and operates under the executive authority of the ISG charter.

(5) The PM/Sponsor should contact their respective ISG member and coordinate with the Joint Staff to determine if their IT has a JPR. A list of Service/Agency ISG members can be found on JITC's ISG Resource website: https://jitc.fhu.disa.mil/projects/isgsite. Agencies not listed as chartered members of the ISG should coordinate directly with the ISG Executive Secretary for the processing of ICTO's, Waiver Requests, and other pertinent joint interoperability process issues.

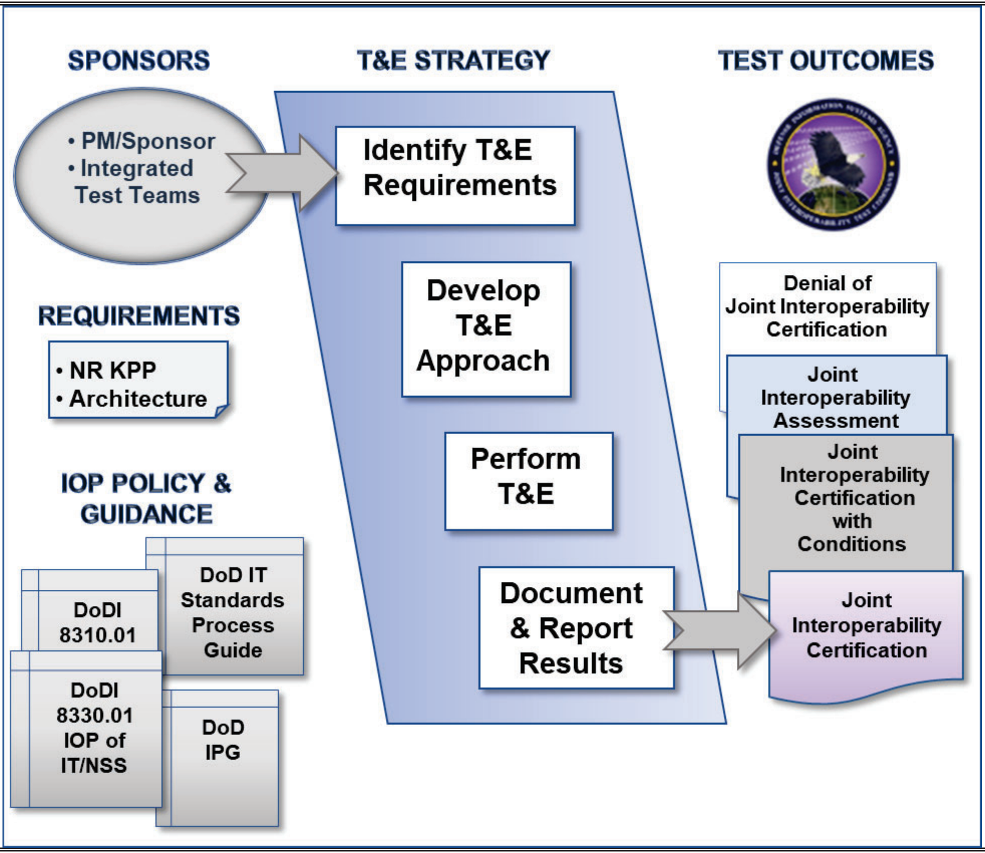
(6) The IPG outlines procedures to support joint interoperability TE&C, ICTO requests, waiver submissions, and OARL process. The IPG will be updated periodically.

(7) This IPG does not address certification processes for Department of Defense Information Network (DoDIN) Capabilities. Interoperability certification policy, requirements, and processes for DoDIN Capabilities (e.g., voice instruments, video, and mobile devices) are promulgated in the Unified Capabilities Requirements (UCR) Document, DoDI 8100.04, and the

DoDIN Approved Products List Process Guide. Further guidance can be found in the Approved Products List Integrated Tracking System at: https://aplits.disa.mil/.

(8) The PMs/Sponsors that do not have NR KPP or DoDAF architecture artifacts need to contact Joint Staff for guidance. See Section 10 of the IPG for more information on requirements for JIC.

b. Interoperability within the Acquisition Life-Cycle. Figure 2-2 depicts a typical joint interoperability T&E process. The PMs/Sponsors will coordinate with JITC (DoD's sole joint interoperability certifier) to tailor the TE&C approach for JIC based on their acquisition pathway and specific program needs. JITC T&E services are provided on a cost reimbursable basis.


SPONSORS
T&E STRATEGY
TEST OUTCOMES
• PM/Sponsor
• Integrated Test Teams
Identify T&E Requirements
REQUIREMENTS
• NR KPP
• Architecture
Develop T&E Approach
Denial of Joint Interoperability Certification
Joint Interoperability Assessment
Perform T&E
IOP POLICY & GUIDANCE
Joint Interoperability Certification with Conditions
DoDI 8310.01
DoD IT Standards Process Guide
Document & Report Results
Joint Interoperability Certification
DoDI 8330.01 IOP of IT/NSS
DoD IPG

LEGEND:

&	and	IT	Information Technology
DoD	Department of Defense	NSS	National Security Systems
DoDI	Department of Defense Instruction	NR KPP	Net-Ready Key Performance Parameter
IOP	Interoperability	PM	Program Manager
IPG	Interoperability Process Guide	T&E	Test and Evaluation

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

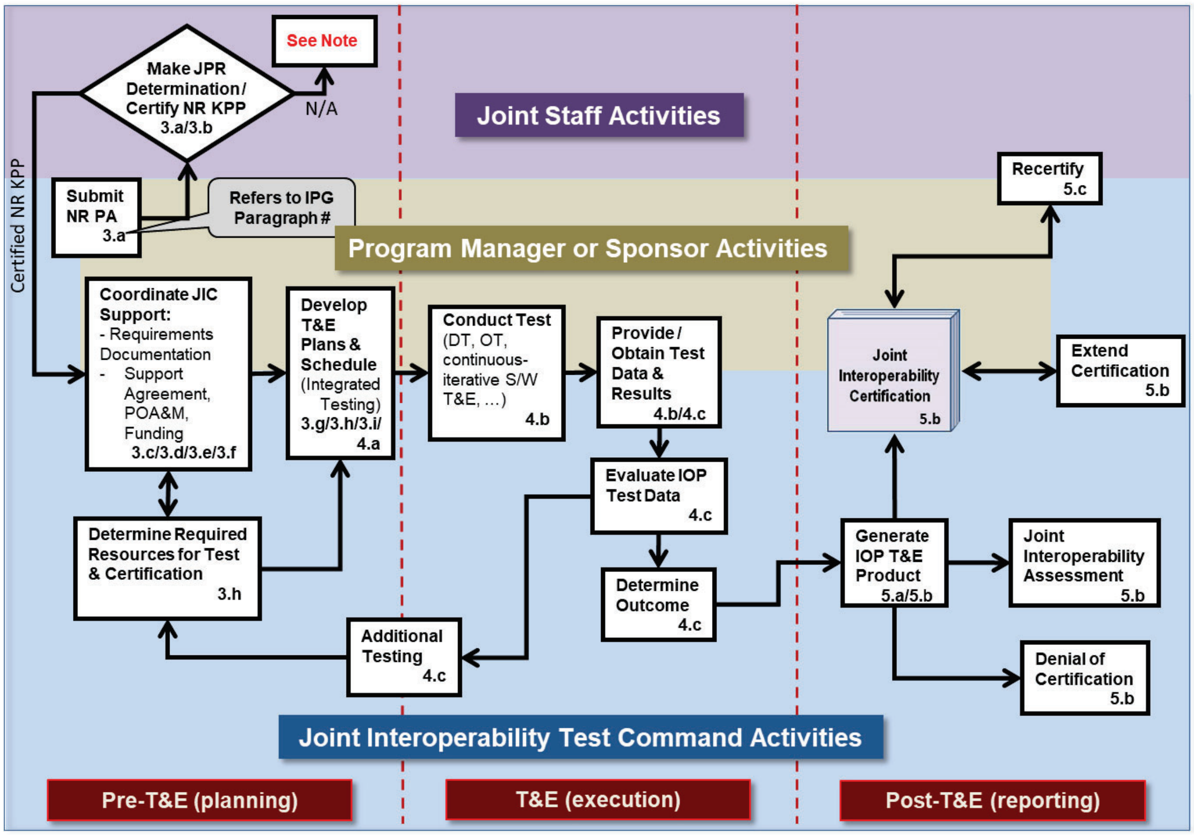
(1) Programs may use any test organization to conduct the testing, so long as they follow the prescribed processes detailed within this IPG. Programs may engage JITC to support their testing or execute their testing in totality. Regardless of the test method, JITC must concur with the data sources and evaluate the results to make an interoperability determination.

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

c. Operating at Risk List. If an IT is denied certification (due to an interoperability shortfall) or has not made significant progress toward achieving JIC, the IT may be placed on the OARL. The ISG Executive Secretary maintains the OARL on behalf of the ISG listing all IT operating on a DoD network without a JIC, ICTO, or approved waiver to DoDI 8330.01. See Section 8 of the IPG for OARL policy and procedures.

d. Network Connection. IT must satisfy at least one of these conditions before connection to any DoD network (other than for test purposes): (1) be certified for joint interoperability (2) possess an ICTO (3) possess a waiver to policy, or (4) be exempt from JIC (e.g., Joint Urgent Operational Need) in accordance with DoDI 8330.01. A JIC with conditions may be issued under certain circumstances. These conditions may constrain use of network interfaces that do not meet all critical requirements (threshold NR KPP) while not limiting use of other interfaces and associated information exchanges. The appropriate connection approval office determines final network connection approval with interoperability certification being merely one of the determining factors.

e. Joint Interoperability TE&C Process Overview. Sections 3 through 5 of the IPG detail the Joint Interoperability T&E phases. Figure 2-3 shows a notional process flow for a program of record; therefore, the steps would be applicable to most IT requiring a certification.


See Note
Make JPR Determination/ Certify NR KPP 3.a/3.b
N/A
Joint Staff Activities
Certified NR KPP
Submit NR PA 3.a
Refers to IPG Paragraph #
Program Manager or Sponsor Activities
Recertify 5.c
Coordinate JIC Support: - Requirements Documentation - Support Agreement, POA&M, Funding 3.c/3.d/3.e/3.f
Develop T&E Plans & Schedule (Integrated Testing) 3.g/3.h/3.i/ 4.a
Conduct Test (DT, OT, continuous-iterative S/W T&E, …) 4.b
Provide/ Obtain Test Data & Results 4.b/4.c
Joint Interoperability Certification 5.b
Extend Certification 5.b
Evaluate IOP Test Data 4.c
Determine Required Resources for Test & Certification 3.h
Determine Outcome 4.c
Generate IOP T&E Product 5.a/5.b
Joint Interoperability Assessment 5.b
Additional Testing 4.c
Denial of Certification 5.b
Joint Interoperability Test Command Activities
Pre-T&E (planning)
T&E (execution)
Post-T&E (reporting)

NOTE: If Net-Ready Certification is not required (i.e., no joint interoperability requirements), the PM/Sponsor should receive a Not Applicable memorandum from the Joint Staff. The authority to approve or certify the (non-joint) Net-Ready performance attribute passes to the DoD Component.

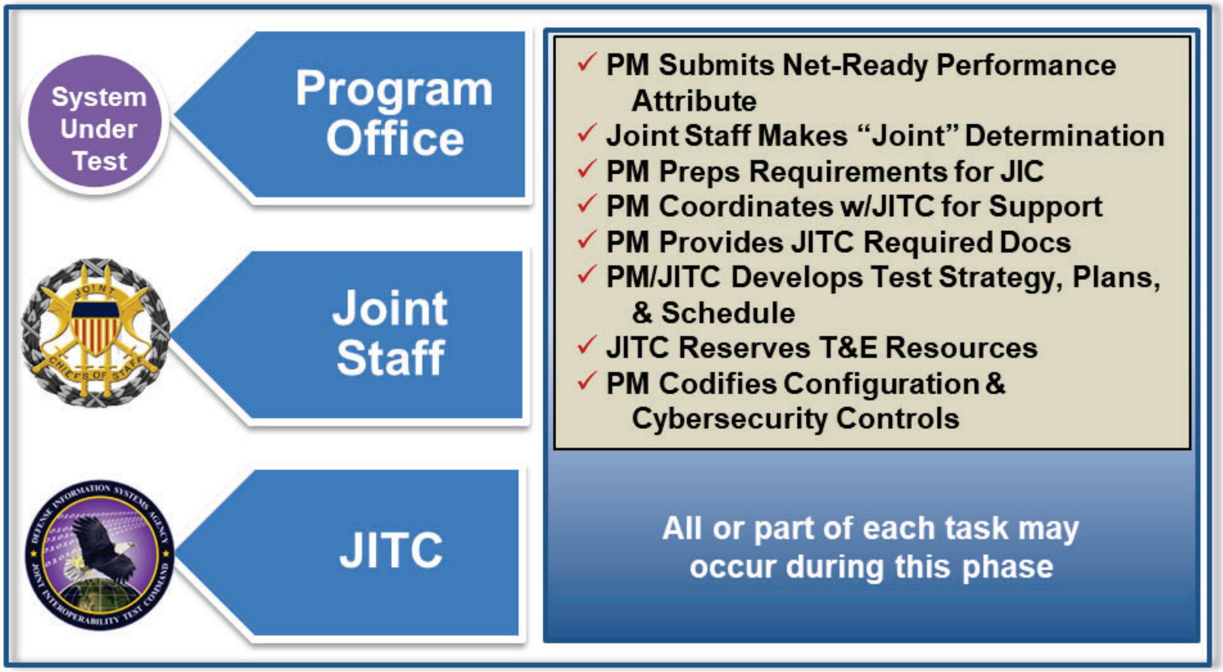
LEGEND:

&	and	NR KPP	Net-Ready Key Performance Parameter
#	Location (Paragraph)	PA	Net-Ready Performance Attribute
DT	Development Testing	OT	Operational Testing
IOP	Interoperability	POA&M	Plan of Action and Milestones
IPG	Interoperability Process Guide	S/W	Software
JIC	Joint Interoperability Certification	T&E	Test and Evaluation
JPR	Joint Performance Requirement		

Figure 2-3. Notional Joint Interoperability Certification Process

3. Pre-Test and Evaluation Procedures (planning)

Figure 3-1 typifies the range of test planning activities that routinely occur during the pre-T&E phase.



- ✓ PM Submits Net-Ready Performance Attribute
- ✓ Joint Staff Makes "Joint" Determination
- ✓ PM Preps Requirements for JIC
- ✓ PM Coordinates w/JITC for Support
- ✓ PM Provides JITC Required Docs
- ✓ PM/JITC Develops Test Strategy, Plans, & Schedule
- ✓ JITC Reserves T&E Resources
- ✓ PM Codifies Configuration & Cybersecurity Controls

All or part of each task may occur during this phase

LEGEND:

&	and	PM	Program Manager
Docs	Documents	T&E	Test and Evaluation
JIC	Joint Interoperability Certification	w/	With
JITC	Joint Interoperability Test Command		

Figure 3-1. Pre-T&E Activities

a. Initial Conditions/Assumptions. The program is acquiring and fielding an IT capability.

(1) The PM/Sponsor submitted the Net-Ready performance attribute to the Joint Staff for review.

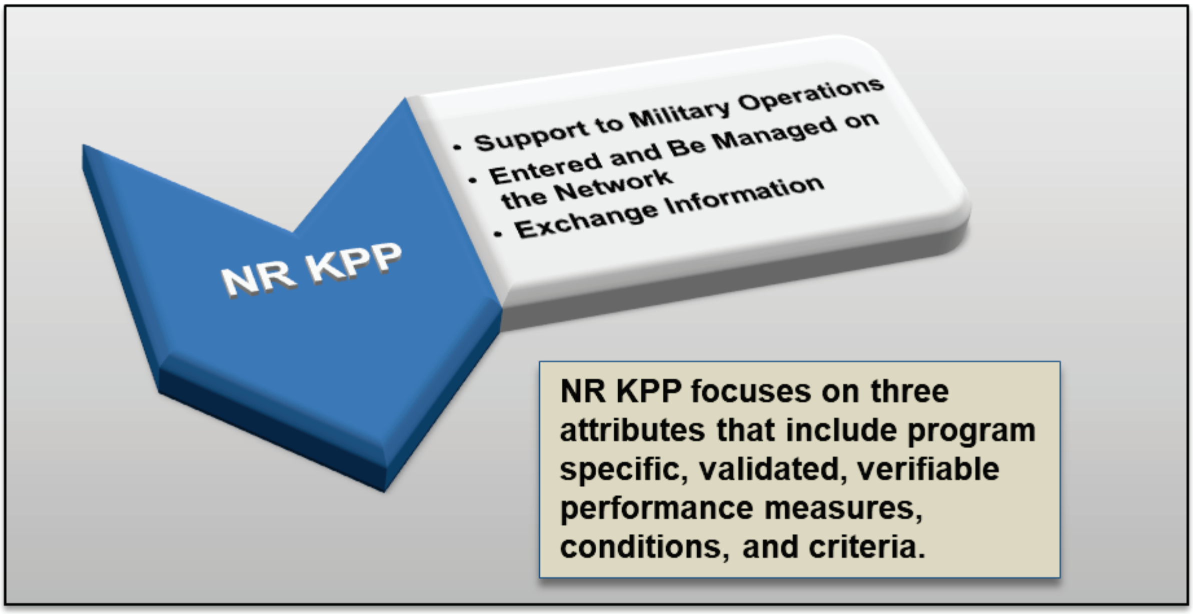
(2) Joint Staff determined there is a JPR (i.e., the IT has joint equities).

(3) The PM/Sponsor is coordinating with Joint Staff to prepare an NR KPP for joint DoD review via Knowledge Management and Decision Support (KM/DS) or Global Information Grid (GIG) Technical Guidance Federation (GTG-F).

(4) The program is pursuing a Net-Ready Certification (i.e., NR KPP) from the Joint Staff and a JIC from JITC.

(5) The PM/Sponsor initiated coordination with JITC to assess interoperability of the IT based on the NR KPP to support a JIC determination.

b. Interoperability Evaluation Framework. The three NR KPP attributes and the technical requirements defined in, or derived from, the solution architecture data are the framework for the JIC (see Figures 3-2 and 3-3 for information and policy about the NR KPP). An early step in preparation for JIC is a joint interoperability requirements review, which includes Joint Staff certification of the NR KPP. Information requirements, information timeliness, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange in an appropriately stressed environment (including cyber), are addressed in the NR KPP. The NR KPP always contains measures of performance (MOP) and occasionally uses measures of effectiveness; however, this guide will use the term "measure." The NR KPP consists of testable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given IT via criteria associated with three attributes: support to military operations, entered and be managed on the network, and exchange information. Early coordination between the PM/Sponsor, Joint Staff, and JITC during NR KPP development is essential to ensure the architecture viewpoints identify the information needed to support joint interoperability TE&C. Issues with NR KPP requirements will be raised with the Joint Staff for resolution as soon as possible.


NR KPP
• Support to Military Operations
• Entered and Be Managed on the Network
• Exchange Information

NR KPP focuses on three attributes that include program specific, validated, verifiable performance measures, conditions, and criteria.

LEGEND:

NR KPP	Net-Ready Key Performance Parameter

Figure 3-2. NR KPP Focus

(1) NR KPP Attribute 1: "Support to Military Operations." This attribute involves measures used to evaluate interoperability for military operations (e.g., mission and mission threads) as well as operational tasks an IT supports. The evaluation considers whether the right information is received, when needed, in a format that can be used to support the task. Normally, the test organization responsible for the OT&E of the IT will provide test data for this attribute.

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

(3) NR KPP Attribute 3: "Exchange Information." This attribute specifies the information elements produced and consumed by each mission and Net-Ready operational task identified above. It identifies information elements the information system (IS) produces, sends, or makes available to external or joint interfaces and information elements the IS receives from external or joint interfaces (since Net-Ready content focuses on interactions with external systems, e.g., potential interactions with allied/partner nations and other U.S. Government systems). For each information element, measures are used to assess the information element's production or consumption effectiveness.

c. Prepare Requirements for Joint Interoperability Certification. The PM/Sponsor has the responsibility for developing the requisite interoperability requirements documents and associated architecture data. Early coordination between the PM/Sponsor and JITC during T&E planning is essential to identify the needed test data, data collection methods, and data collection opportunities. Test planners should consider leveraging standardized architecture viewpoints to facilitate automation in T&E and certification (see Appendix D) for improved cost, schedule, and performance. The PM/Sponsor prepares the appropriate requirements documentation and obtains a Joint Staff Net-Ready Certification. The following policy and guidance, as well as appropriate DoD Component policy, govern preparation of joint interoperability requirements (see Appendix A for additional references).

(1) For programs required to provide JCIDS documentation, the Chairman of the Joint Chiefs of Staff (CJCS) Instruction (CJCSI) 5123.01 directs JCIDS documentation to be prepared and submitted in accordance with the JCIDS Manual.

(2) In addition, the JCIDS Manual provides guidance (content) for developing the Net-Ready performance attribute and certifying the Net-Ready content for all acquisition pathways that require JIC in accordance with DoDI 8330.01.

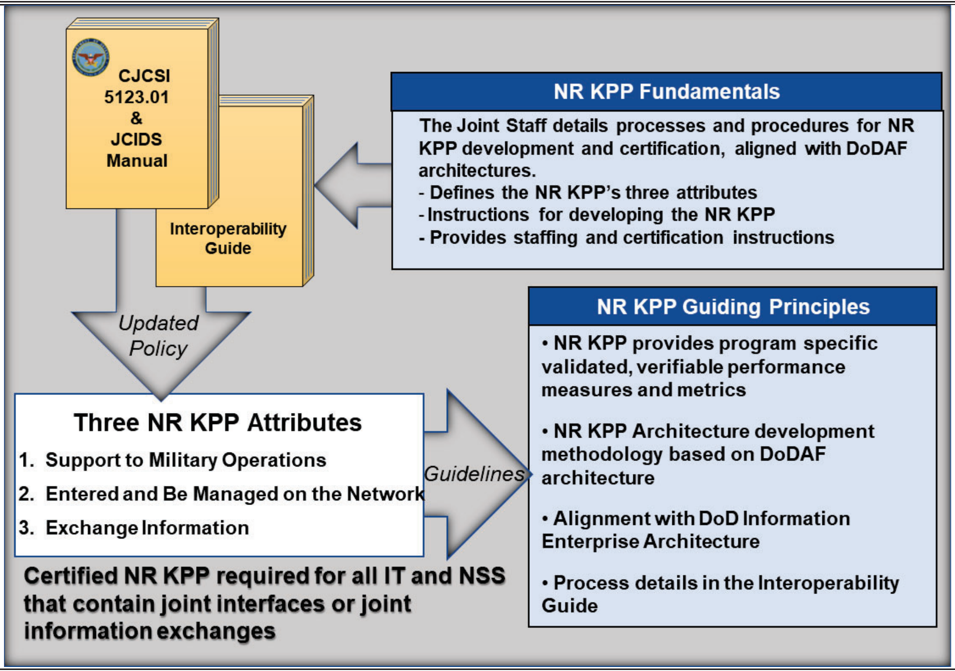
(3) The DoDI 5000.02 and the acquisition pathway instructions provide policy on documenting interoperability requirements. For example, DoDI 5000.75 addresses the products that contain the interoperability requirements for the defense business systems (DBS) acquisition pathway as part of the capability implementation plan (CIP). In addition, the functional acquisition instructions provide policy applicable to planning and execution. Note: Some acquisition pathways are not required to provide JCIDS documentation.

(4) DoDI 8330.01:

(a) Provides policy on the ISP process. Appendix E of this guide provides additional information on the ISP process.

(b) Identifies interoperability certification requirements for the Adaptive Acquisition Framework (AAF) pathways that are not required to produce an ISP. Appendix F of this guide provides additional information on AAF requirements process.

(5) Interface control agreements (ICAs) provide information that testers use to understand the interface (e.g., the concept of operations for the interface, the message structure and protocols which govern the interchange of data, and the communication paths along which the data is expected to flow).



NR KPP Fundamentals

The Joint Staff details processes and procedures for NR KPP development and certification, aligned with DoDAF architectures.
- Defines the NR KPP's three attributes
- Instructions for developing the NR KPP
- Provides staffing and certification instructions

Three NR KPP Attributes

1. Support to Military Operations
2. Entered and Be Managed on the Network
3. Exchange Information

Certified NR KPP required for all IT and NSS that contain joint interfaces or joint information exchanges

NR KPP Guiding Principles

- NR KPP provides program specific validated, verifiable performance measures and metrics
- NR KPP Architecture development methodology based on DoDAF architecture
- Alignment with DoD Information Enterprise Architecture
- Process details in the Interoperability Guide

LEGEND:

&	and	JCIDS	Joint Capabilities Integration Development System
CJCSI	Chairman of the Joint Chiefs of Staff Instruction	KPP	Key Performance Parameter
DoD	Department of Defense	NR	Net-Ready
DoDAF	Department of Defense Architecture Framework	NR KPP	Net-Ready Key Performance Parameter
IT	Information Technology	NSS	National Security Systems

Figure 3-3. Policies Governing Requirements Preparation

(6) The DoD CIO website: https://dodcio.defense.gov/Library/ contains a detailed description of the current version of DoDAF, and its application in developing capability solution architectures.

(7) DoDI 8310.01, "Information Technology Standards in the DoD," establishes policy for standards compliance and conformance. Program requirements documents will identify standards and technical specifications prescribed for the capability in accordance with DoDI 8310.01, or other applicable governance.

d. Coordinate with Executive Agent. When applicable, the PM/Sponsor will coordinate with Executive Agents (EA) for functional areas to identify funding and requirements. Examples of EAs include:

(1) National Geospatial-Intelligence Agency (NGA) EA.

(2) National Security Agency (NSA) EA.

(3) Common Data Link EA.

e. Coordinate JITC Support. The PM/Sponsor must work through their respective ISG member to establish contact with JITC early (e.g., during initial development phases or prior to development/contracts for Agile/development, security, and operations (DevSecOps) programs) and begin coordination for joint interoperability testing, test automation, evaluation, and certification. In addition, the JITC public website: http://jitc.fhu.disa.mil/, provides forms and contact information. The PM/Sponsor is responsible for arranging funding for planning, testing, analysis, and reporting associated with interoperability certification. The PM/Sponsor and JITC will document the responsibility details of both parties in a support agreement (Fiscal Service Form 7600A or plan of action and milestones (POA&M)) that provides the technical information for the support. The agreement must be in place and funding received by JITC prior to the start of any JITC support (ideally 120 days before).

f. Gather Required Documentation. The PM/Sponsor must provide JITC the following information prior to T&E activity that will support JIC (typically within 120 days or as coordinated between the PM/Sponsor and JITC):

(1) Approved requirements documents (or requirements for JIC) as described in paragraph 3.c. above and in Section 10 of the IPG. Information must include:

(a) A Joint Staff certified NR KPP.

(b) Appropriate supporting architecture viewpoints, as indicated in the Interoperability Guide (JCIDS Manual: Annex A, Appendix G, to Enclosure B) and the information provided in the architecture viewpoints required for JIC, as described in Section 11 of this document and the JITC Test and Evaluation Guide, "Architectures for Joint Interoperability Test, Evaluation and Certification," which can be found on JITC's ISG Resource website: https://jitc.fhu.disa.mil/projects/isgsite.

(2) Interface Documentation.

(a) ICAs, if available, for each external interface of the IT to be certified.

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

(3) Standards Conformance/Compliance Documentation. JITC requires documentation for IT employing technology governed by policy mandating specific standards conformance requirements. In accordance with DoDI 8310.01, the interoperability certification authority assesses standards conformance as part of the interoperability certification process when applicable (e.g., standards critical for joint information exchanges). The following are part of the standards conformance/compliance documentation in accordance with DoDI 8310.01:

(a) Available standards conformance test plans, test reports, assessments, or certifications to inform interoperability TE&C planning activities.

(b) Standards information provided in architecture viewpoints required for a standards conformance/compliance documentation package in Section 11 of the IPG.

(4) The PM/Sponsor must ensure an operationally representative test environment that includes the system configured in accordance with the system's security authorization documentation package submitted to the Authorizing Official in support of the system's authorization to operate (ATO), per the DoDI 8510.01, "Risk Management Framework for DoD Systems."

(5) Version Identification Information. The PM/Sponsor will provide JITC version identification information for the IT or IT components (both services and data) to be certified, and for applicable interfacing capabilities and enterprise components.

(6) Increment Requirements. JITC evaluates all joint interoperability requirements for a JIC as defined in the requirements documentation for a given increment (e.g., releases, versions, blocks, and phases). The PM/Sponsor will coordinate with JITC to identify which increments to assess for a JIC. If the Joint Staff certified NR KPP does not delineate requirements for an increment, then JITC will evaluate all joint requirements for the JIC. The Joint Staff may require recertification of the NR KPP if the requirements for an increment are modified (e.g., implementation or criticality of the requirements).

(7) Approved PM/Sponsor and responsible test organization test plans and planning documents as described in paragraph 3.g.

(8) A current Program Security Classification Guide.

g. Develop Test Strategy, Plans, and Schedule. The PM/Sponsor will coordinate with JITC to integrate interoperability test requirements and resources into the IT's T&E documents (e.g., test and evaluation master plan (TEMP), applicable acquisition pathway's T&E strategy, System Engineering Plans, Acquisition Program Baselines, and test plans). JITC needs to be involved early in the program's acquisition TEMP review process to ensure joint requirements are testable and measurable during service-level DT&E and OT&E events. JITC may produce an interoperability assessment strategy as part of a joint interoperability evaluation plan (JIEP). The plan(s) used will depend on several factors: the complexity of the IT (e.g., single item, number of external interfaces); development approach (e.g., commercial-off-the-shelf, evolutionary with numerous increments); and the anticipated number of JITC and non-JITC conducted test events. JITC and the PM/Sponsor may need to update the POA&M after review of the test strategy, plans, and schedule. 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 IT must meet for each increment to be certified.

(1) Test and Evaluation Strategy.

(a) The PM/Sponsor is responsible for the acquisition artifacts (e.g., requirements, T&E strategy, etc.) and provisioning the testing infrastructure, and tools during the pre-T&E (planning) phase.

(b) The PM/Sponsor will coordinate with JITC to develop an integrated T&E strategy (e.g., developmental testing and operational testing) and will ensure the T&E strategy addresses all the joint interoperability requirements in the certified NR KPP.

(c) The PMs/Sponsors must tailor T&E strategies for programs that use AAF pathways (i.e., DBS acquisition (DoDI 5000.75), middle tier acquisition (MTA) (DoDI 5000.80), or software acquisition (DoDI 5000.87), in coordination with JITC to determine the frequency and scope of interoperability test, evaluation, and certification. For IT with joint interoperability requirements, the PM/Sponsor should coordinate with JITC to ensure the T&E capability or activity is adequate to evaluate the joint interoperability requirements. JITC must concur with the PM/Sponsor's proposed interoperability T&E strategy to ensure data is valid for a JIC determination.

(d) JITC can leverage test data from multiple sources to support a JIC determination (e.g., data from DT&E, OT&E, standards conformance). The PM/Sponsor needs to coordinate with JITC to determine usability of data (e.g., available and credible) when developing the T&E approach as appropriate to reflect in TEMPs, test plans, or similar documents. The following are considerations to accept or accredit usability of data sources (i.e., venue):

1. A JIC determination is based on results from events that are as operationally representative as feasible. This normally entails collection of data obtained from operational testing, operationally realistic exercise events, or from actual operational use.

2. Developmental test data may be used to augment operational test data for TE&C if collected using an operationally relevant configuration and environment.

3. The PMs/Sponsors that use agile development processes, such as software acquisition pathways using DevSecOps, should coordinate with JITC in the planning phase to discuss the specific T&E requirements for DevSecOps and the use of automated test scripts/cases, to collect data, analyze test results (including immediate access to failures), assess acceptance criteria, record failures, etc.

(e) The PM/Sponsor and responsible test organization will coordinate test plans with JITC prior to any test event supporting interoperability evaluation.

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

(g) Testers must use measures from the NR KPP and established Joint Mission Threads (JMTs) during test planning. Mission threads are critical to verify the operational effectiveness of information exchanges. If established JMTs are not available, then testers will derive appropriate mission operational tasks (activities) from the Joint Staff certified NR KPP and approved architecture viewpoints (i.e., as in operational viewpoints (OV)-5b and OV-6c).

(h) Standards conformance serves as a foundation for interoperability (for more information on standards conformance, see DoDI 8310.01). The PM/Sponsor must coordinate with JITC during the planning of standards conformance testing to ensure interoperability evaluation needs are adequately addressed (e.g., standards that enable required joint information exchanges). JITC can leverage planned standards conformance testing during joint interoperability T&E planning.

(i) PM/Sponsor and responsible test organization should negotiate coordination and scheduling considerations with proponents of interfacing IT (e.g., the certification process requires interfacing ITs be available during interoperability testing).

(j) Programs following the software acquisition pathway typically need continuous engagement with JITC to provide decision makers with periodic assessments/certifications consistent with dynamic changes characteristic with the software pathway. JITC employs three primary approaches to support T&E of a DevSecOps, or aspiring DevSecOps/agile-programs: Embedded Testing; Periodic Audit and Evaluation (Test Event); and Hybrid of Embedded and Periodic Audit/Evaluation. The PMs should coordinate with their JITC Point of Contact (POC) to determine the best approach.

(2) JIEP.

(a) A JIEP is an initial T&E planning document in the joint interoperability test, evaluation, and certification process. The JIEP establishes the overall strategy or plan of how an IT (system) or combination of IT (i.e., system of systems) is evaluated and serves as JITC's version of a TEMP. The JIEP contains the overarching approach to evaluate IT compliance to the NR KPP. The JIEP contains the test strategy, joint interoperability requirements, planned test events, requirements testers expect to address in each test event, timeline sequence, and estimated resources. It includes a system description and operational use of the IT under test, derived from the applicable JCIDS and/or requirements documentation.

(b) A JIEP is required when multiple test events are necessary to complete interoperability evaluation. A JIEP is optional if only a single event is required (i.e., or as coordinated between the PM/Sponsor and JITC POC). The JIEP will be updated if needed to reflect changes to interoperability requirements (e.g., changes to the certified NR KPP).

(3) Interoperability Test Plan (ITP). JITC uses ITPs as the test planning documents for JITC-conducted test events. JITC develops an ITP when no previous or planned testing will produce the data needed to evaluate interoperability, or where programmatic or other constraints preclude inclusion of suitable data collection in planned testing. An ITP describes the IT to be tested, test objectives, and detailed test procedures for an interoperability test. ITPs are written for individual test or data collection events. These plans detail the testing, data collection and analysis procedures that apply to that event. JITC can also use data obtained from other test venues that use different types of test plans (e.g., OT&E, Joint Interoperability Tests, Combined Interoperability Tests, and standards conformance).

(4) Test Support Package (TSP). JITC uses TSPs to augment the responsible test organization's test plan. The purpose of the TSP is to ensure required data are collected, needed to support JITC joint interoperability evaluation, during the test event. The TSP also explains how JITC will evaluate joint interoperability requirements (e.g., the information exchanges, networks, and tasks).

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

(a) Status of IT interoperability and standards conformance issues.

(b) Confirmation that all required developmental testing relating to IT interoperability has been successfully completed and passed.

(c) Details of any interoperability issues that must be resolved before the start of OT&E.

h. Determine Required Resources for Test and Certification. The PM/Sponsor should develop a cost and resource estimate with JITC that ensures cost covers resources needed to evaluate interoperability in an operationally relevant environment, to include appropriate cybersecurity considerations, consistent with coordinated T&E strategy and plans. The resources should be sufficient to collect the data necessary to support the interoperability evaluation, to include the test events/environments planned to produce that data. To be cost effective, the PM/Sponsor should integrate the evaluation of an IT's interoperability into the overall test, evaluation, and development processes as early in the developmental life-cycle as possible. This is especially important for programs under the software acquisition pathway where:

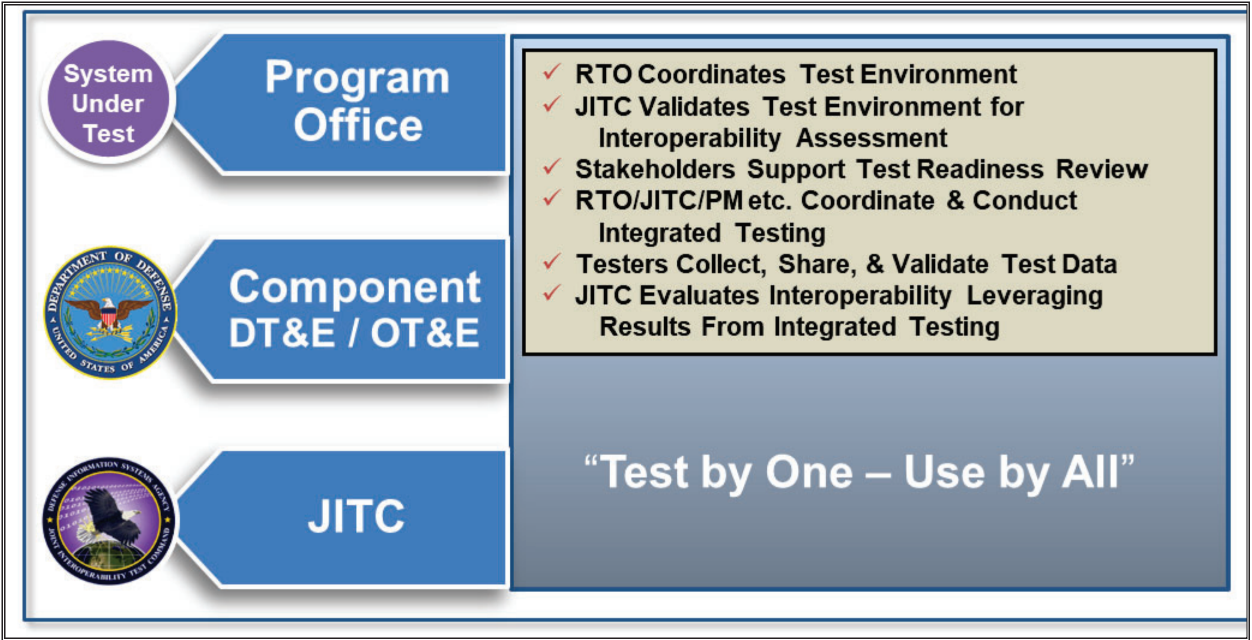
(1) The potential to deliver capabilities at a faster pace than traditional development methods is greater and may require JITC to dedicate more resources to program test support.

(2) New program test requirements can emerge within each development cycle, so it is equally important that JITC actively participate in each development cycle to capture new or changing test requirements, influence their testability, and ensure allocation of appropriate test resources.

i. Identify Equipment Configuration/Application of Required Cybersecurity Controls. Interoperability evaluation should be based on test of a production representative IT in an operationally representative environment to the extent feasible. Testing includes the use of test scenarios with a typical message mix, loading that reflects normal and wartime modes that include benign and hostile environments. IT test configurations will represent realistic cybersecurity aspects of the operational environment to include application of the cybersecurity controls. If testing does not use the proper cybersecurity configuration, then the test results may be rejected, requiring additional testing. It is important in the planning stages to recognize the need for a suitable interoperability environment (for the SUT and interfacing IT), including cybersecurity considerations.

4. Test and Evaluation Procedures (execution)

During testing, a variety of structured events surround successful interoperability T&E. Figure 4-1 summarizes the range of activities that typically occur during the T&E phase.



- ✓ RTO Coordinates Test Environment
- ✓ JITC Validates Test Environment for Interoperability Assessment
- ✓ Stakeholders Support Test Readiness Review
- ✓ RTO/JITC/PM etc. Coordinate & Conduct Integrated Testing
- ✓ Testers Collect, Share, & Validate Test Data
- ✓ JITC Evaluates Interoperability Leveraging Results From Integrated Testing

"Test by One – Use by All"

LEGEND:

&	and	OT&E	Operational Test and Evaluation
DT&E	Developmental Test and Evaluation	PM	Program Manager
etc	et cetera	RTO	Responsible Test Organization
JITC	Joint Interoperability Test Command		

Figure 4-1. T&E Activities

a. Initial Conditions/Assumptions. The following activities have been accomplished in the Pre-T&E phase (planning):

(1) The PM provisioned an operationally representative test environment.

(2) The PM ensured the cybersecurity configuration of the SUT is defined.

(3) The PM identified the responsible test organization.

(4) JITC completed an ITP or TSP.

(5) The PM ensured delivery of previous T&E results to JITC (e.g., standards conformance or other testing, as part of an integrated T&E strategy).

(6) JICs inform the Milestone Decision Authority (MDA) or acquisition decision authority (as appropriate) for:

(a) Major capability acquisition (MCA) pathway programs for Milestone C decisions (see DoDI 5000.85).

(b) DBS acquisition pathway programs for a fielding decision.

(c) Software acquisition pathway programs supporting delivery of software capability releases.

(d) Rapid fielding MTA pathway programs transitioning to other AAF pathways.

b. Test Conduct.

(1) The PM/Sponsor is responsible for obtaining a JIC for the SUT and therefore responsible for coordinating with the appropriate sources (e.g., test organizations) to provide the data needed for interoperability evaluation.

(2) The tester should apply these basic tenets of testing to ensure data, critical for analysis, is valid:

(a) The requirements, used to develop test plans, are approved and certified.

(b) The SUT is properly configured including cybersecurity controls.

(c) The SUT is appropriately configured with the required software version and operating system.

(d) The version and configurations of interfacing IT are documented. This information is essential for meaningful test & evaluation.

(3) Integrated T&E ("test by one, use by all") is encouraged to leverage test events to make the most effective and efficient use of resources. Integrated testing typically consists of multiple test events, conducted by one or more organizations, to address and test to requirements. Coordinated test plans facilitate data sharing from integrated testing to support independent evaluators, each performing the appropriate analysis to address their specific test issues and measures. For example, data collected during developmental testing, deployment (e.g., DevSecOps), and operational testing can be compiled into a shared database for JITC to support JIC. Integrated testing is achieved through collaboration during planning, testing, and evaluation. See DoDI 5000.89 for more information on integrated testing.

c. Joint Interoperability Test, Evaluation, and Certification Process.

(1) Interoperability test and evaluation are dependent on the test environment (e.g., test infrastructure, test interfaces, network loading, and test participants). JICs are based on T&E of production representative IT (hardware/software) employed in an operationally representative environment, to the extent feasible, including use of authorized cybersecurity configurations.

(2) JITC will leverage multiple T&E sources to evaluate the end-to-end interoperability within as operationally representative environment as practicable. Resources for T&E information include:

(a) Joint Staff certified NR KPP and information prescribed in Section 11 of the IPG.

(b) Mission-related information.

(c) Data from different events. Those events can be DT&E, OT&E, acceptance testing, exercise venues, or other demonstrations, consistent with any approved TEMP, or other interoperability data collection requirements. The operational impacts of all unresolved interoperability deficiencies must be determined by the appropriate users or user representatives and be reported to JITC to support a joint interoperability evaluation.

(d) Interoperability T&E criteria, measures, and requirements established by intelligence functional managers (e.g., NGA and NSA).

(3) JITC will review results of standards conformance testing or certifications. Standards conformance testing is usually conducted during DT&E. JITC can use results obtained from standards conformance testing as part of the data for interoperability evaluation, wherever applicable.

(4) JITC will record requirements (NR KPP) issues discovered during T&E, resolve issues in coordination with Joint Staff and PM/Sponsor, and document the resolution.

(5) JITC evaluates deviations from test plans (e.g., changes in test environment) and test limitations. Examples of deviations include any departure from planned execution of testing a requirement to include substitution of a required interface version because of unavailability, operational network access and loading procedures, or satellite transponders. An example of a test limitation is the use of test equipment with a precision capability less than what is required to measure the performance of a measure. This is a test limitation because it can constrain or limit what can be concluded from the test. The overall impact to interoperability (from test deviations and limitations) is assessed during the evaluation process. JITC must consider the impact of deviations during the interoperability evaluation for a JIC, even if deviations are beyond the control of the PMs/Sponsors.

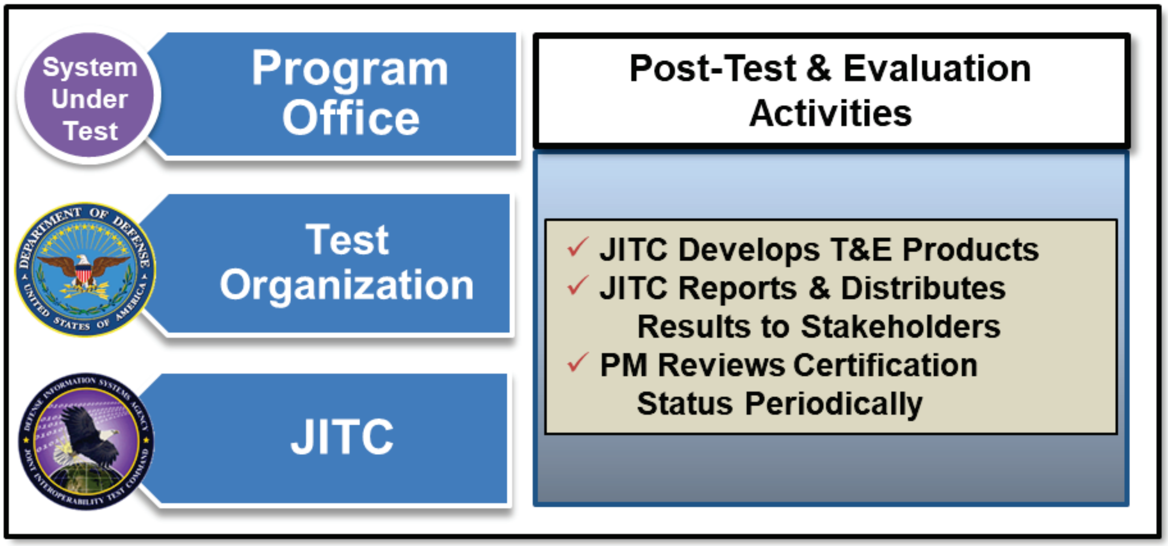
(6) JITC will notify the PM/Sponsor if, during the TE&C process, JITC determines there is insufficient data to support the joint interoperability decision, and when applicable, coordinate an appropriate course of action (e.g., to plan and conduct an additional test). PM/Sponsor will coordinate with JITC (e.g., to plan and conduct an additional test) if insufficient data to support the joint interoperability decision. JITC may issue a Joint Interoperability Assessment to document interoperability status, in lieu of a JIC, when there is not sufficient information (e.g., test data, requirements, or relevant test environment) to support a JIC.

(7) JITC will document in the JIC or Assessment any cybersecurity and survivability issues discovered during an interoperability evaluation with significant negative impacts on joint interoperability. Cybersecurity and survivability are not part of the NR KPP attributes.

(8) The JIC does not substitute for any other certifications that may be required (e.g., spectrum certifications, network manager approval to connect (ATC), and/or other validations/approvals).

5. Post-Test and Evaluation Procedures (reporting)

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 activities that routinely occur during the post-T&E phase.



- ✓ JITC Develops T&E Products
- ✓ JITC Reports & Distributes Results to Stakeholders
- ✓ PM Reviews Certification Status Periodically

LEGEND:

&	and	PM	Program Manager
JITC	Joint Interoperability Test Command	T&E	Test and Evaluation

Figure 5-1. Post-T&E Activities

a. Overview.

(1) The PM/Sponsor and responsible test organization must provide JITC all relevant reports, system/test configuration information (including for interfacing IT), test data, trouble reports, analysis of any discrepancies, etc., in a timely fashion if results are to be considered in the interoperability evaluation. All parties should keep in mind the JITC processing time required after receipt of test information – the sooner organizations provide the required information, the sooner they can receive their certification.

(2) JITC will:

(a) Provide the results of the joint interoperability evaluation to the PM/Sponsor (e.g., JIC and Assessments).

(b) Provide the results of the joint interoperability evaluation to the following stakeholders:

1. MDA or acquisition decision authority to support a fielding decision.

2. Appropriate connection approval office (CAO) for DoD network connection approval of the ATC or interim ATC.

3. ISG members.

(c) Deliver the results of the joint interoperability evaluation to the PM/Sponsor with a goal of within 60 calendar days once JITC is in receipt of all required test information and adjudication of deficiencies is complete.

(d) Record the JIC decision in the authoritative database (e.g., JITC System Tracking Program (STP)).

(3) JITC issues JICs for IT under the DBS, MCA, MTA, and software acquisition pathways based upon meeting the joint interoperability requirements set forth by the Joint Staff certified NR KPP and approved architecture viewpoints (see Section 11).

(4) In general, JICs expire in 4 years or when changes to the IT functionality, requirements, employment, or environment impact joint interoperability. See T&E Products, paragraph 5.b., and Recertifications, paragraph 5.c, for variations on JIC expirations.

b. Test and Evaluation Products. JITC has a family of T&E products that document various T&E outcomes. The paragraphs below describe JITC family of products associated with possible outcomes. See Figure 5-2.

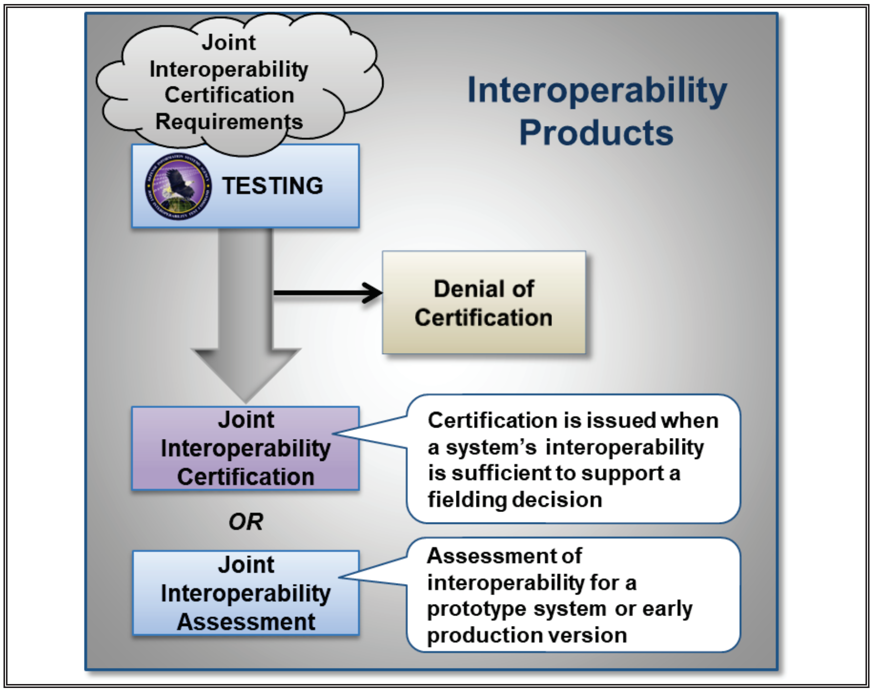

Joint Interoperability Certification Requirements
Interoperability Products
TESTING
Denial of Certification
Joint Interoperability Certification
Certification is issued when a system's interoperability is sufficient to support a fielding decision
OR
Joint Interoperability Assessment
Assessment of interoperability for a prototype system or early production version

Figure 5-2. T&E Products

(1) Joint Interoperability Certifications (JIC).

(a) Joint Interoperability Certification. JITC issues a JIC when an IT is evaluated against all Joint Staff certified NR KPP requirements and the IT's interoperability status is sufficient to support a fielding decision.

1. Traditional. For programs fielding complete capabilities (e.g., using traditional waterfall approach), the JIC addresses all the Joint Staff certified NR KPP requirements. JICs issued for traditional programs expire 4 years from the issue date. Changes meeting recertification criteria are addressed in accordance with Recertification (paragraph 5.c.).

2. Incremental. For programs with an approved plan to field capability incrementally (e.g., software, MTA, and DBS acquisition pathways using agile/DevSecOps development), the scope of a JIC can be tailored to align with the increment of capability fielded (i.e., all the joint requirements implemented in the increment).

a. The certification issued for the initial increment of capability is the baseline JIC. The initial increment of certification (baseline) expires 4 years from the issue date.

b. Subsequent JICs may address the additional (certified) requirements implemented in a specific increment or address all requirements implemented to date (i.e., roll-up. Subsequent certifications that cover increments of capabilities inherit the expiration date of the baseline certification. See an example in paragraph 5.b.(1)(a)2.d. below for more detail.

c. A roll-up JIC, addressing all requirements implemented to date, becomes the new baseline. The expiration of the baseline is reset if the program does a roll-up JIC.

d. For example, a program following the software acquisition pathway coordinates a capability needs statement (CNS) and roadmap that specifies fielding approved capability in five increments (e.g., five minimum viable capability releases (MVCRs), with separate versions 1.1 to 1.5). Joint interoperability testing is planned to evaluate the initial MVCR (according to the certified joint interoperability requirements implemented), with a joint IOP certification or assessment issued as appropriate. So, if a JIC was issued, it will be the baseline JIC. For each subsequent MVCR, joint interoperability testing is planned based on the additional or remaining certified joint interoperability requirements implemented in that release. JITC will also determine if changes in the new release require reevaluation of any past joint interoperability requirements that were previously addressed in a JIC. This process will continue until all the certified joint interoperability requirements have been addressed through testing and certification. The last release (MVCR V 1.5) addresses all certified requirements implemented and becomes the new JIC baseline with a new 4-year expiration date.

(b) Joint Interoperability Certification with Conditions. JITC may issue a JIC “with conditions” when a subset of the requirements is met. A JIC with conditions enables fielding useful capabilities, despite not testing or not meeting all joint interoperability requirements when there are no expected critical operational impacts or adverse effects on the joint interoperability environment. The Conditions to the certification are based on assessment of operational impact and describe the interoperability risks assessed to requirements not tested or not met. Conditions to certifications inform decision makers of risks to interoperability when making acquisition, fielding, and employment decisions. To clear conditions, the PM/Sponsor coordinates with JITC to provide information, typically obtained from additional testing or field operations, needed for evaluation to determine if associated joint requirements are met with no operational impacts. JIC with conditions follow the respective expirations rules for Traditional or Incremental programs, as appropriate.

(c) Joint Interoperability Certification Extension. JITC grants a certification extension to extend coverage (scope) of an existing certification for modifications not affecting joint interoperability made before the certification expires. The extension has the same expiration date as the baseline certification. For example, a certification issued for version 1.0 (with expiration date 4 years later) could receive a certification extension covering the follow-on version 1.1, while retaining the same 4-year expiration date of the baseline certification. The PM/Sponsor will contact their JITC action officer (AO) to coordinate information and resources required for a JIC extension. At a minimum, certification extension requests must include:

1. A written statement by the PM/Sponsor that the modification does not affect interoperability.

2. Sufficient information for JITC to independently determine the impact of any changes.

(d) Denial of Certification.

1. 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 Joint Interoperability Certification. This provides CIOs, Joint Staff, MDAs (or acquisition decision authorities (as appropriate)), and PMs notification of problems that warrant immediate attention.

2. Revocation and Reissuance of Joint Interoperability Certification. JICs may be rescinded, revoked, or reissued by JITC. This would occur if a deficiency was discovered creating a critical operational impact (e.g., a significant difference between a fielded configuration and the tested configuration, a change in data exchange partners, a change in system configuration, or an interoperability deficiency discovered post-test). All organizations that received the original certification notice will be notified of changes in interoperability certification status.

(2) Joint Interoperability Assessment. A Joint Interoperability Assessment is issued to document an IT's joint interoperability strengths and weaknesses. Assessments are appropriate in cases where requirements documents have not been finalized, high-risk areas warranting early feedback, etc., but are not sufficient to support a fielding decision. Joint Interoperability Assessments can be conducted during DT&E or OT&E events, acceptance testing, interoperability exercises, or other test venues. The PM/Sponsor must coordinate with and fund JITC to establish the exact assessment needs and identify documentation requirements.

c. Recertification. Recertification is the process to evaluate an IT with the existing JIC when specified criteria are met and, when appropriate, issue a (new) JIC. Interoperability can degrade over time and must be carefully monitored throughout the IT's life-cycle. The criteria for recertification are based on changes to IT, requirements, or operating environment. For example, changes to standards, interfacing IT, or cumulative minor upgrades impact the ability of IT to interoperate. The Joint Staff Net-Ready Certification does not expire. However, the requirements may change over time and may require Joint Staff revalidation. The PM/Sponsor is responsible to coordinate with the Joint Staff, JITC, and affected DoD Component ISG members (i.e., for the affected joint interfacing/joint information exchanging IT), to assess changes for impact to joint interoperability (e.g., system, requirements, environment, etc.) and coordinate T&E support. The PM/Sponsor recertification request provides key information to procure JITC support.

(1) Recertification Criteria. Recertification is required when:

(a) Changes to certified system (IT) impact joint interoperability, such as materiel related changes (e.g., hardware or software modifications, including firmware) and interface changes. Refer to JIC Extension if changes were made, or are anticipated, to the system, that do not impact joint interoperability.

(b) Changes to IT requirements impacting interoperability (to include implemented standards) that occurred or are anticipated to occur (e.g., new increment to be fielded, hosting platform, or other materiel changes).

(c) Changes to the environment that impact joint interoperability occurred including changes to:

1. Systems (IT) interfacing to the certified system.

2. Materiel related (e.g., hardware or software modifications, including firmware) to the system that affect joint interoperability, or materiel changes to interfacing systems.

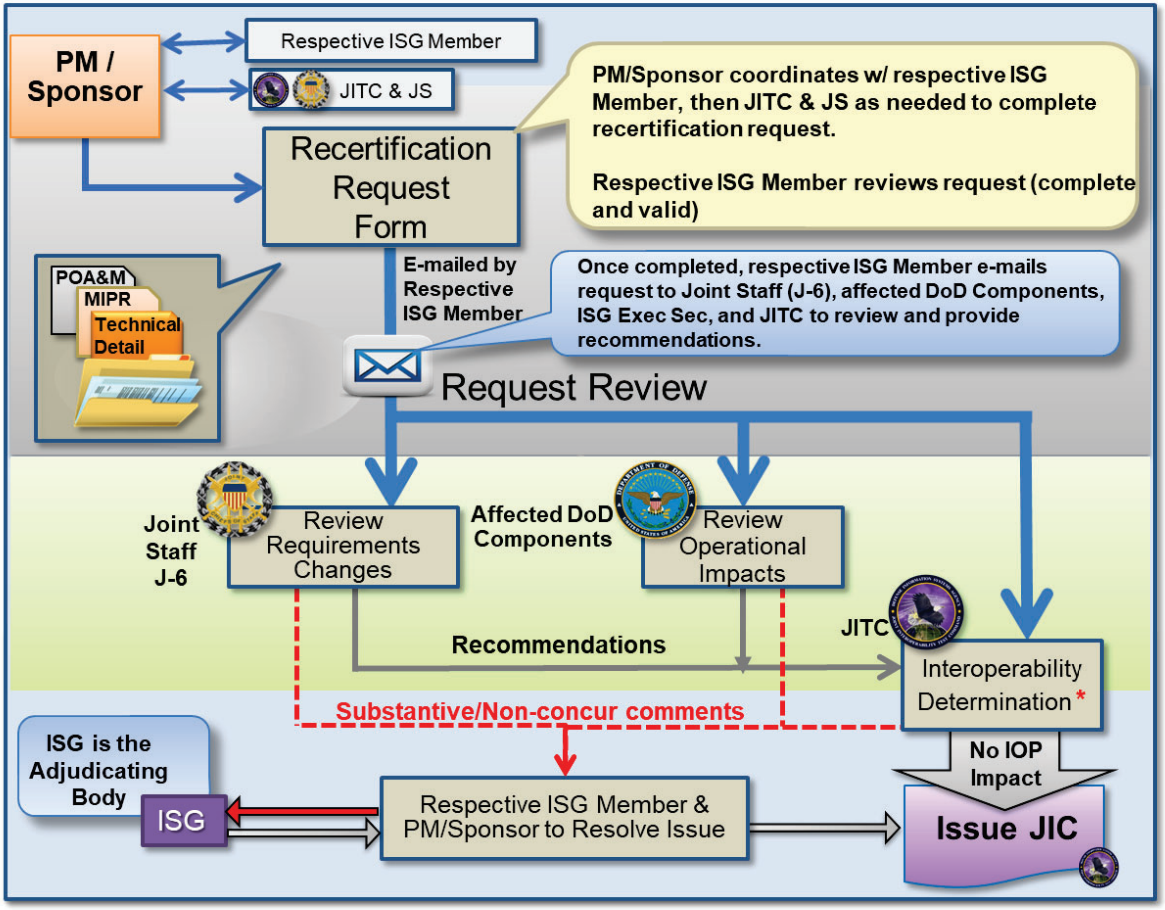
3. IT standards (i.e., impacting the environment), to include prescribed DoD Information Technology Standards Registry (DISR) standards or other IT standards with a DoD CIO approved compliance waiver (e.g., where a substantive revision constitutes a change in the interoperability environment which could result in a need for recertification) implemented by interfacing IT.

4. Non-materiel related items (i.e., Doctrine, Organization, Training, Leadership and education, Personnel, and Facilities-Policy (DOTLPF-P)).

(d) The JIC expires at the end of 4 years due to continuous evolution in technology and operating environments.

(e) The JIC is revoked (e.g., critical operational deficiencies (caused by interoperability issues) are reported (discovered) after fielding).

(2) Recertification Procedures. Figure 5-3 depicts the recertification request procedures presented in this section.


PM / Sponsor
Respective ISG Member
JITC & JS
Recertification Request Form
PM/Sponsor coordinates w/ respective ISG Member, then JITC & JS as needed to complete recertification request.
Respective ISG Member reviews request (complete and valid)
POA&M
MIPR
Technical Detail
E-mailed by Respective ISG Member
Once completed, respective ISG Member e-mails request to Joint Staff (J-6), affected DoD Components, ISG Exec Sec, and JITC to review and provide recommendations.
Request Review
Joint Staff J-6
Review Requirements Changes
Affected DoD Components
Review Operational Impacts
JITC
Recommendations
Interoperability Determination *
Substantive/Non-concur comments
ISG is the Adjudicating Body
ISG
Respective ISG Member & PM/Sponsor to Resolve Issue
No IOP Impact
Issue JIC

NOTE: * PM/Sponsor will coordinate with JITC for additional evaluation if changes are determined to impact joint IOP.

LEGEND:

&	and	JITC	Joint Interoperability Test Command
DoD	Department of Defense	JS	Joint Staff
E-mail	Electronic Mail	MIPR	Military Interdepartmental Purchase Request
Exec	Executive	PM	Program Manager
IOP	Interoperability	POA&M	Plan of Action and Milestones
ISG	Interoperability Steering Group	POC	Point of Contact
J-6	Joint Staff Directorate for Command, Control, Communications, & Computers/Cyber	Recert	Recertification
		Sec	Secretary
JIC	Joint Interoperability Certification	w/	With

Figure 5-3. Recertification Request Procedures Summary.

(a) The PM/Sponsor must perform the following activities when any Recertification Criteria (a), (b), or (c) (per IPG paragraph 5.c.(1) above) are met:

1. The PM/Sponsor coordinates with their respective ISG member to determine if any recertification criteria are met.

2. The respective ISG member will provide the PM/Sponsor with the recertification request form (the form can be found on the ISG Resource website:

https://jitc.fhu.disa.mil/projects/isgsite), which identifies required technical and funding information.

3. The PM/Sponsor coordinates with JITC if changes to the POA&M and Military Interdepartmental Purchase Request are required.

4. The PM/Sponsor coordinates with JITC and Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber (J-6) as needed to complete the recertification request.

5. The PM/Sponsor will complete, sign, and send the request form to the respective ISG member for review.

6. The respective ISG member will return the form to the PM/Sponsor if the request is not complete and valid. If the respective ISG member concurs, the respective ISG member will forward the recertification request form via e-mail 'To' Joint Staff J-6, affected DoD Component ISG members, ISG Executive Secretary, and JITC (disa.huachuca.jt.mbx.jitc-iop-re-certification-requests@mail.mil) to initiate coordination for interoperability evaluation. Copies are sent to the remaining ISG members for situational awareness (unless distribution is limited). ISG members that wish to be added to the review will coordinate with the respective ISG member.

7. Reviewers will take the following actions upon receipt of a valid recertification request (i.e., via the respective ISG member).

a. Joint Staff J-6 will review requirements information (i.e., if the Net-Ready Certification is still valid or if changes impact joint performance requirements and a new Net-Ready Certification is needed). If Joint Staff J-6 concurs (i.e., with requirements status or proposed actions), they will forward concurrence to JITC with courtesy copy (Cc) to the respective ISG member and PM/Sponsor. If Joint Staff J-6 non-concurs, they will return requests to the respective ISG member, with Cc to the PM/Sponsor and JITC. Objective: within 30 calendar days from receipt of recertification request form.

b. The respective ISG member will coordinate with the affected DoD Components to obtain the operational user inputs for the IT requesting recertification and document them in the request form.

c. The affected DoD Components will review the request and report on operational (i.e., observed) or potential interoperability impacts to their respective (fielded) capabilities. The affected DoD Components ISG members forward the response to the respective ISG member, with Cc to Joint Staff, PM/Sponsor, and JITC for consideration and evaluation. Objective: within 30 calendar days from receipt of the recertification request form. If other ISG members (Cc'd) have comments, they can send them to the respective ISG member to coordinate and adjudicate also within the same 30 calendar days as appropriate.

d. JITC reviews requests to assess impact of changes and identify data requirements to support a joint interoperability determination (recertification). Objective: within 30 calendar days from concurrence by Joint Staff J-6 and the respective ISG member.

e. If all reviewers of the request concur that changes do not impact joint interoperability, then a new certification is not required.

8. PM/Sponsor coordinates with Joint Staff about Net-Ready Certification when requirements changes impact joint interoperability.

9. The PM/Sponsor provides data from past events (tests, exercises, or operational venues), and /or coordinates for JITC T&E support to obtain additional data essential to evaluate interoperability of the IT with applied changes for a new certification. If all changes cannot be tested, such as an update to an interfacing IT, it may be appropriate to obtain a JIC with conditions.

10. JITC evaluates the relevant data with respect to the certified joint interoperability requirements, issues a JIC or JIC with conditions as appropriate, and records the certification in STP.

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

12. The ISG will resolve any disagreements between the PM/Sponsor and JITC whether additional testing is required. The ISG decision will be provided in writing to both parties.

(b) If the JIC is scheduled to expire, and the PM/Sponsor desires recertification without additional testing, the following procedures apply:

1. The PM/Sponsor should contact JITC through the respective ISG member early enough to allow sufficient time for the recertification process. It is recommended this process be started as early as 12 months, but no later than 6 months, prior to JIC expiration.

2. The respective ISG member will provide the PM/Sponsor with the recertification request form (the form can be found on the ISG Resource website: https://jitc.fhu.disa.mil/projects/isgsite), which identifies required technical and funding information.

3. The PM's/Sponsor's recertification request will provide written verification that the interoperability environment (including the IT and interfacing IT) and joint interoperability requirements (in certified NR KPP and approved architectures) have been reviewed and have not changed such that they affect interoperability. The PM/Sponsor will summarize operational history of the IT (e.g., deployment and exercises), identifying any interoperability related operational impacts, and status of conditions documented in current JIC (if applicable). If changes have occurred, the PM/Sponsor will list deltas from the prior certified version and provide rationale why changes do not impact interoperability.

4. The PM/Sponsor will complete, sign, and send the recertification request form to the respective ISG member to review.

5. The respective ISG member will return the form to the PM/Sponsor if the request is not complete and valid. If the respective ISG member concurs, then the respective ISG member will forward the recertification request form via e-mail 'To' Joint Staff J-6, affected DoD Component ISG members, ISG Executive Secretary, and JITC (disa.huachuca.jt.mbx.jitc-iop-re-certification-requests@mail.mil) to initiate coordination for interoperability evaluation. Copies are sent to the remaining ISG members for situational awareness (unless distribution is limited). ISG members that wish to be added to the review will coordinate with the respective ISG member.

6. Reviewers will take the following actions upon receipt of a valid recertification request (i.e., via the respective ISG member).

a. Joint Staff J-6 will review requirements information (i.e., if the Net-Ready Certification is still valid or if changes impact joint performance requirements and a new Net-Ready Certification is needed). If Joint Staff J-6 concurs (i.e., with requirements status or proposed actions), they forward concurrence to JITC with courtesy copy (Cc) to the respective ISG member and PM/Sponsor. If they non-concur, they return requests to the respective ISG member, with Cc to PM/Sponsor and JITC. Objective: within 30 calendar days from receipt of recertification request form.

b. The respective ISG member will coordinate with the affected DoD Components to obtain the operational user inputs for the IT requesting recertification and document them in the request form.

c. The affected DoD Components will review the request and report on operational (i.e., observed) or potential interoperability impacts to their respective (fielded) capabilities. The affected DoD Components ISG members forward the response to the respective ISG member, with Cc to Joint Staff, PM/Sponsor and JITC for consideration and evaluation. Objective: within 30 calendar days from receipt of recertification request form. If other ISG members (Cc'd) have comments, they can send them to the respective ISG member to coordinate and adjudicate also within the same 30 calendar days as appropriate.

d. JITC will review all requests and perform an analysis to provide an interoperability determination to the PM/Sponsor and respective ISG member. Objective: within 30 calendar days from receipt of concurrence from Joint Staff J-6 and the respective ISG member.

- JITC may issue a new certification without additional interoperability testing if: 1) the joint interoperability requirements, system configuration, and operational environment of the IT are current and have not changed in a manner that impacts joint interoperability, 2) no new operational impacts have been identified, and 3) funding has been received. Objective: within 30 calendar days of making the determination.

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

7. In the case of disagreement between JITC and the PM/Sponsor regarding the determination for the recertification , the PM/Sponsor will have the opportunity to provide a rebuttal to JITC.

8. The ISG will resolve any disagreements between the PM/Sponsor and JITC whether additional testing is required. The ISG decision will be provided in writing to both parties.

(c) If certification is revoked, the PM/Sponsor must perform the following procedures:

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

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

(3) Recertification Coordination. JITC supports recertification requests as a fee for service. The PM/Sponsor is responsible to coordinate with JITC to ensure funding will not impact the published recertification timelines. The JITC AO will coordinate with the PM/Sponsor to return unused funding.

6. Interim Certificate to Operate Procedures

An ICTO permits an IT to be fielded for operational use without a JIC. An ICTO is the authority to operate an IT for a limited time (up to one year) to allow operational use while pursuing JIC per DoDI 8330.01.

a. ICTO Process:

(1) Representatives from the DoD CIO, the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the CJCS serve as the Tri-Chairs of the ISG. The ISG Tri-Chairs adjudicate and approve ICTOs for IT with joint interoperability requirements. ICTOs must only be granted when the IT is progressing toward a JIC and there is a documented need to operate the IT until a JIC can be issued.

(2) The ISG Tri-Chairs will 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 prior to JIC.

(b) JITC or other DoD Component test organizations are unable to assess all requirements for the IT undergoing interoperability evaluation.

(c) In either case, the PM/Sponsor of the IT must engage with JITC and pursue JIC.

(3) Factors impacting ICTO decisions include:

(a) Urgent operational need.

(b) Existing test results/artifacts.

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

(d) Plan of action to complete JIC.

(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) The ISG Tri-Chairs will confer with JITC and ISG members to determine if an ICTO is appropriate for IT that fails to meet identified interoperability requirements during joint interoperability testing and are not progressing towards a JIC. These IT may be candidates for placement on the OARL.

(6) The ISG Tri-Chairs will confer with JITC and ISG members to determine if an ICTO is appropriate for fielded IT that does not have approved interoperability requirements. Fielded IT validated through a Joint Urgent Operational Need or Joint Emergent Operational Need, as defined in CJCSI 5123.01 and DoDI 5000.81, does require an ICTO, JIC, or Waiver to Policy

unless it is determined that the capability serves an enduring purpose and will transition to a program of record.

(7) JITC's ISG Resource website contains additional instructions regarding the ICTO procedures, templates, and ISG POCs: https://jitc.fhu.disa.mil/projects/isgsite.

(8) ICTO memoranda for programs can be obtained using the search engine on the STP: https://stp.jitc.disa.mil/. ICTO status information can be found under the STP drop-down menu "Reports/Document Reports/ICTO Report" section.

(9) Each time a CAO decision is made, including renewals, the CAO must verify that any ICTOs have not expired.

(10) Operational IT, for which ICTO requests have expired without action by the PM/Sponsor or have been disapproved by the ISG and do not have a JIC, will be considered for placement on the OARL for monitoring and tracking purposes.

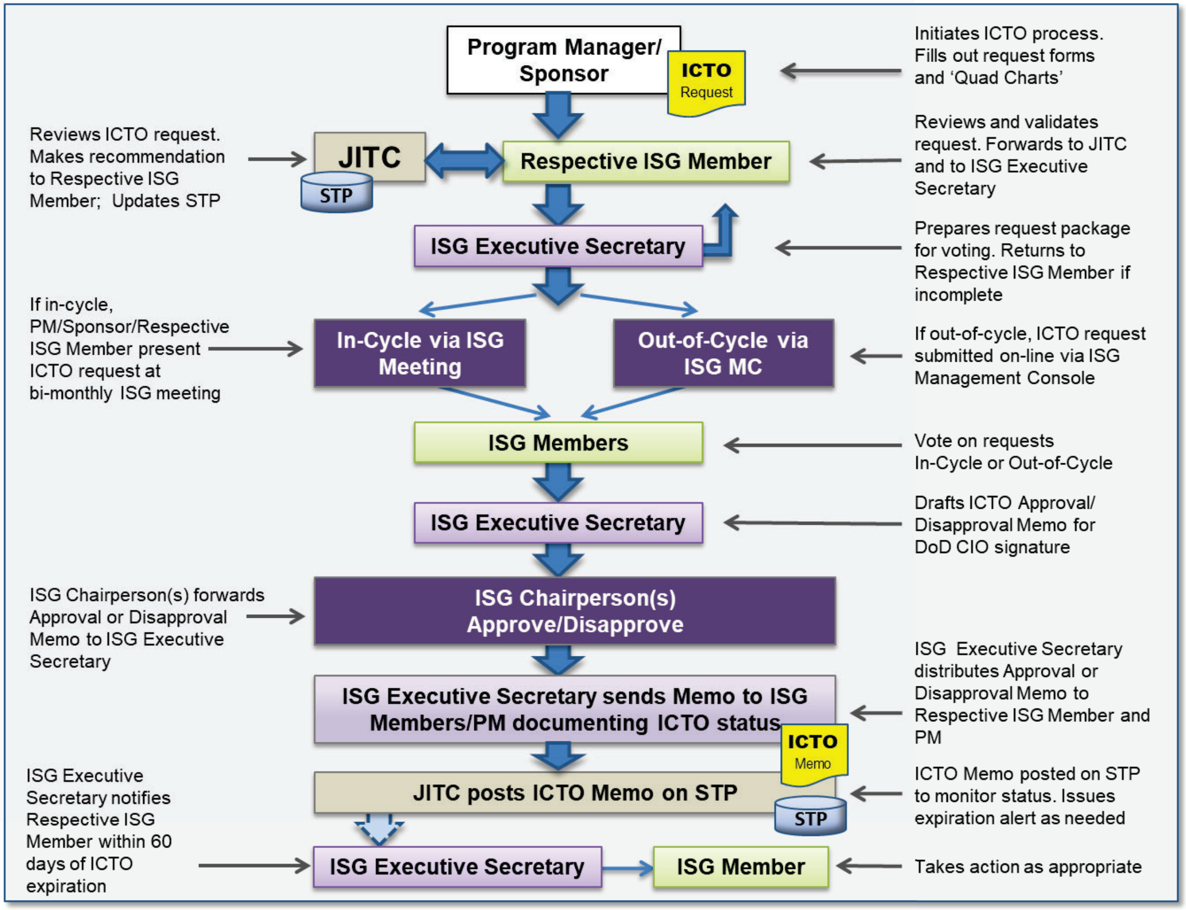
(11) Total duration of an ICTO must normally not exceed one (1) year; however, the ISG may consider an extension if, and only if, progress is made towards interoperability certification. Each request will be reviewed on a case-by-case basis.

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

(1) The PM/Sponsor submits ICTO requests in coordination with their respective ISG representative; JITC cannot submit requests for ICTOs. The JITC ISG Resource website contains templates and forms for ICTO requests: https://jitc.fhu.disa.mil/projects/isgsite. The PM/Sponsor should coordinate with JITC for the content and correctness of ICTOs prior to formal submission.

(a) When requesting an "initial" ICTO, the PM/Sponsor must submit the requisite ICTO Quad Chart and Systems Viewpoint (SV)-1 (i.e., Systems Interface Description) diagram through their respective ISG member. Agencies not listed as chartered members of the ISG should coordinate directly with the ISG Executive Secretary for the submission of ICTO requests. The PMs/Sponsors submitting initial ICTO requests will work with the respective ISG member (or ISG Executive Secretary if appropriate) to initiate contact with JITC; JITC will then identify an action officer.

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


Program Manager/ Sponsor
ICTO Request
Initiates ICTO process. Fills out request forms and 'Quad Charts'
Reviews ICTO request. Makes recommendation to Respective ISG Member; Updates STP
JITC
STP
Respective ISG Member
Reviews and validates request. Forwards to JITC and to ISG Executive Secretary
ISG Executive Secretary
Prepares request package for voting. Returns to Respective ISG Member if incomplete
If in-cycle, PM/Sponsor/Respective ISG Member present ICTO request at bi-monthly ISG meeting
In-Cycle via ISG Meeting
Out-of-Cycle via ISG MC
If out-of-cycle, ICTO request submitted on-line via ISG Management Console
ISG Members
Vote on requests In-Cycle or Out-of-Cycle
ISG Executive Secretary
Drafts ICTO Approval/ Disapproval Memo for DoD CIO signature
ISG Chairperson(s) forwards Approval or Disapproval Memo to ISG Executive Secretary
ISG Chairperson(s) Approve/Disapprove
ISG Executive Secretary sends Memo to ISG Members/PM documenting ICTO status
ICTO Memo
ISG Executive Secretary distributes Approval or Disapproval Memo to Respective ISG Member and PM
JITC posts ICTO Memo on STP
STP
ICTO Memo posted on STP to monitor status. Issues expiration alert as needed
ISG Executive Secretary notifies Respective ISG Member within 60 days of ICTO expiration
ISG Executive Secretary
ISG Member
Takes action as appropriate

LEGEND:

CIO	Chief Information Officer	JITC	Joint Interoperability Test Command
DoD	Department of Defense	MC	Management Console
ICTO	Interim Certificate to Operate	PM	Program Manager
ISG	Interoperability Steering Group	STP	System Tracking Program

Figure 6-1. Procedures for Processing ICTO Requests

(2) The PM/Sponsor will send the ICTO request to the respective ISG member. The ISG POC List on JITC's ISG Resource website contains a complete list of ISG members and contact information: https://jitc.fhu.disa.mil/projects/isgsite.

(3) The ISG member will review and validate the ICTO request. If the ISG member concurs with the request, the ISG member will forward the request to the JITC AO for further validation. If the ISG member or JITC AO do not concur, the request will be sent back to the PM/Sponsor for corrective action

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

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

(6) The JITC AO input will be provided by filling out the five questions listed under the system's STP entry labeled "ISG Questions & Answers" using the web-based STP.

(7) If the mandatory sections of the ICTO Quad Chart are not completed properly, the request will be returned to the ISG member for corrective action. Once the quad chart has been completed properly, the ISG member will send the ICTO request to the ISG Executive Secretary. The ISG Executive Secretary will coordinate with the JITC AO regarding outstanding programmatic issues, interoperability testing status, funding for Joint Interoperability TE&C support, and recommendations pertaining to the ICTO request.

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

(9) If processed Out-of-Cycle (OOC), the ISG member will forward the ICTO request to the ISG Executive Secretary for input in the ISG Management Console. The ISG Executive Secretary 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) The PMs/Sponsors submitting initial ICTO requests for OOC processing must:

1. 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.

2. Brief the panel at the next scheduled ISG meeting if significant progress has not been made towards JIC.

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

(10) The ISG Executive Secretary will forward signed/approved ICTO memoranda to the PM/Sponsor and the ISG members documenting the ICTO status.

(11) JITC will post all ICTO memoranda (including disapproval memoranda) 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 30 days.

(12) Each time a CAO decision is made, including renewals, the CAO must verify that any ICTOs have not expired.

(13) When an ICTO is within 60 days of expiration, the ISG Executive Secretary will notify the ISG member that action is needed. It is the responsibility of the ISG members to ensure resolution of all expiring or expired ICTOs.

7. Waivers to IT Interoperability Policy

a. Components IT. The DoD Components may approve requests to waive Component interoperability policy for DoD Component-unique IT interoperability requirements (i.e., no joint, multinational, or interagency interoperability requirements). Upon approval, the DoD Component will provide the DoD CIO with copies of the waiver request, waiver approval memorandum, and the Joint Staff Net-Ready Certification documenting that joint certification is not applicable (i.e., a Not Applicable memorandum).

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

c. Waiver Process:

(1) The DoD CIO, in coordination with JITC, Joint Staff, and USD(A&S), will consider policy waivers only if one of the following criteria are met:

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

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

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

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

(3) The DoD CIO, in coordination with the USD(A&S) and the CJCS, grants waivers to DoD interoperability policy for IT with joint interoperability requirements. The DoD Components grant waivers to Component interoperability policy.

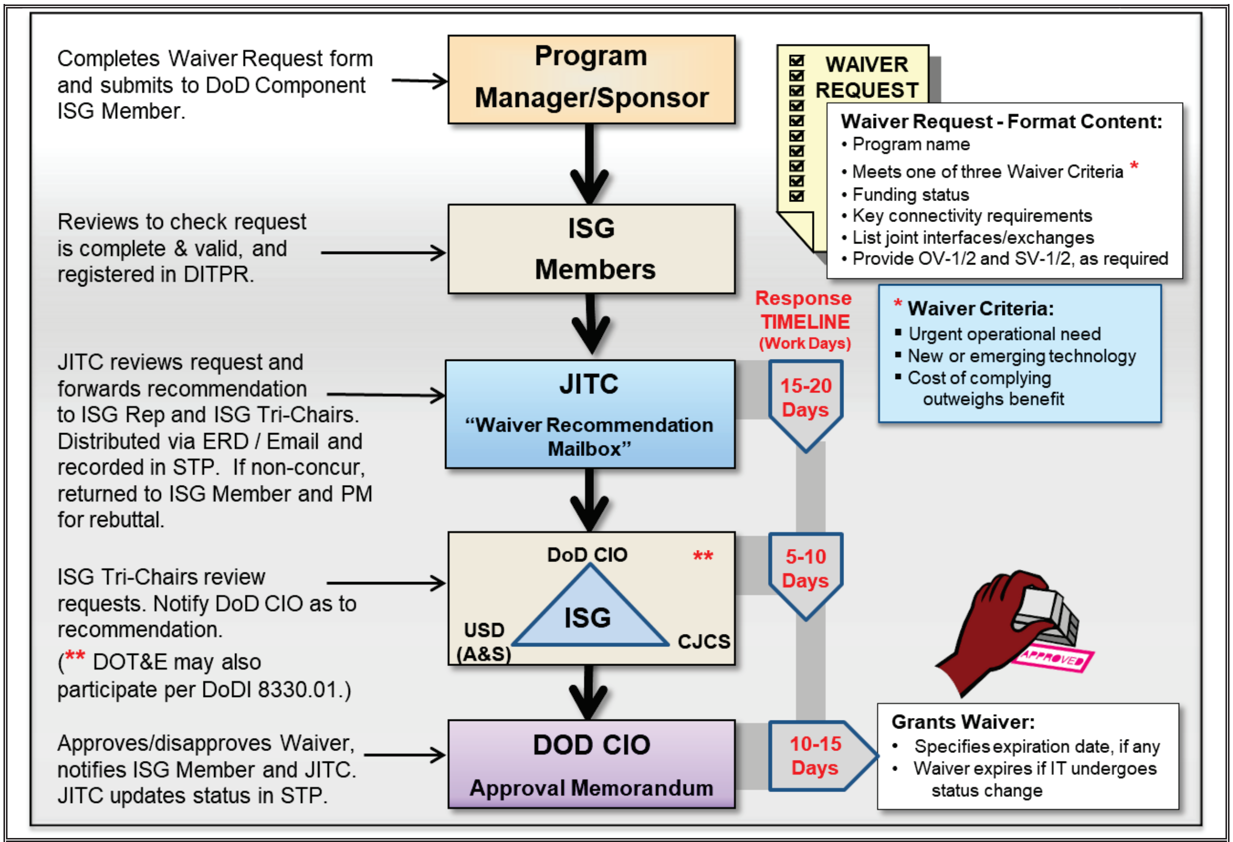
(4) JITC must review all requests for waivers of interoperability policy requiring DoD CIO approval, analyze those requests by assessing risk to the network and DoD operations, and provide a recommendation to the DoD CIO.

(a) The final decision on the waiver request will be made by the DoD CIO.

(b) If approved, the IT will be waived from the interoperability policy requirements cited in the request.

(5) Each time a CAO decision is made, including renewals, the CAO must verify that any waivers have not expired.

d. Waiver Procedures. The PM/Sponsor is responsible for generating the waiver request, using the request form available: https://jitc.fhu.disa.mil/projects/isgsite. Figure 7-1 summarizes these procedures.



Completes Waiver Request form and submits to DoD Component ISG Member.

Reviews to check request is complete & valid, and registered in DITPR.

JITC reviews request and forwards recommendation to ISG Rep and ISG Tri-Chairs. Distributed via ERD / Email and recorded in STP. If non-concur, returned to ISG Member and PM for rebuttal.

ISG Tri-Chairs review requests. Notify DoD CIO as to recommendation.

(** DOT&E may also participate per DoDI 8330.01.)

Approves/disapproves Waiver, notifies ISG Member and JITC. JITC updates status in STP.

Waiver Request - Format Content:

- Program name
- Meets one of three Waiver Criteria *
- Funding status
- Key connectivity requirements
- List joint interfaces/exchanges
- Provide OV-1/2 and SV-1/2, as required

*** Waiver Criteria:**

- Urgent operational need
- New or emerging technology
- Cost of complying outweighs benefit

Grants Waiver:

- Specifies expiration date, if any
- Waiver expires if IT undergoes status change

LEGEND:

&	and	ERD	Electronic Report Distribution
CIO	Chief Information Officer	ISG	Interoperability Steering Group
CJCS	Chairman of the Joint Chiefs of Staff	IT	Information Technology
DITPR	Department of Defense Instruction Information Technology Portfolio Repository	JITC	Joint Interoperability Test Command
DoD	Department of Defense	OV- #	(DoDAF) Operational Viewpoint
DoDAF	Department of Defense Architecture Framework	PM	Program Manager
DoDI	Department of Defense Instruction	STP	System Tracking Program
DOT&E	Director, Operational Test and Evaluation	SV- #	(DoDAF) Systems Viewpoint
Email	Electronic Mail	USD(A&S)	Undersecretary of Defense for Acquisition and Sustainment

Figure 7-1. Waivers to IT Interoperability Policy Process

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

(2) Requests should be sent to the applicable DoD Component ISG member for review and concurrence. Refer to the ISG Resource website: https://jitc.fhu.disa.mil/projects/isgsite for a listing of the ISG representatives.

(3) ISG members will ensure requests are complete and valid, to include verifying the IT is registered in the DoD Information Technology Portfolio Repository: https://dadms.cloud.navy.mil. If the request is not complete and valid, the ISG member will return it to the PM/Sponsor.

(4) Once the respective ISG member completes and validates the request, the ISG member will send it via e-mail to the JITC waiver recommendation mailbox: disa.huachuca.jt.mbx.waiver-recommendation@mail.mil.

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

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

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

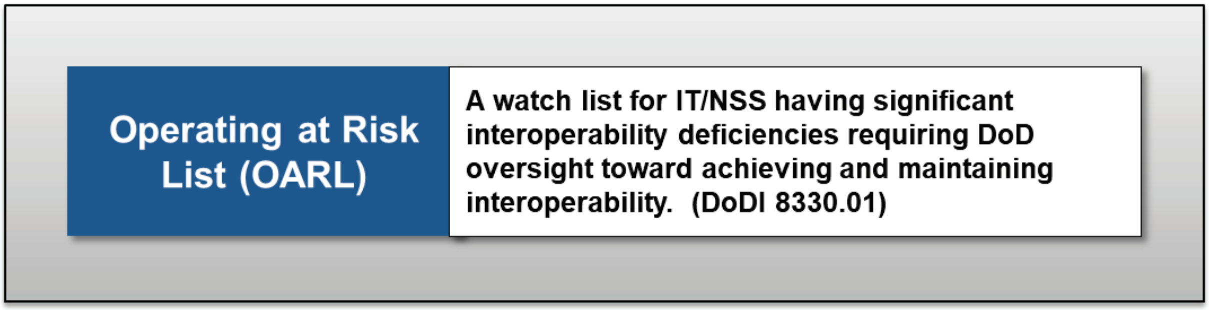
(6) DoD CIO, in coordination with the ISG Tri-chairs (and members if necessary), will approve or disapprove the waiver within 10 to 15 working days of receipt of the waiver request package, which included the request, JITC recommendation, and PM/Sponsor rebuttal if provided. If approved, the IT will be waived from the interoperability requirements of the policy cited in the request form. Waivers may be either permanent or temporary, at the discretion of the DoD CIO. If disapproved, the PM/Sponsor will comply with the interoperability policy as written.

(7) A waiver to policy memorandum will be issued following the initial e-mail approval verifying the IT 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 IT undergoes changes that affect interoperability. Status, recommendations, and memoranda for waiver requests are stored in the JITC STP: https://stp.jitc.disa.mil/.

e. Rescission of Waivers. Policy waivers granted by the DoD CIO may be rescinded when waiver criteria are no longer valid (e.g., when the cost of complying with the policy does not outweigh the benefit to DoD). JITC and ISG members may provide recommendations for waiver rescissions to the ISG Tri-Chairs for consideration and recommendation with a final determination by the DoD CIO.

8. Operating At Risk List

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



Operating at Risk List (OARL)

A watch list for IT/NSS having significant interoperability deficiencies requiring DoD oversight toward achieving and maintaining interoperability. (DoDI 8330.01)

LEGEND:

DoD	Department of Defense	NSS	National Security Systems
DoDI	Department of Defense Instruction	OARL	Operating at Risk List
IT	Information Technology		

Figure 8-1. OARL Description

b. Criteria. Joint IT connected to any operational DoD network will be considered for placement on the OARL when operating without a JIC, ICTO, or have not received an appropriate waiver to DoDI 8330.01. In addition, criteria for nominating IT to the OARL include, but are not limited to:

(1) Joint interoperability deficiencies observed during operational exercises or real-world operations.

(2) Operational problems noted with tactics, techniques, and procedures, and training that impact joint interoperability for fielded (legacy) IT.

(3) No plans for JIC (when it is required).

(4) Deficiencies that prevent issuing JIC and no plan to address deficiencies.

(5) Lack of interoperability requirements products or test documentation.

(6) Unresolved issues from other activities concerned with interoperability (e.g., Overarching Integrated Product Teams).

(7) Non-compliance with approved integrated architectures.

(8) No plans to address interoperability T&E criteria, measures, and requirements established by intelligence functional managers (e.g., NGA and NSA).

(9) No plans to upgrade to prescribed standards (e.g., new or revised standards), or no DoD CIO approved waiver to DoD IT standards policy, in accordance with DoDI 8310.01.

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

d. Access. The OARL is maintained on the ISG Management Console and direct access is given only to ISG voting members. Other authorized personnel can obtain a copy of the OARL from the ISG Executive Secretary by request only.

e. Distribution. The Defense Information Systems Agency (DISA) updates the OARL, and DoD CIO distributes at least quarterly to all DoD MDAs; affected IT fielding authorities (for non-Acquisition Category (ACAT) IT); the CJCS; the DoD Component CIOs; the Combatant Commands (CCMDs) CIOs; the USD(A&S), the USD Research and Engineering and the DISA CAO. The USD(A&S) and DoD Component heads assist the DoD CIO to distribute the OARL to all DoD Component MDAs and affected IT fielding authorities.

(1) The DoD CIO will send a “Memorandum of Notification” to the responsible Service Component or Agency (ATTENTION: ISG Representative) upon the ISG’s initial decision to place an IT on the OARL.

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

e. Effect. Placement on the OARL may require the applicable PM/Sponsor to appear before the ISG for status updates as required. If the ISG is not satisfied with the program's progress towards JIC, the ISG will notify the appropriate MDA or acquisition decision authority and the DISA CAO for further action.

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

9. Supporting Evaluations and Resources

a. Standards Based T&E. Standards based T&E is a fundamental part of fielding an IT. A standards conformance or compliance assessment and certification is a significant step towards verifying interoperability and other IT or capability requirements, however, is not sufficient to ensure joint interoperability. Components fielding joint capabilities should ensure IT standards profiles are monitored throughout the lifecycle to identify changes (e.g., to the IT or environment) and pursue IT updates and retesting to address changes.

(1) Standards Conformance. This type of standards based T&E is confirmation by testing that an IT, product, IT service, or interface adheres to a standard, standards profile, or specification. Standards conformance assessments and certifications are issued at the conclusion of technical testing against a standard/standards profile to describe the degree of conformance to that standard/profile.

(2) Standards Compliance. This type of standards based T&E is the verification and validation that documentation for a system, product, IT services, or interface complies with the policy in this issuance in accordance with DoDI 8310.01.

(3) PMs need to coordinate with the appropriate test organization to conduct necessary standards based T&E.

b. Foreign Systems T&E. JITC can evaluate interoperability of foreign IT systems and issue an assessment when interoperability requirements are defined. Validation of interoperability requirements for foreign systems are routed through the Coalition Interoperability, Assurance, and Validation (CIAV) office of Joint Staff J-6 DDC5I. JITC can evaluate interoperability of foreign IT and issue a JIC only if (1) there are Joint Staff certified joint interoperability requirements (i.e., Net-Ready Certification) and (2) the IT has a DoD Component sponsor. Standards based assessments and certifications may be issued for foreign systems and may be used to support interoperability evaluations. All DoD evaluations of foreign IT must be coordinated through the Foreign Military Sales process.

c. Other Federal/States IT T&E. JITC may evaluate interoperability of other Federal/States IT when the IT interfaces to, or exchanges information with, DoD IT. JITC can only issue an Interoperability Assessment for IT outside DoD. JITC can also issue standards conformance assessments or certifications for IT based on defined standards.

d. Stimulators/Simulators and Training Systems. Stimulators/simulators and training IT, separate from operational systems, may be used in the testing of IT and to support exercises. These devices may interface with other IT in the testing environment. Using these IT 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 IT that only perform the function of simulation or training and only store, process, or exchange simulated (i.e., not operational) data do not require a JIC. However, they may require accreditation if used for testing, and are not automatically exempt from cybersecurity, spectrum, network connection, and similar policies.

e. IPG Related Information. The JITC public website: 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 IT in the STP, which includes (unclassified) information on ICTOs, and certification status. Authorized users (.mil/.gov) may refer to the STP website: https://stp.jitc.disa.mil/ for access instructions.

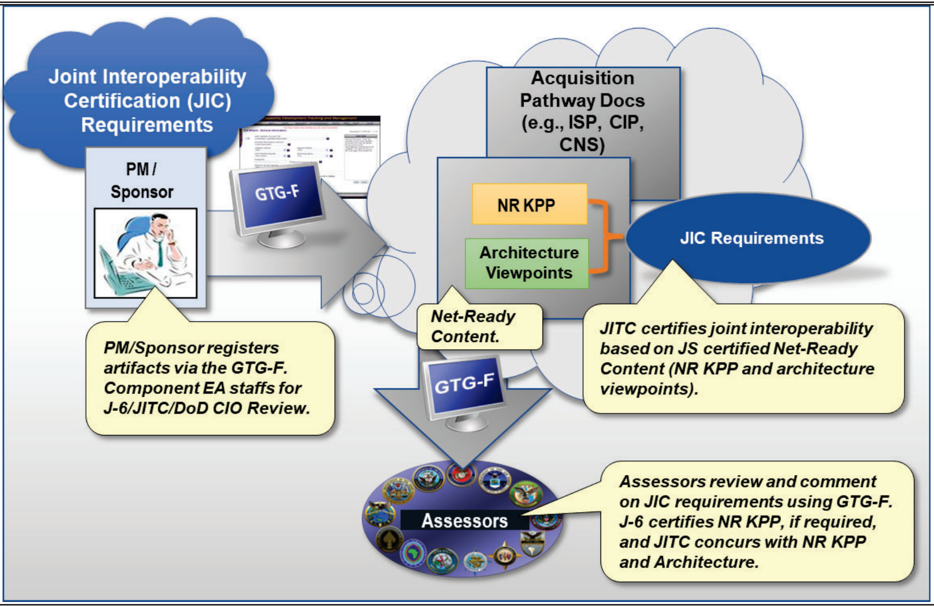
10. Requirements for Joint Interoperability Certification

Sources for approved joint interoperability requirements include, the Capability Development Document (CDD), the Software Initial Capabilities Document ISP, CNS, and other documents specified in the JCIDS Manual or acquisition pathway policies. These requirements documents, when approved, should contain the information needed to support a JIC (i.e., a certified NR KPP and the required architecture viewpoints). Requirements documents are approved after undergoing a joint review. The purpose of these joint reviews is to enable DoD Components to formally verify that their interoperability equities are considered., e.g., the Air Force can review Army programs for Air Force interoperability equities. The Joint Staff J-6 utilizes their NR KPP and Interoperability Smart Book during a joint review to assess the NR KPP for both JCIDS and non-JCIDS documents.

a. Joint Interoperability Requirements Overview (JCIDS).

(1) The Joint Staff uses the KM/DS Tool to review and approve JCIDS documents, which contain the NR KPP and associated architecture viewpoints required for documenting IT requirements and evaluating joint interoperability.

(2) See the JCIDS Manual for detailed process and procedures.


Joint Interoperability Certification (JIC) Requirements
PM / Sponsor
GTG-F
Acquisition Pathway Docs (e.g., ISP, CIP, CNS)
NR KPP
Architecture Viewpoints
JIC Requirements
Net-Ready Content.
GTG-F
Assessors

PM/Sponsor registers artifacts via the GTG-F. Component EA staffs for J-6/JITC/DoD CIO Review.

JITC certifies joint interoperability based on JS certified Net-Ready Content (NR KPP and architecture viewpoints).

Assessors review and comment on JIC requirements using GTG-F. J-6 certifies NR KPP, if required, and JITC concurs with NR KPP and Architecture.

LEGEND:

CIO	Chief Information Officer	GTG-F	GIG Technical Guidance Federation
CIP	Capability Implementation Plan	ISP	Information Support Plan
CNS	Capability Needs Statement	J-6	Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber
Docs	Documents		
DoD	Department of Defense	JITC	Joint Interoperability Test Command
e.g.	for example	JS	Joint Staff
EA	Executive Agent	NR KPP	Net-Ready Key Performance Parameter
GIG	Global Information Grid	PM	Program Manager

Figure 10-1. Joint Interoperability Requirements Process Overview (Non-JCIDS)

b. Joint Interoperability Requirements Overview (Non-JCIDS).

(1) The DoD Components use the GTG-F for joint review and approval of ISPs that contain the NR KPP and associated architecture viewpoints required for evaluating joint interoperability.

(2) DoD Components using pathways specific artifacts (e.g., non-ISP and non-JCIDS products such as a CIP or CNS) also use the GTG-F for review and approval of their joint interoperability requirements. The pathway artifacts are comprised of the same (or "similar") required artifacts, for joint interoperability evaluation (See Figure 10-1).

(3) Section 11 of this guide identifies the minimum set of architecture information.

(4) See Appendices E and F of this guide for development and approval of requirements in ISP and non-ISP products (e.g., CIPs, CNS, etc.) respectively.

c. Non-JCIDS Joint Interoperability Requirements Development and Review. PM/Sponsor development of interoperability requirements for a JIC uses the federated suite of tools found in the GTG-F: https://gtg.csd.disa.mil. Detailed instructions for creating and tasking the DoD Components for joint reviews are available on the GTG-F. The PM/Sponsor may request a review of partial requirements–those meeting the minimum needs for JIC–before the full set of documentation has been produced. This allows for expedited certification. The following highlights the JIC requirements review and approval process:

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

(2) Net-Ready Certification is documented within the GTG-F tool suite for NR KPPs that are not certified within the JCIDS process (e.g., NR KPPs for programs under the MTA pathway). Net-Ready Certification occurs at, or before, the Milestone C final review for programs under the MCA pathway. The point for Net-Ready Certification varies for other acquisition pathways.

(a) The Joint Staff is the Net-Ready Certification authority for IT with joint interoperability requirements.

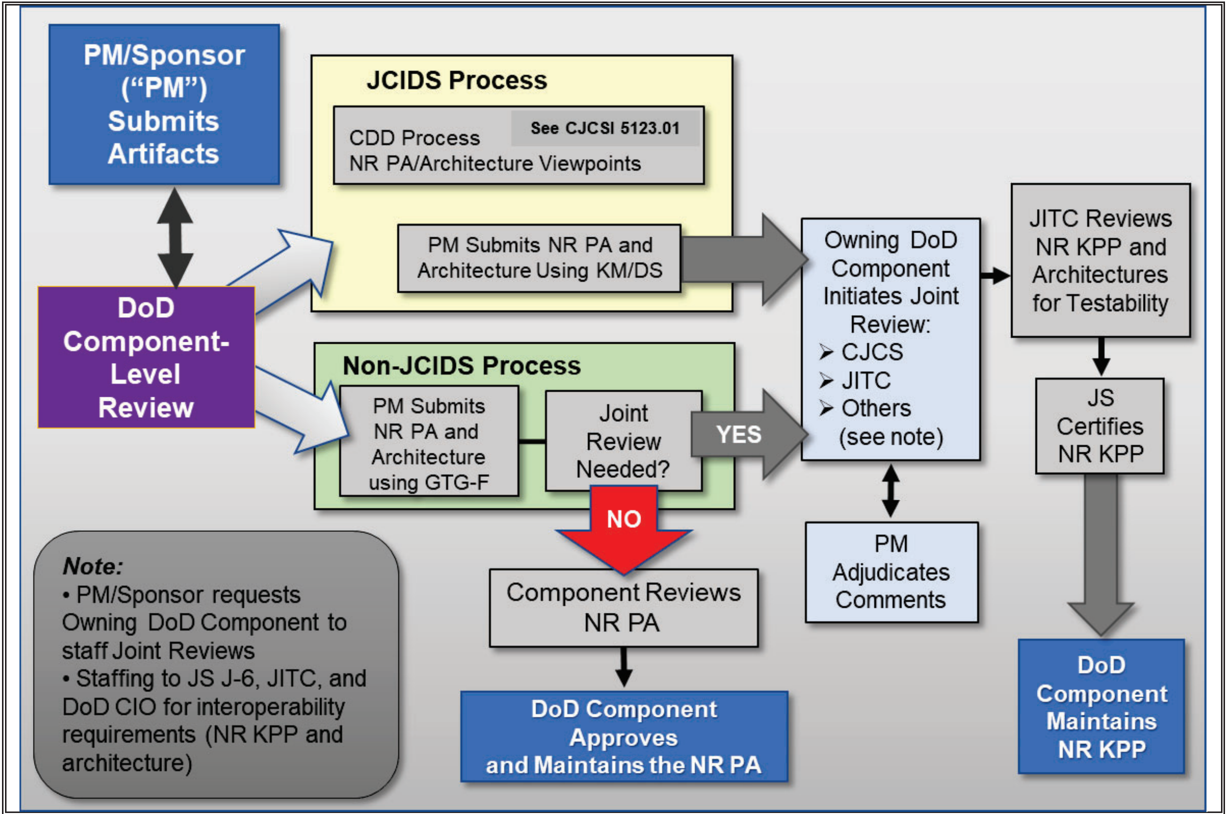
(b) DoD Components approve the Net-Ready performance attribute for IT without joint interoperability requirements.

(3) JITC reviews the NR KPP and required architecture to verify they are testable and measurable to support a JIC prior to Joint Staff Net-Ready Certification.

(4) The ISG will address unresolved issues, when needed.

(5) Regardless of the acquisition pathway, the Joint Staff Net-Ready Certification is required before a JIC can be issued.

d. Additional Requirements Considerations. The review process includes internal DoD Component-level and joint-level reviews/approvals, with the PM/Sponsor submitting artifacts via the GTG-F. Figure 10-2 depicts the joint interoperability requirements review and approval process.


PM/Sponsor ("PM") Submits Artifacts
DoD Component-Level Review
JCIDS Process
CDD Process
NR PA/Architecture Viewpoints
See CJCSI 5123.01
PM Submits NR PA and Architecture Using KM/DS
Non-JCIDS Process
PM Submits NR PA and Architecture using GTG-F
Joint Review Needed?
YES
NO
Owning DoD Component Initiates Joint Review:
➢ CJCS
➢ JITC
➢ Others
(see note)
JITC Reviews NR KPP and Architectures for Testability
JS Certifies NR KPP
PM Adjudicates Comments
Component Reviews NR PA
DoD Component Approves and Maintains the NR PA
DoD Component Maintains NR KPP
Note:
• PM/Sponsor requests Owning DoD Component to staff Joint Reviews
• Staffing to JS J-6, JITC, and DoD CIO for interoperability requirements (NR KPP and architecture)

LEGEND:

CDD	Capability Development Document
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
DoD	Department of Defense
EA	Executive Agent
GTG-F	Global Information Grid (GIG) Technical Guidance Federation
J-6	Joint Staff Directorate for Command, Control, Communications, & Computers/Cyber
JCIDS	Joint Capabilities Integration Development System
JITC	Joint Interoperability Test Command
JS	Joint Staff
KM/DS	Knowledge Management and Decision Support
NR KPP	Net-Ready Key Performance Parameter
NR PA	Net-Ready Performance Attribute
PM	Program Manager

Figure 10-2. Joint Interoperability Requirements Review and Approval Process

(1) For JCIDS IT (e.g., MCA programs required to comply with the JCIDS), they may include an NR KPP already certified by the Joint Staff as part of the CDD process. If so, the Joint Staff will verify that no major changes have occurred since NR KPP certification.

(2) For non-JCIDS IT, the PM/Sponsor will request a joint review and Joint Staff Net-Ready Certification of the Net-Ready performance attribute. If Net-Ready Certification is not required (i.e., no joint interoperability requirements), the PM/Sponsor should receive a Not Applicable memorandum from the Joint Staff. The authority to approve or certify the (non-joint) Net-Ready performance attribute passes to the DoD Component.

(3) For joint reviews,

(a) JITC reviews the NR KPP and the associated architecture to verify they are testable and measurable for a JIC.

(b) The Joint Staff certifies the NR KPP, if needed.

(c) The DoD CIO reviews the NR KPP and the associated architecture for standards compliance.

(4) The DoD Component maintains the NR KPP after Joint Staff Net-Ready Certification. The IT should be ready for T&E leading to JIC when the IT is sufficiently mature to provide a joint capability and the NR KPP is certified.

(5) The DoD Component will coordinate with the Joint Staff when changes are made to the NR KPP to determine when updated requirements need to be staffed for Net-Ready Certification.

e. Requirements Document Review Staffing Guidance.

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

(a) Identify the deficiency.

(b) Provide a specific recommendation.

(c) Provide rationale for the comment/recommendation.

(2) The goal is to identify all critical comments early, so they can be resolved before the final review stages. Critical comments provided during a final review can affect a Milestone C/fielding decision. If an issue will prevent the IT from achieving interoperability certification, then the comment should be marked "critical." All other concerns should be marked "substantive" or "administrative," as appropriate. Reviewers/assessors should contact the PM/Sponsor about critical questions or concerns to avoid misunderstandings that may cause unnecessary delays. The PM/Sponsor also needs to work closely with the reviewers/assessors to provide any additional requested input or clarification. Adequately addressing the issues to improve the accuracy and completeness of the document will help move it through the review process in a timely manner. Reviewers/assessors must contact the PM/Sponsor about any critical comments during final reviews to allow for proper coordination and timely resolution of the critical issue.

f. Joint Interoperability Certification Requirements Data Repository.

(1) Artifacts associated with requirements for JIC (e.g., NR KPP, Joint Staff Net-Ready Certification, or 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 PM/Sponsor must:

(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 IT life-cycle.

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

11. Minimum Set of Architecture Information Required for Joint Interoperability Evaluation

JITC needs the information provided in DoDAF viewpoints, identified in Figures 11-1 and 11-2, to evaluate IT for JIC. These viewpoints, with the exceptions of the All Viewpoint (AV)-2 and OV-5b, are required for JCIDS submissions and may be included in an ISP or other requirements document. Additionally, Joint Staff uses the OV-2, OV-4, OV-5a, and SV-1 or SV-2 for determination of Net-Ready applicability (joint equities). The PMs/Sponsors should coordinate with Joint Staff and JITC early to address the NR KPP and architecture viewpoints (i.e., the joint interoperability requirements).

a. Architecture Viewpoints Required for Joint Interoperability Certification. The architecture viewpoints must be complete, accurate representations of the IT, and information in each product should represent the underlying integrated set of architecture data. The "Required" viewpoints are the minimum set needed to provide JITC the information to build a test plan and evaluate the performance of the IT. "Conditional" viewpoints become required when the IT has heavy reliance on services, or the viewpoints do not give a full picture of resources but are otherwise not necessary for interoperability test and certification. Additional viewpoints are often useful. The PM/Sponsor must coordinate with the JITC AO to establish specific architecture viewpoint requirements, and ensure those requirements are complete, detailed, measurable, and testable.

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

(1) Data and Information Viewpoints (DIV)-2 and DIV-3 are required when critical Operational/System Resources are not clearly defined in the OV-3/SV-6 (respectively).

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

(3) AV-2 is required when acronyms, abbreviations, and special terms are not elsewhere defined and explained in the required architecture viewpoints that the PM/Sponsor provides.

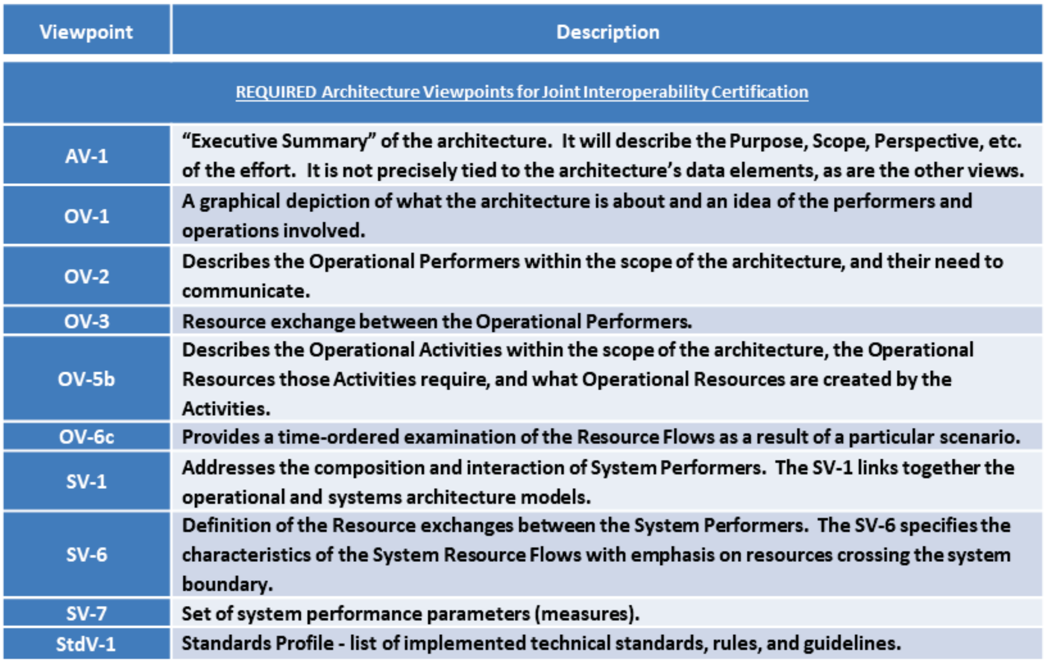
(4) SV-2 is required when the networks or communications media are not identified in the NR KPP (Attribute 2), SV-1, SV-6, SV-7, OV-3, and OV-6c. JITC needs to align IT tasks and information exchanges with networks to ensure all exchange paths are tested.

(5) SV-5a is required when required viewpoints do not provide enough clarity or JITC needs more detailed information on the relationship of IT activities (information

exchanges/elements) to mission activities and tasks, enabling JITC in creating test scenarios to verify that user actions and information exchanges exercise IT functions.

(6) Standards Viewpoint (StdV)-2 is required when a system implements emerging standards.

c. Detailed Interoperability Architecture Requirements and Interoperability Requirements Processing. The ISG Resource website: https://jitc.fhu.disa.mil/projects/isgsite contains detailed information (the "JITC Test and Evaluation Guide for Action Officers Architectures for Joint Interoperability Test, Evaluation and Certification") on the minimum set of architecture requirements and data elements used for certification. The Joint Staff Warfighting Mission Area Architecture Federation and Integration Portal: https://wmaafip.js.mil/ contains additional architecture information. This portal provides important reference architecture information including the WMA Architecture Development Standard, the Joint Information Environment architectures, JMTs, Integrated Dictionary information, and links to related sites.

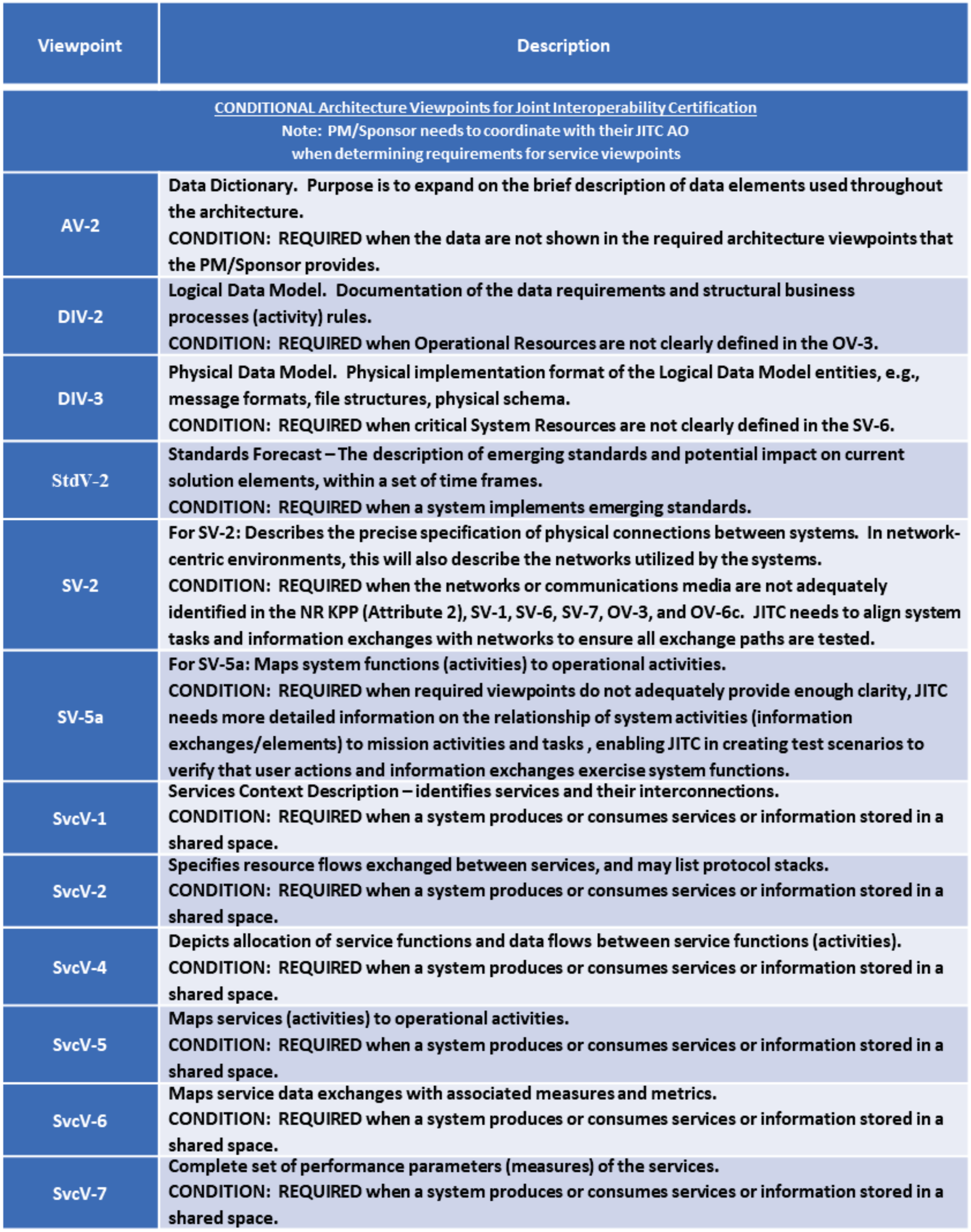


Viewpoint	Description
REQUIRED Architecture Viewpoints for Joint Interoperability Certification	
AV-1	"Executive Summary" of the architecture. It will describe the Purpose, Scope, Perspective, etc. of the effort. It is not precisely tied to the architecture's data elements, as are the other views.
OV-1	A graphical depiction of what the architecture is about and an idea of the performers and operations involved.
OV-2	Describes the Operational Performers within the scope of the architecture, and their need to communicate.
OV-3	Resource exchange between the Operational Performers.
OV-5b	Describes the Operational Activities within the scope of the architecture, the Operational Resources those Activities require, and what Operational Resources are created by the Activities.
OV-6c	Provides a time-ordered examination of the Resource Flows as a result of a particular scenario.
SV-1	Addresses the composition and interaction of System Performers. The SV-1 links together the operational and systems architecture models.
SV-6	Definition of the Resource exchanges between the System Performers. The SV-6 specifies the characteristics of the System Resource Flows with emphasis on resources crossing the system boundary.
SV-7	Set of system performance parameters (measures).
StdV-1	Standards Profile - list of implemented technical standards, rules, and guidelines.

LEGEND:

AV- #	(DoDAF) All Viewpoint	OV- #	(DoDAF) Operational Viewpoint
DoDAF	Department of Defense Architecture Framework	SV- #	(DoDAF) Systems Viewpoint
e.g.	for example	StdV- #	(DoDAF) Standards Viewpoint
etc.	et cetera (and so on)		

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



Viewpoint	Description
CONDITIONAL Architecture Viewpoints for Joint Interoperability Certification Note: PM/Sponsor needs to coordinate with their JITC AO when determining requirements for service viewpoints	
AV-2	Data Dictionary. Purpose is to expand on the brief description of data elements used throughout the architecture. CONDITION: REQUIRED when the data are not shown in the required architecture viewpoints that the PM/Sponsor provides.
DIV-2	Logical Data Model. Documentation of the data requirements and structural business processes (activity) rules. CONDITION: REQUIRED when Operational Resources are not clearly defined in the OV-3.
DIV-3	Physical Data Model. Physical implementation format of the Logical Data Model entities, e.g., message formats, file structures, physical schema. CONDITION: REQUIRED when critical System Resources are not clearly defined in the SV-6.
StdV-2	Standards Forecast – The description of emerging standards and potential impact on current solution elements, within a set of time frames. CONDITION: REQUIRED when a system implements emerging standards.
SV-2	For SV-2: Describes the precise specification of physical connections between systems. In network-centric environments, this will also describe the networks utilized by the systems. CONDITION: REQUIRED when the networks or communications media are not adequately identified in the NR KPP (Attribute 2), SV-1, SV-6, SV-7, OV-3, and OV-6c. JITC needs to align system tasks and information exchanges with networks to ensure all exchange paths are tested.
SV-5a	For SV-5a: Maps system functions (activities) to operational activities. CONDITION: REQUIRED when required viewpoints do not adequately provide enough clarity, JITC needs more detailed information on the relationship of system activities (information exchanges/elements) to mission activities and tasks , enabling JITC in creating test scenarios to verify that user actions and information exchanges exercise system functions.
SvcV-1	Services Context Description – identifies services and their interconnections. CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.
SvcV-2	Specifies resource flows exchanged between services, and may list protocol stacks. CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.
SvcV-4	Depicts allocation of service functions and data flows between service functions (activities). CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.
SvcV-5	Maps services (activities) to operational activities. CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.
SvcV-6	Maps service data exchanges with associated measures and metrics. CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.
SvcV-7	Complete set of performance parameters (measures) of the services. CONDITION: REQUIRED when a system produces or consumes services or information stored in a shared space.

LEGEND:

AO	Action Officer (JITC)	JITC	Joint Interoperability Test Command
AV- #	(DoDAF) All Viewpoint	OV- #	(DoDAF) Operational Viewpoint
DIV	(DoDAF) Data and Information Viewpoint	PM	Program Manager
DoDAF	Department of Defense Architecture Framework	SV- #	(DoDAF) Systems Viewpoint
e.g.	for example	SvcV- #	(DoDAF) Services Viewpoint

Figure 11-2. Conditional Architecture Viewpoints for Joint Interoperability Certification

Appendix A References

Chairman of the Joint Chiefs of Staff Instruction 5123.01I, “Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS),” October 30, 2021. Available at: https://www.jcs.mil/Library/CJCS-Instructions/

DoD Architecture Framework (DoDAF). Available at: http://dodcio.defense.gov/dodaf20.aspx

Department of Defense Information Network (DoDIN) Approved Products List (APL) Process Guide. Available at: https://aplits.disa.mil/

DoD Directive 5000.01, “The Defense Acquisition System,” September 9, 2020, as amended. Available at: https://www.esd.whs.mil/Directives/issuances/dodd/

DoD Instruction 5000.02, “Operation of the Adaptive Acquisition Framework,” January 23, 2020, as amended. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 5000.75, “Business Systems Requirements and Acquisition,” February 2, 2017, as amended. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 5000.80, “Operation of the Middle Tier of Acquisition (MTA),” December 30, 2019. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 5000.81, “Urgent Capability Acquisition,” December 31, 2019. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 5000.85, “Major Capability Acquisition,” August 6, 2020, as amended. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 5000.87, “Operation of the Software Acquisition Pathway,” October 2, 2020. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 5000.89, "Test and Evaluation,” November 19, 2020. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 8100.04, “DoD Unified Capabilities (UC),” December 9, 2010. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 8310.01, “Information Technology Standards in the DoD,” April 7, 2023. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 8330.01, “Interoperability of Information Technology, Including National Security Systems,” September 27, 2022. Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 8510.01, “Risk Management Framework for DoD Systems,” July 19, 2022, Available at: https://www.esd.whs.mil/Directives/issuances/dodi/

Global Information Grid Technical Guidance Federation[1].

Interoperability Guide (contained in the Manual for the Operation of the Joint Capabilities Integration and Development System, October 30, 2021). Available at: https://intellipedia.intelink.gov/wiki/Joint_Capabilities_Integration_and_Development_System

JITC System Tracking Program. Available at: https://stp.jitc.disa.mil/

JITC Test and Evaluation Guide, "Architectures for Joint Interoperability Test, Evaluation and Certification, Version 2.2," March, 2023. Available at: https://jitc.fhu.disa.mil/projects/isgsite

Joint Mission Thread (JMT) information on Joint Staff J-6, Warfighting Mission Area Architectures tab. Available at: https://wmaafip.js.mil/

Joint Staff J-6 NR-KPP and Interoperability Smart Book, April 13, 2023. Available at: https://jitc.fhu.disa.mil/projects/isgsite

Knowledge Management and Decision Support System, Version 2, August 15, 2018[2]

Manual for the Operation of the Joint Capabilities Integration and Development System,

October 30, 2021. Available at: https://intellipedia.intelink.gov/wiki/Joint_Capabilities_Integration_and_Development_System

TE-21 Project Charter, May 29, 2018.

TE-21 Cost Benefit Analysis (Final), August 2, 2018.

Unified Capabilities Requirements (UCR). Available at: https://aplits.disa.mil/

[1] Available at: https://gtg.csd.disa.mil/

[2] Available on the SIPRNET at: https://jrockmdsbpm.js.smil.mil (Note: Access requires registration)

Appendix B Abbreviations & Acronyms

A&S	Acquisition and Sustainment
AAF	Adaptive Acquisition Framework
ACAT	Acquisition Category
ATC	Approval to Connect
ATO	Authorization to Operate
AV- #	(DoDAF) All Viewpoint
CAO	Connection Approval Office
Cc	Courtesy Copied
CCDR	Combatant Commander
CCMD	Combatant Command
CIAV	Coalition Interoperability, Assurance, and Validation
CIP	Capability Implementation Plan
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNS	Capability Needs Statement
DAFA	Defense Agencies and DoD Field Activities
DBS	Defense Business System
DevSecOps	Development, Security, and Operations
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry

DIV- #	(DoDAF) Data and Information Viewpoint
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
DOT&E	Director, Operational Test and Evaluation
DOTLPF-P	Doctrine, Organization, Training, Leadership and education, Personnel, and Facilities – Policy
DT&E	Developmental Test and Evaluation
EA	Executive Agent (GTG-F)
GIG	Global Information Grid
GTG-F	GIG Technical Guidance Federation
IATM	Integrated Architecture Traceability Matrix
ICA	Interface Control Agreement
ICTO	Interim Certificate To Operate
IPG	Interoperability Process Guide
IS	Information System
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
JIEP	Joint Interoperability Evaluation Plan
JITC	Joint Interoperability Test Command
JMT	Joint Mission Thread
JPR	Joint Performance Requirement
KM/DS	Knowledge Management and Decision Support
KPP	Key Performance Parameter
MCA	Major Capability Acquisition
MDA	Milestone Decision Authority
MILDEP	Military Department
MOP	Measures of Performance
MTA	Middle Tier of Acquisition
MVCR	Minimum Viable Capability Release
NGA	National Geospatial-Intelligence Agency
NIPRNET	Nonclassified Internet Protocol Router Network
NR KPP	Net-Ready Key Performance Parameter
NSA	National Security Agency
NSS	National Security Systems

OARL	Operating at Risk List
OOC	Out-of-Cycle
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OV- #	(DoDAF) Operational Viewpoint
PDF	Portable Data File
PM	Program Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
RAFT	Requirements Analysis Framework for Test
SIPRNET	SECRET Internet Protocol Router Network
StdV- #	(DoDAF) Standards Viewpoint
STP	System Tracking Program
SUT	System Under Test
SV- #	(DoDAF) Systems Viewpoint
SvcV- #	(DoDAF) Services Viewpoint
T&E	Test and Evaluation
TE&C	Test, Evaluation, and Certification
TEMP	Test and Evaluation Master Plan
TSP	Test Support Plan

UC	Unified Capabilities
UCR	Unified Capabilities Requirements
U.S.	United States
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment

Appendix C Definitions

***Assessment*.** The act or result of determining the contribution or disposition of an activity, product, or condition, based on an appraisal of the state of IT interoperability. [DoDI 8330.01]

***Authorization to Operate (ATO)*.** The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. [NIST SP 800-39].

***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.]

***DoD Component*.** For the purposes of this IPG, DoD Component is defined as Military Departments, Combatant Commands, Defense Agencies and DoD Field Activities (DAFAs), and OSD Components.

***End-to-End Testing*.** The logical means to conduct a mission-based evaluation. End-to-end testing is easiest thought of as testing a mission thread. Mission threads result from a careful analysis of a unit's mission using the system and can be derived from the joint mission essential task list, from the Component-specific mission essential task list, concept of employment, or the Army's operational mission summary and mission profile. The threads should make operational sense and evaluate the intended operational mission from beginning to end. The end-to-end evaluation of each mission thread should rely on testing that includes the entire thread in a single operational event.

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

***External Partner*.** For the purposes of this IPG, External Partner is defined as another DoD Component, U.S. Government Department or Agency (including federal, state, and local), Coalition partners, non-governmental organizations, or any combination thereof that utilize the same interfaces and/or exchange information produced/consumed/shared or distributed by the IT. [derived from DoDI 8330.01 and others]

***GTG-F (GIG Technical Guidance Federation)*.** The online tool that facilitates the creation of Information Support Plans (ISPs) and Standards Viewpoints (StdVs), as well as staffing and reviews of Net-Ready Key Performance Parameters (NR KPP) and DoDAF Architectures. The tool also provides access to the DoD IT Standards Registry (DISR). The GTG-F website is at: https://gtg.csd.disa.mil/.

Interface. The generic connection between two elements that implement information technology in which information is capable of being transmitted from the source element to the destination element" [DoDAF 2.0, Volume 2]

Interface Control Agreement (ICA). ICAs are interface agreements established for each external interface to the IT.

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

Information Support Plan (ISP). A set of information supporting interoperability test and certification. It is entered through the GTG-F, the ISP contains or links the Net-Ready performance attribute along with supporting architectural data. Instructions for completion of the ISP are found on the GTG-F. [DoDI 8330.01]

Information Systems (IS). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Title 44 U.S.C. § 3502]

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). [U.S. Code]

Interface Control Document. An interface control document communicates all possible inputs to and all potential outputs from an IT 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]

Interim Certificate to Operate (ICTO). A temporary authorization to proceed to connection without completing JIC. Issued by the ISG to PMs who have an urgent need to operate IT, have not completed JIC, but are making satisfactory progress towards that goal as determined by the ISG. [DoDI 8330.01]

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 exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment in its operational environment including appropriate cybersecurity aspects. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions in appropriately stressed operational environments over the system's life-cycle. [DoDI 8330.01]

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

Interoperability 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 joint, combined, and coalition forces, other U.S. Government Departments and Agencies (including federal, state, and local), and non-governmental organizations, as appropriate. [derived from DoDI 8330.01 and other sources]

Joint Capabilities Integration and Development System (JCIDS). The primary system used by the Joint Requirements Oversight Council and its subordinate boards to fulfill the CJCS's statutory responsibilities in assessing joint military capabilities, and identifying, approving, and prioritizing gaps in such capabilities, to meet applicable requirements in the National Defense Strategy. [CJCSI 5123.01I]

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 joint, combined, and coalition forces, other U.S. Government Departments and Agencies (including federal, state, and local), and non-governmental organizations, as appropriate. Coalition partners, non-governmental organizations, etc., which share the same physical/logical interfaces will also make an interface "joint." Not all information exchanges over an interface need to be joint for it to be considered a joint interface. [derived from multiple sources]

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

Joint Interoperability Certification. A formal statement of adequacy, provided by the responsible joint interoperability certification authority agency, that a system has met its joint interoperability requirements. [DoDI 8330.01]

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

Joint Interoperability Requirements**.** Any requirement levied on an IT to implement information exchanges to other IT across or beyond a MILDEPs, CCMDs, DAFAs, and OSD Component's boundaries or implement a web service with the explicit or implicit intention to share information with other IT across or beyond their boundaries. [DoDI 8330.01]

Milestone Decision Authority (MDA). The designated individual with overall responsibility for a program. The MDA has the authority to approve entry of an acquisition program into the next phase of the acquisition process and is accountable for cost, schedule, and performance reporting to a higher authority, including congressional reporting. For interoperability purposes, the MDA uses the information and recommendations of the Net-Ready Certification authority and interoperability certification authority to decide if a system is ready to move to the next acquisition milestone. [DoDI 8330.01]

Mission Critical. The criticality of information being exchanged that meets the following categories:

- Force Command and Control – critical and high-level information (e.g., emergency action message or commander's guidance)
- Mission Operations – required in support of operations (e.g., joint task force contingency plans and operations plans)
- Core Functions – ongoing information exchanges (e.g., configuration and guidance information, restricted frequency list)

[DoDAF 1.5, Volume 2]

National Security Systems (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. [U.S. Code]

***Net-Ready*.** DoD IT that meets required information needs, information timeliness requirements, has a cybersecurity accreditation, and meets the attributes required to support military operations, to be entered and managed on the network, and to effectively exchange information for both the technical exchange of information and the operational effectiveness of that exchange.

DoD IT that is net-ready enables warfighters and DoD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all participants.

Net-readiness requires that IT operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure communications within and across diverse media; information is in a common format with a common meaning; common human-computer interfaces for users and effective means to protect the information exist.

Net-readiness is critical to achieving the envisioned objective of a cost-effective integrated environment. Achieving and maintaining this vision requires interoperability within a joint task force or CCMD area of responsibility; across CCMD area of responsibility boundaries; between strategic and tactical systems; within and across Military Services and agencies; from the battlefield to the sustaining base; among U.S., allied, and coalition forces; and across current and future systems. [DoDI 8330.01]

***Net-Ready Certification Authority*.** The office with the authority to certify Net-Ready content. It verifies that the PM/Sponsor has properly scoped, refined, and justified the interoperability requirements of the system. The CJCS is the Net-Ready Certification authority and may delegate this authority to the appropriate MILDEPs, CCDRs, DAFAs, and OSD Components for all IT with no joint interoperability requirements. [DoDI 8330.01]

***Net-Ready Performance Attribute*.** Ensures interoperability between individually developed and fielded capability solutions as outlined in the JCIDS Manual. [DoDI 8330.01]

***Non-JCIDS*.** Any IT, including NSS, programs, that are not requiring JCB/JROC approval, by law, regulation, or policy, but still requiring DoD CIO review/approval. [Derived from Joint Staff J6].

***Operating at Risk List (OARL)*.** A watch list for critical IT and NSS systems having significant interoperability deficiencies requiring DoD oversight toward achieving and maintaining interoperability as defined in the IPG. [DoDI 8330.01]

***Program Manager (PM)*.** The person tasked with developing and fielding the new IT system. [DoDI 8330.01]

Requirements Review Comment Criticality:

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

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

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

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

***Test and Evaluation*.** Process by which a system or components are exercised and results analyzed to provide performance-related information. The information has many uses including risk identification and risk mitigation. Test and evaluation enables an assessment of the systems attainment of the technical performance, specifications, and system maturity. [DoDI 8330.01]

***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]

Appendix D Process Improvement Through Automation

1. GENERAL. The program manager (PM)/Sponsor is encouraged to leverage automation capabilities to improve cost, schedule, and performance. Automation improves rigor and efficiency in joint interoperability test and evaluation (T&E) and certification, mitigating risk to acquisition programs. The Joint Interoperability Test Command (JITC) established a common joint interoperability evaluation framework and standard requirements content and format, based on attributes of the Net-Ready Key Performance Parameter (NR KPP), enabling testers to evolve automation capabilities including tools, templates, and products to support all phases of joint interoperability T&E and certification (pre-test, test, and post-test). Sections 2 through 5 describes anticipated automation capabilities. TE-21 Project Charter and the final TE-21 Cost Benefit Analysis identify potential benefits/reduction in costs/impacts to the PM/Sponsor. The PM/Sponsor should coordinate with JITC early in planning process to identify interoperability requirements information needed and available T&E and certification automation capabilities.

2. REQUIREMENTS ANALYSIS.

a. Ingest Architecture Viewpoints. The capability to consume data from architecture viewpoints in multiple formats facilitates assembly and management of requirements data allowing testers to accelerate interoperability requirements review, analysis, discovery of issues, and resolution through the development of an Integrated Architecture Traceability Matrix (IATM). The ability to ingest architecture viewpoints and automate analysis products (e.g., IATM) will vary based on the formats and content provided by the PM/Sponsor. The analysis products enable the DoD to “shift left” by facilitating meaningful dialog between the PM/Sponsor and testers earlier in the acquisition process (e.g., during pre-test activities).

b. Conduct Requirements Head Start Review. JITC conducts Requirements Head Start Reviews to facilitate pre-test activities. Products include a measures summary (an itemized list of measures, criteria, and conditions organized by NR KPP attribute), traceability nomograph, and standards review. These products identify gaps, discrepancies, and ambiguities in the interoperability requirements products, such as producer-consumer mismatches (e.g., between joint information technology (IT)) and orphaned information exchanges (i.e., exchanges that do not trace to a mission or task). Automation of the Requirements Head Start Review improves timeliness and quality of interoperability requirements.

c. Produce a Requirements Analysis Framework for Test (RAFT). JITC performs detailed reviews of IT requirements to develop the RAFT, which supports requirements analysis, T&E planning (test plans), data collection (e.g., Data Management and Analysis Plan), analysis, and reporting (certifications). Automation of the RAFT improves timeliness and rigor of the interoperability T&E and certification process. The RAFT documents test threads, tracing an IT’s requirements to JITC’s data collection and analysis requirements (i.e., test cards and test methodology). These products support pre-test, test, and post-test activities.

3. TEST PLANNING.

a. Generate Input for Interoperability Test Plan or Test Support Package. JITC uses test plans to document data needs, test methodology, and data collection methods (JITC uses an

Interoperability Test Plan when conducting a test as the responsible test organization and a Test Support Package when JITC is not the responsible test organization). Integrating standardized test plan content with requirements analysis enables automation of test plans and test support packages, which improves timeliness and reduces risk to the PM/Sponsor. These products support test and post-test activities.

b. Generate Test Cards. Test cards include the "who, what, when, where, and how" to evaluate the requirements and explain the test methodology and data collection for individual Information Exchange Requirements, networks, and missions. Auto-generation of test cards improves timeliness, consistency, and rigor of test plan and analysis. This product supports test and post-test activities.

4. DATA ANALYSIS/DATA MANAGEMENT.

a. Improve Data Analysis. Automation capabilities will facilitate the managing, analyzing, and archiving data to improve the timeliness, quality, and consistency of reports. This product supports test and post-test activities.

b. Generate a Test Product Deficiency Report. There are multiple benefits to automating deficiency reports of IT discrepancies/anomalies identified during the T&E process. JITC can use the information to determine conditions to JIC and develop various metrics to track and characterize joint interoperability. This product supports test and post-test activities.

c. Archive the Data. The automation capabilities will support auto-archiving and organization of test data, which facilitates statistical analysis and data sharing across multiple IT and test events. It also will provide testers with a repository to capture deficiencies, evaluation trends and report problems in a timely manner. This product supports test and post-test activities

5. TEST REPORTING.

a. Generate Input for Joint Interoperability Certification (JIC). Using a standardized certification template, automation capabilities will auto-generate portions of the JIC (e.g., NR KPP attribute result and status tables) using requirements analysis and evaluation results, improving timeliness and quality. This product supports post-test activities.

Appendix E ISP Process

1. GENERAL. The information support plan (ISP) is a key document for achieving a joint interoperability certification (JIC). The ISP describes the information technology (IT) and its information needs, dependencies, and interfaces with other IT. It addresses the efficient and effective exchange of information that enables the IT's capabilities. This appendix provides guidance on the ISP process to include the development, submission, review, approval, and archive of ISP requirements. Each Service has its own guide for ISP content. Refer to Department of Defense Instruction 8330.01 for ISP requirements. The Manual for the Operation Joint Capabilities Integration and Development System (JCIDS) provides guidance on how to develop the Net-Ready content.

a. The program manager (PM) will produce an ISP for each milestone or key decision point, such as a critical design review, in accordance with acquisition pathway policies. The milestone decision authority or other decision maker must approve any recommendations from the PM as to what regulatory information should be in the ISP.

b. As part of the ISP and in addition to any Component guidance, the PM must submit architectural data in accordance with Section 11 of this guide to describe the Net-Ready content and interoperability requirements of the IT. The ISP review process will assist the PM to refine the architecture viewpoints resulting in a set of detailed, measurable interoperability criteria for use in interoperability test and evaluation. The IPG Appendix F provides guidance on the development, submission, review, approval, and archive of interoperability requirements for acquisition pathways that are not required to submit an ISP.

c. DoD Components must establish processes to conduct reviews of unclassified ISPs within the Global Information Grid Technical Guidance Federation (GTG-F): https://gtg.csd.disa.mil. DoD Components that do not have a mature ISP review process may request Department of Defense, Chief Information Officer (DoD CIO) assistance, via the appropriate ISG representative: https://jitc.fhu.disa.mil/projects/isgsite, with conducting joint reviews.

d. The PM uses the GTG-F to develop Unclassified or Controlled Unclassified Information ISP content on the Nonclassified Internet Protocol Router Network (NIPRNET). The PM may download a shell of the NIPRNet ISP to develop Classified ISPs in accordance with instructions documented in GTG-F.

e. The procedures in this appendix are based on using GTG-F. The GTG-F contains guides (user documentation/training) that provide technical details on using the tools.

f. The GTG-F serves as a repository for unclassified ISPs and the supporting architecture artifacts. The PM may have additional artifacts stored on another site and include that site address in the ISP. In this case, the PM must provide full instructions for locating and requesting access to the site and artifacts. This is especially important when the documentation includes classified artifacts (e.g., artifacts stored on the SECRET Internet Protocol Router Network (SIPRNET), Joint Worldwide Intelligence Communications System, and special access program).

2. DEVELOP AND SUBMIT. The following details the process for the development and submission of ISP requirements:

a. The PMs of IT programs that do not receive Net-Ready Certification via the JCIDS process must submit the ISP at least 60 days before the scheduled submission date to the Net-Ready Certification Authority, to allow 30 days to review and 30 days to adjudicate comments.

b. The PM begins ISP development on the GTG-F.

c. The Joint Staff and DoD Component must approve any deviations from the GTG-F structure. The PM will be able to develop specialized packages for Standards View, Net-Ready Performance Attribute, or Architecture reviews.

d. The GTG-F can process and store unclassified and controlled unclassified information ISPs. If the ISP is classified or has classified architecture artifacts, the PM should create a shell ISP and provide instructions to locate and request access to the classified material. Instructions for processing classified ISPs on the SIPRNET are posted on GTG-F.

e. The analysis section of the ISP is the major data entry portion. The subsections are also accessible in GTG-F. The GTG-F provides guidance for completing the parts.

f. The PM uses the GTG-F to identify information technology standards. The tool creates a separate Standards View-1 showing the standards to be implemented in the IT. The process can also create a Standards View-2 forecasting the standards for future increments.

g. The GTG-F has multiple ways to include program documents and architecture artifacts. Architecture viewpoints can be associated to relevant sections of the ISP. Documents can also be uploaded to the GTG-F.

h. When the draft ISP is finished, the PM should staff it to the DoD Component for approval. On the GTG-F, the ISP can be downloaded in portable data file (PDF) format. The PDF format can be printed or shared electronically but the reader cannot open embedded artifacts. Some organizations use the GTG-F distribution system to staff internal reviews, but this requires the reviewers to have a GTG-F account.

i. When the ISP has completed a Component-only review, the PM submits it in the GTG-F to the Owning Executive Agent, who is the DoD Component representative responsible for staffing the ISP to other stakeholders for review (i.e., Joint ISP assessment). The PM provides any special instructions, such as particular organizations to review the ISP or how to access additional artifacts. The DoD CIO acts as Owning Executive Agent for many Fourth Estate agencies. Each Service has its Owning Executive Agent (e.g., “MARCORSYSCOM SEAL” is the Owning Executive Agent for Marine Corps programs).

3. REVIEW AND APPROVE. The following details the process for the review and approval of ISP requirements:

a. The DoD Component, via the Owning Executive Agent, must lead the review of all ISPs, regardless of acquisition category (ACAT) level. If a program meets the criteria for a joint review listed below, the DoD Component must staff the ISP for review:

(1) For ACAT II and below IT programs, as well as non-ACAT, the owning DoD Component must select the appropriate additional DoD Components to participate for the joint review; however, the review must include, at the minimum, Joint Staff J-6 DDC4/Requirements Division, DoD CIO Executive Agent, DISA Chief of Staff Executive Agent, and DISA JITC Executive Agent.

(2) For all ACAT I IT programs, the owning DoD Component must staff the ISP to all DoD Components including the Joint Staff J-6 DDC4/Requirements Division, DoD CIO Executive Agent, DISA Chief of Staff Executive Agent, and DISA JITC Executive Agent.

b. The Owning Executive Agent reviews the submitted ISP for completeness and can reject it if it is missing key artifacts.

c. The PM must allow sufficient time before any decision point for the ISP review and adjudication of comments. The typical sequence for the initial review usually allows 30 calendar days for the review and 30 calendar days for adjudication of the comments. The typical sequence for the second and subsequent reviews usually allows for 15 calendar days for the review and 15 calendar days for adjudication of comments. In any case, if more time is needed to complete the review, the assessor or lead assessor may request a review extension via coordination with the Owning Executive Agent.

d. The reviewer or assessor makes comments directly on the GTG-F. The PM should provide a comment resolution matrix or instructions about how to submit comments for classified ISPs or artifacts.

e. The comments should identify the issue, provide a suggested way to address the issue, and the level of importance (Critical, Substantive, or Administrative). Refer to “Requirements Review Comment Criticality” in Appendix C for more information.

f. Comments are only visible within a reviewer’s organization until a lead assessor closes the review, or the review period ends. The reviewer must have permission (i.e., be a lead assessor or Executive Agent) to publish comments, so there may be a delay for stakeholders in seeing all ISP comments. The GTG-F automatically publishes all comments when the review period closes.

g. An organization’s lead assessor is responsible for reviewing the organization’s comments and closing the review for the organization based on the level of importance of the comments in paragraph 3.e.

h. The PM should respond to all comments with acceptance or rejection. The PM also provides the rationale for the response and what actions will be taken.

i. The reviewer should address critical comments with the PM directly and not wait for them to appear on the GTG-F. Critical comments that cannot be resolved will be elevated through the Component designated representative to the DoD CIO for resolution.

j. The PM and reviewer should discuss the proposed adjudication to comments where there are issues with the adjudication. The reviewer should only 'Disapprove' a proposed adjudication as a last resort. Entering 'Disapproved' closes the comment from any further modification to the response by the PM."

k. Critical comments are grounds for a non-concur organizational recommendation. A reviewing organization may provide a non-concur recommendation if they have numerous substantive comments (i.e., inserting a critical comment stating, due to numerous substantive issues a non-concur organizational input is warranted).

l. All critical comments must be, and all substantive comments should be fully adjudicated. The PM will update the ISP based on the agreed to adjudications. The updated ISP will be submitted for follow-on review.

m. All critical comments must be fully adjudicated before the Owning Executive Agent can issue the final approval of the ISP. Upon approval, the ISP becomes the ISP of record. During the system's operations and sustainment lifecycle the PM may have to submit new ISPs to address changes to interfacing systems. The updated or revised ISP becomes the ISP of record.

4. ARCHIVE.

a. The ISP of record and its supporting documentation is saved in the GTG-F.

b. If the Owning Executive Agent or PM prefers to place a copy of the ISP of record in an additional repository to GTG-F, it is recommended that the location of this different repository is referenced on the GTG-F with access instructions.

Appendix F Requirements Process for Other Acquisition Pathways

1. GENERAL. Programs will identify joint interoperability requirements using the processes and products established in the applicable acquisition pathway policies, the Manual for the Operation Joint Capabilities Integration and Developments System (JCIDS Manual) for Net-Ready performance attribute development, and this guide.

a. This appendix provides guidance on the requirements documents process (other than the information support plan (ISP) or JCIDS process) to include the development, submission, review, approval, and archival of the joint interoperability requirements contained in the following documents (not all inclusive):

(1) Net-Ready Key Performance Parameter and supporting architectures (see Section 11 of this guide).

(2) Capability needs statement for software acquisition pathway.

(3) Capability implementation plan for the defense business systems (DBS) acquisition pathway.

(4) Other documents for the middle tier acquisition (MTA) pathway.

b. The program manager (PM)/Sponsor will produce products containing joint interoperability requirements for each key decision point in accordance with acquisition pathway policies or the JCIDS Manual as applicable.

c. As part of the products containing joint interoperability requirements, the PM/Sponsor must submit architectural data in accordance with Section 11 of this guide to describe the Net-Ready content and interoperability requirements of the information technology (IT). The requirements review process will assist the PM/Sponsor to refine the architecture viewpoints, and result in a set of detailed, measurable interoperability criteria for use in interoperability test and evaluation.

d. DoD Components must establish processes to conduct reviews of unclassified products within the Global Information Grid Technical Guidance Federation (GTG-F): https://gtg.csd.disa.mil. DoD Components that do not have a mature review process may request Department of Defense, Chief Information Officer (DoD CIO) assistance, via the appropriate ISG representative: https://jitc.fhu.disa.mil/projects/isgsite, with conducting joint reviews.

e. The GTG-F serves as a repository for unclassified products containing joint interoperability requirements and the supporting architecture artifacts. The PM/Sponsor may have classified artifacts stored on another site that need to be included in the review process. In this case, the PM/Sponsor must provide full instructions for locating and requesting access to the site and artifacts.

2. DEVELOP AND SUBMIT. The PM/Sponsors of MTA, DBS, and software acquisition pathways will develop pathway documents, containing joint interoperability requirements, consistent with the lead Component and appropriate DoD acquisition policies and processes.

The PM/Sponsors will submit the joint interoperability requirements (in the acquisition products) for the DoD Component level (joint) review following the process outlined in Appendix E.

3. REVIEW AND APPROVE. The review and approval of the joint interoperability requirements in the GTG-F will follow the process as described in Appendix E.

4. ARCHIVE. The process for the archiving requirements document will follow the process as described in Appendix E.