**DEFENSE INFORMATION SYSTEMS AGENCY**
P.O. BOX 549
FORT MEADE, MARYLAND 20755-0549

JITC Instruction 380-50-02* 9 January 2017

# INTEROPERABILITY

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

1. **Purpose.** This instruction prescribes policy and assigns responsibilities for JITC joint interoperability and standards conformance T&E and certification of Department of Defense (DoD) Information Technology (IT), including National Security Systems (NSS) and Defense Business Systems. This instruction does not preclude the need to refer to guidance and direction in applicable DoD interoperability policy documents. This edition of the instruction incorporates policy previously contained in JITC Instruction (JITCI) 210-85-01, "Documentation of Test, Evaluation, and Certification Activities."

2. **Applicability.** This instruction applies to all JITC military and civilian personnel and contractors engaged in performing interoperability and standards conformance T&E and certification efforts on behalf of JITC.

3. **Authority.** This instruction implements DoD policy for joint interoperability of IT, including NSS (primarily DoD Instruction 8330.01).

4. **References.** See reference section.

5. **Definitions.** See glossary of definitions and acronym list sections.

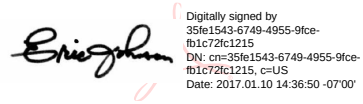
6. **Policy.** All JITC personnel will use and comply with the provisions of this instruction and referenced guidance in performing Joint Interoperability Certification, Standards Conformance Certification, and associated T&E. JITCI 210-85-01 is hereby cancelled; however, the companion "JITC Guide to Test Documentation" remains in effect to specify required content and format of plans and reports, as required by this instruction.

7. **Implementation and Supplementation.** JITC divisions will implement the policy, processes, and procedures covered by this instruction to conduct interoperability and standards conformance T&E and certification. This instruction will not be supplemented without the prior approval of the Chief, Strategy, Plans, and Engineering Division (JT4).

8. **Exceptions.** Submit all requests to waive provisions of this instruction to the Chief, Strategy, Plans, and Engineering Division (JT4). JT4 will forward requests to remove programs/systems from the Commander's Watch List (CWL) to the JITC Commander. JT4 will facilitate requests to waive provisions of DoD interoperability policy with the DoD Chief Information Officer (CIO) in accordance with the JITC Interoperability Process Guide (IPG). All requests need to be coordinated through the respective Division Chief.

9. **Responsibility.** See Chapter 2 for roles and responsibilities.

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




ERIC JOHNSON
CAPTAIN, USN
Commander

SUMMARY OF SIGNIFICANT CHANGES. Changes include a new document structure, planning activities and artifacts required for a joint interoperability certification, updated documentation requirements, and reflect policy changes due to issuance of DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," and related DoD interoperability policy and procedures.

---

* This instruction supersedes JITCI 380-50-02, dated 10 September 2010
OPR: JT4
DIST: All JITC Civilians, Military, and Contractor Personnel

# CONTENTS

**LIST OF FIGURES**

**LIST OF FIGURES (continued)**



**LIST OF TABLES**

# REFERENCES

## Department of Defense (DoD)


- DoD Directive (DoDD) 5000.01, "The Defense Acquisition System," May 12, 2003, certified current as of November 20, 2007.
- DoD Instruction (DoDI) 5000.02, "Operation of the Defense Acquisition System," January 7, 2015
- DoDI 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010
- DoDI 8310.01, "Information Technology Standards in the DoD," February 2, 2015
- DoDI 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
- DoDI 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
- DoDI 8500.01, "Cybersecurity," March 14, 2014
- "DoD Architecture Framework," http://dodcio.defense.gov/Library/DoD-Architecture-Framework/
- Defense Standardization Program (DSP) Acquisition Streamlining and Standardization Information System (ASSIST) database, http://www.dsp.dla.mil/Specs-Standards/
- DoD Information Technology (IT) Portfolio Registry (DITPR), https://ditpr.dod.mil/
- DoD Chief Information Officer (CIO) Interoperability Steering Group (ISG) website, http://jitc.fhu.disa.mil/projects/isgsite/index.aspx


## Chairman of the Joint Chiefs of Staff (CJCS)


- CJCS Instruction (CJCSI) 3170.01I, "Joint Capabilities Integration and Development System (JCIDS)," 23 January 2015
- CJCSI 5123.01G, "Charter of the Joint Requirements Oversight Council (JROC)," 12 February 2015
- Content Guide for the Net-Ready KPP Wiki Page, https://intellipedia.intelink.gov/wiki/Content_Guide_for_the_Net-Ready_KPP [This guide augments the JCIDS Manual (Appendix E to Enclosure D) and replaces the JS NR KPP Wiki Page (formerly referred to as the NR KPP Manual)]
- "Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)" ("JCIDS Manual"), 12 February 2015, including errata as of 18 Dec 2015

**Defense Information Systems Agency (DISA)**

- Global Information Grid Technical Guidance Federation (GTG-F) website, https://gtg.csd.disa.mil/uam/homepage
- Unified Capabilities Requirements (UCR), http://www.disa.mil/Network-Services/UCCO/Policies-and-Procedures
- Unified Capabilities (UC) Approved Products List (APL) Process Guide, http://www.disa.mil/Services/Network-Services/UCCO/

**Joint Interoperability Test Command (JITC)**

- JITC Action Officer's (AO's) Guide, https://disa.deps.mil/org/JT1/JT1A/JITC%20Instruction%20Updates/Forms/AllItems.aspx
- JITC Automated Workflow Service (JAWS), https://jitcnet.fhu.disa.mil/scripts/dr/pageDirectory.asp?FD=M~ytV90eZ9w-XCer9
- JITC Distributed Testing Unified Capabilities Implementation Guide, https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx (T&E pad)
- JITC Electronic Report Distribution (ERD), https://jit.fhu.disa.mil/tools/erd/index.aspx
- JITC Electronic Report Library (ERL), https://jit.fhu.disa.mil/pages/ERL
- JITC Guide to Test Documentation, see JIST T&E pad
- JITC Hotline, http://jitc.fhu.disa.mil/
- JITC Industry Toolkit (JIT), https://jit.fhu.disa.mil
- JITC Information Sharing Tool (JIST), https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx
- JITC Interoperability Process Guide (IPG), Version 2.0, 23 March 2015, http://jitc.fhu.disa.mil/projects/isgsite/pubs.aspx
- JITC Intranet Website, https://jitcnet.fhu.disa.mil
- JITC NR KPP Evaluation Guidebook, see JIST T&E pad
- JITC Public Website, http://jitc.fhu.disa.mil/index.aspx
- JITC System Tracking Program (STP), https://stp.fhu.disa.mil

**Other**

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 9646 standard, http://www.iso.org/iso/home/standards.htm

# GLOSSARY OF DEFINITIONS

This section clarifies several key T&E related terms and phrases as they are used throughout this document; it is not a comprehensive list.

***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.]

***Interoperability.*** The ability of systems, units or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the lifecycle and must be balanced with cybersecurity. [DoDI 8330.01]

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

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

***Joint Interface.*** A "joint" interface is an interface (as defined in DoDAF models for systems and services, such as the Systems Viewpoint (SV)-1, SV-3, and the various service models) between or among systems or services that is considered "joint" per the definition above…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. [IPG - 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 source 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). Coalition partners, non-governmental organizations, etc., that exchange information produced/consumed/shared or distributed by the system under test will result in "joint" exchanges. Information exchanges include all the data products and waveforms used or produced by the system (including sensor platforms). [IPG - derived from multiple sources]

***Joint Interoperability Certification.*** Joint Interoperability Certification (issued only by JITC) involves an evaluation of information interoperability with respect to certified joint interoperability requirements. Interoperability certifications must be updated throughout a system's lifecycle to reflect changes in the system, joint interoperability requirements (capabilities), status, and operational environment. [IPG - derived from multiple sources]

***Joint Interoperability Requirements.*** The subset of interoperability requirements (i.e., NR KPP and architecture viewpoints) that address measures used to evaluate joint interoperability.

***National Security System (NSS).*** Information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which: (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [U.S. Code]

***Service.*** 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]

***System.*** Refers to IT, including NSS and Defense Business Systems, which provide a capability being evaluated for joint interoperability. The term is used interchangeably with System Under Test, Enterprise Service, and a program of record. These terms are commonly used in the T&E community when referring to a set of software, hardware, and processes that collectively provide a capability. [Derived from multiple sources]

**Valid Data.** Refers to data that is sufficient to satisfy the T&E objectives (satisfies data collection requirements, test environment is suitable, provides appropriate level of precision, is statistically significant, etc.). [Derived from multiple sources]

# ACRONYM LIST

| | |
|---|---|
| ACAT | Acquisition Category |
| ANSI | American National Standards Institute |
| AO | Action Officer |
| APL | Approved Products List |
| ASSIST | Acquisition Streamlining and Standardization Information System |
| BCL | Business Capability Lifecycle |
| BEA | Business Enterprise Architecture |
| CAC | Common Access Card |
| CDD | Capability Development Document |
| CIO | Chief Information Officer |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CJCSI | CJCS Instruction |
| CM | Configuration Management |
| COTS | Commercial-Off-The-Shelf |
| CPD | Capability Production Document |
| CRM | Comment Resolution Matrix |
| CWL | Commander's Watch List |
| DBS | Defense Business Systems |
| DCR | DOTmLPF-P Change Recommendation |
| DEPS | DoD Enterprise Portal Service |
| DISA | Defense Information Systems Agency |
| DISR | DoD IT Standards Registry |
| DITPR | DoD Information Technology Portfolio Repository |
| DMAP | Data Management and Analysis Plan |
| DoD | Department of Defense |
| DoDAF | DoD Architecture Framework |
| DoDD | DoD Directive |
| DoDI | DoD Instruction |
| DoDIN | DoD Information Network |
| DOT&E | Director, Operational Test and Evaluation |
| DOTmLPF-P | Doctrine, Organization, Training, materiel, Leadership and education, Personnel, and Facilities – Policy |
| DSP | Defense Standardization Program |
| DT | Developmental Testing |
| DT&E | Developmental Test and Evaluation |
| EA | Executive Agent |
| EISP | Enhanced Information Support Plan |
| ERD | Electronic Report Distribution |
| ERL | Electronic Report Library |
| ETSI | European Telecommunications Standards Institute |

| | |
|---|---|
| FCB | Functional Capabilities Board |
| FOUO | For Official Use Only |
| GAO | Government Accountability Office |
| GIG | Global Information Grid |
| GTG-F | Global Information Grid Technical Guidance Federation |
| GTP | GIG Technical Profiles |
| IAM | Interoperability and Supportability Assessment Module |
| IATM | Integrated Architecture Traceability Matrix |
| ICD | Initial Capabilities Document |
| ICTO | Interim Certificate to Operate |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IOP | Interoperability |
| IPG | Interoperability Process Guide |
| IPR | In-Progress Review |
| IS-CDD | Information System Capability Development Document |
| IS-ICD | Information System Initial Capabilities Document |
| ISEC-TIC | Information Systems Engineering Command – Technical Integration Center (Army) |
| ISG | Interoperability Steering Group |
| ISO | International Organization for Standardization |
| ISP | Information Support Plan |
| IT | Information Technology |
| ITP | Interoperability Test Plan |
| ITSC | Information Technology Standards Committee (replaced by JESC) |
| ITU | International Telecommunication Union |
| J-RAD | JITC Risk Assessment Database |
| JAWS | JITC Automated Workflow Service |
| JCA | Joint Capability Area |
| JCIDS | Joint Capabilities Integration and Development System |
| JDMT | JITC Data Management Tool |
| JESC | Joint Enterprise Standards Committee (formerly ITSC) |
| JIC | Joint Interoperability Certification |
| JIE | Joint Information Environment |
| JIEP | Joint Interoperability Evaluation Plan |
| JIST | JITC Information Sharing Tool |
| JIT | JITC Industry Toolkit |
| JITC | Joint Interoperability Test Command |
| JITCI | JITC Instruction |
| JROC | Joint Requirements Oversight Council |

| | |
|---|---|
| JSD | Joint Staffing Designator |
| JSR | JITC Standards Research (Team) |
| KM/DS | Knowledge Management/Decision Support |
| MDA | Milestone Decision Authority |
| MIL-STD | Military Standard |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MRTFB | Major Range and Test Facility Base |
| NATO | North Atlantic Treaty Organization |
| NIEM | National Information Exchange Model |
| NIPRNet | Nonsecure Internet Protocol Router Network |
| NIST | National Institute of Standards and Technology |
| NR KPP | Net-Ready Key Performance Parameter |
| NSS | National Security Systems |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OMG | Object Management Group |
| OOC | Out-Of-Cycle |
| OT | Operational Testing |
| OTA | Operational Test Agency |
| OT&E | Operational Test and Evaluation |
| OTRR | Operational Test Readiness Review |
| OV | Operational Viewpoint |
| PIIT | Platform Integration Information Table |
| PMO | Program Management Office |
| PM-P | Program Management Portal |
| POA&M | Plan of Actions and Milestones |
| POC | Point of Contact |
| RM | Records Management |
| RTO | Responsible Test Organization |
| SCG | Security Classification Guide |
| SIPRNet | SECRET Internet Protocol Router Network |
| SPAWAR | Space and Naval Warfare Systems Command (Navy) |
| STANAG | Standardization Agreement (NATO) |
| StdV | Standards Viewpoint |
| STP | System Tracking Program |
| SV | Systems Viewpoint |
| T&E | Test and Evaluation |
| TCR | Test Concept Review |

| | |
|---|---|
| TRR | Test Readiness Review |
| TSP | Test Support Package |
| UC | Unified Capabilities |
| UCCO | Unified Capabilities Certification Office |
| UCR | Unified Capabilities Requirements |
| UJTL | Universal Joint Task List |
| U.S. | United States |
| USD(AT&L) | Under Secretary of Defense (Acquisition, Technology, and Logistics) |
| W3C | World Wide Web Consortium |

# C1. CHAPTER 1. JOINT INTEROPERABILITY OVERVIEW

C1.1 **Overview.** The Joint Interoperability Test Command (JITC) is the Department of Defense's (DoD's) only joint interoperability certifier and only non-Service Operational Test Agency (OTA) for Information Technology (IT)/National Security Systems (NSS). Test and Evaluation (T&E) is essential to reduce the risks faced by warfighters in the field. JITC provides risk-based T&E and certification services, tools, and environments to ensure joint warfighting capabilities are interoperable and support mission needs. In addition, JITC serves as the OTA for other DoD agencies such as Defense Logistics Agency, Defense Finance and Accounting Service, and Defense Commissary Agency as well as providing Developmental Testing for Defense Information System Agency (DISA)-managed programs.

C1.2 **Policy Guidance.** Figure 1-1 depicts policy and instructions applicable to the Joint Interoperability Certification (JIC) process. This includes DoD Instruction (DoDI) 8330.01 and its companion document, the JITC Interoperability Process Guide (IPG). JITC publishes the IPG and coordinates with the T&E community to update or modify guidance contained in the DoD instruction. The Program Management Office (PMO)/Sponsor is the principal audience for the IPG. The JITC workforce is the principal audience for JITC Instruction (JITCI) 380-50-02, which focuses on specific JITC staff responsibilities.

C1.3 **Document Design**. This instruction focuses on policy; the "how to" or guidance information is provided in applicable supplemental guides of the Net-Ready Key Performance Parameter (NR KPP) Evaluation Guidebook. Several chapters have overlapping topics. The goal is to provide the reader with enough background to understand the policy guidance presented in a particular chapter. Some repetition is unavoidable to describe a topic in proper context and to present relationships with policies in other chapters. This instruction also includes a list of important reference materials for the Action Officer (AO) and test team personnel, including major test and certifications policy-related and associated operating procedures documentation relevant to JITC management and test personnel. Chapter 1 is an overview of joint interoperability and Chapter 2 prescribes Roles and Responsibilities. Chapters 3 through 6 address the four (4) phases of JITC's joint interoperability T&E and certification process: Requirements Generation, Planning, Test and Evaluation, and Reporting. Specific tools used during each phase of the process are discussed in the applicable chapters. The remaining chapters describe related activities and processes.

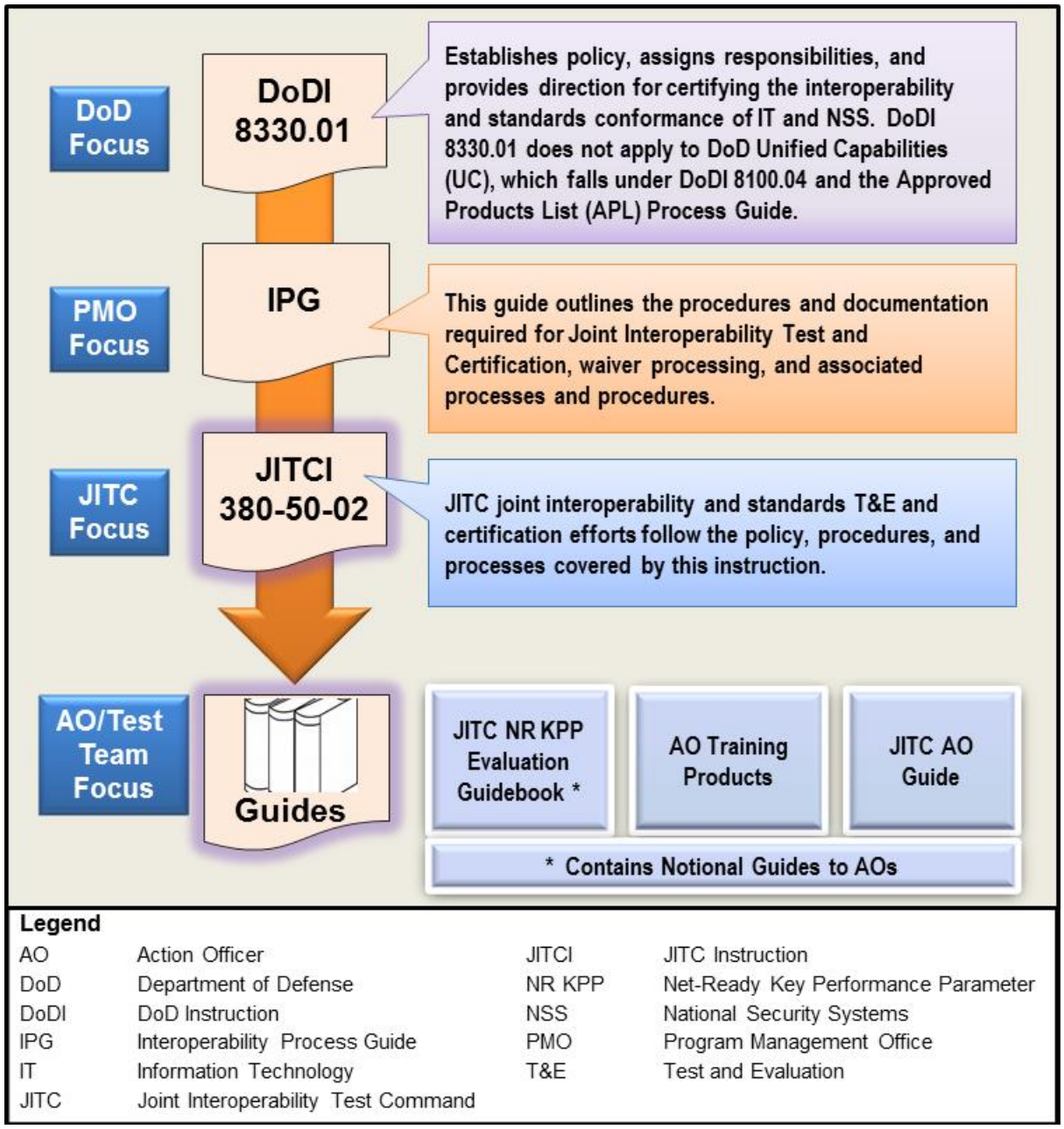



**Figure 1-1. Joint Interoperability T&E and Certification Policy, Processes, and Guidance**

# C2. CHAPTER 2. ROLES AND RESPONSIBILITIES

C2.1 **Overview.** This chapter addresses the primary responsibilities performed by the JITC staff from the Commander to Division and Branch Chiefs to the assigned AOs who form the nucleus of the JITC test teams. Figure 2-1 identifies the key JITC personnel responsible for the activities addressed in this instruction.

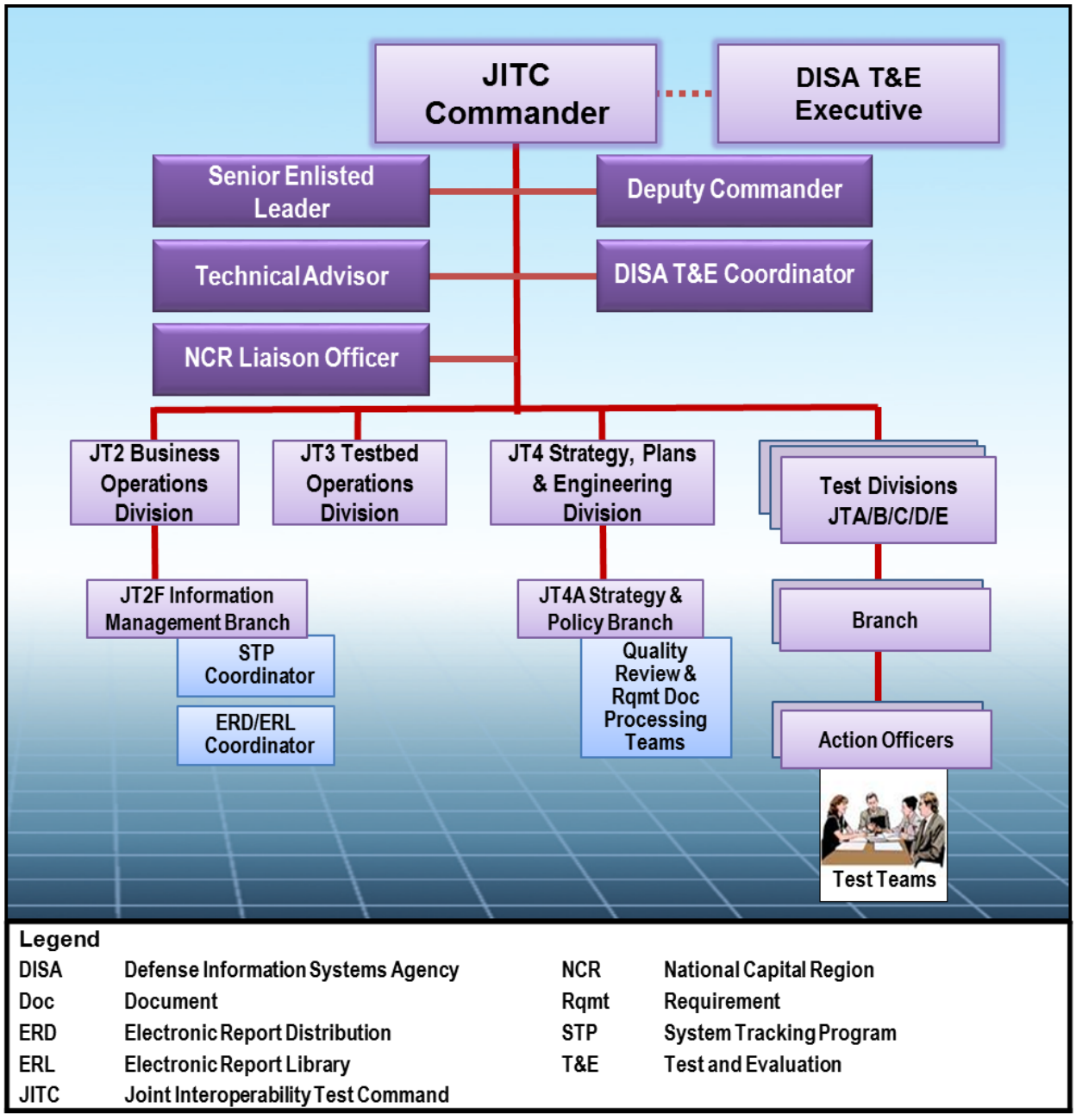



**Figure 2-1. Key JITC Elements with Test & Evaluation, Certification, and Interoperability Functions**

C2.2 **Command Responsibilities:**

C2.2.1 **JITC Commander** will:

- Provide command oversight and direction for all JITC joint test, evaluation, and certification missions.
- Monitor JITC Commander's Watch List (CWL) and approve systems for inclusion or removal.
- Serve as signature authority for all non-certification products (Denial of Joint Interoperability Certification, Standards Conformance Non-Certification, etc.).
- Fulfill the role of the Defense Information Systems Agency (DISA) T&E Executive.

C2.2.2 **JITC Deputy Commander** will fulfill test, evaluation, and certification responsibilities, outlined in this instruction, in the absence or under the authority of the Commander.

C2.2.3 **JITC Technical Advisor** will:

- Review and approve all JITC CWL system test plans, reports, and certification products.
- Facilitate resolution of interoperability-related issues between external organizations and JITC when elevated above the Chief, Strategy, Plans, and Engineering Division (JT4).
- Facilitate resolution and recommend decisions related to the roles of lead/supporting division.

C2.2.4 **National Capital Region Liaison Officer (JT)** will:

- Function as the primary point of contact (POC) representing the command's interests with the Interoperability Steering Group (ISG).
- Maintain current DoD Chief Information Officer (CIO) ISG Website. This site contains ISG related material, e.g., JITC Interoperability Process Guide (IPG), ISG POC list, Waiver to Policy and Interim Certificate to Operate (ICTO) forms and procedures, and access to ISG tools.

C2.2.5 **DISA T&E Coordinator** will:

- Assist the T&E Executive and assist in the oversight of the JITC.
- Provide technical direction and oversight to the T&E offices and DISA.

C2.2.6 **JITC Senior Staff** team comprises select members of the command staff (Test Division Chiefs, Technical Advisor, and JT4 Division Chief). This team will:

- Participate in selecting the subjects and issues, as needed for interoperability policy actions, for such venues as ISG meetings.
- Review and guide JITC test, evaluation, and certification to ensure long-range plans adequately address JITC's evolving DoD interoperability mission.
- Assist JITC staff in resolving test, evaluation, certification, and interoperability issues within JITC.

C2.2.7 **JITC Test Division Chiefs** will:

- Provide system-specific test support in coordination with support Divisions/Branches and assume responsibility for general support of designated functional/mission areas.
- Maintain oversight of all assigned system test activities. This includes requirements review, PMO/Sponsor coordination, planning, budgeting, and execution, as well as reporting, certification, data archiving, and training.
- Plan and budget for testing resources, including tools and necessary infrastructure.
- Establish, in coordination with Chief, Strategy, Plans, and Engineering Division (JT4), guidelines and common practices involving metrics, methods, plans, or reports specific to assigned functional or mission areas.
- Establish a working relationship with designated functional/mission area domain leads. Examples include the Functional Capabilities Boards (FCBs) and Joint Capability Areas (JCAs) to address requirements and capabilities, resources, and status reporting.
- Assist in the development, review, and promulgation of JITC test, evaluation, and certification policy, procedures, and test methodologies as well as resolving related issues within JITC.
- Develop and retain subject matter expertise on functional and operational concepts, joint integrated architectures, and federated or domain metrics.
- Ensure AOs receive training and comply with DoD and JITC interoperability policy and procedures – produce consistent products, enter and maintain required System Tracking Program (STP) and Electronic Report Distribution (ERD) information, and acquire necessary technical expertise.
- Ensure all assigned personnel are responsive to interoperability status inquiries, document review requests, interoperability status reporting requirements, ICTO and Waiver to Policy review requests, and generation of related products. Ensure assigned personnel supporting these tasks coordinate with other Divisions and AOs on a timely basis, as needed.
- Maintain awareness of the interoperability status of systems and capabilities in assigned functional or mission areas.
- Ensure the implications and impacts of test, evaluation, and certification information are correct and clear to warfighters and decision-makers.

- Ensure DoD and JITC policies and guidance are correctly reflected in test, evaluation, and certification information.
- Ensure review of test plans, reports, and certification products through the division and command review process, as appropriate, and distribution to the customer through the ERD tool.
- Ensure JITC documents follow the current content and format guidance, such as specified in the JITC Guide to Test Documentation and JITC NR KPP Evaluation Guidebook.
- Ensure all test, evaluation, and certification documents are technically correct and adequate, fulfill customer needs, and meet JITC documentation standards.
- Exercise signature authority on all designated function or mission products and be accountable for the quality of these products.
- Ensure timely delivery of JITC's formal products to the customers after proper review, approval, and release authorization. Be accountable for the quality of these products.
- Direct assignment of a Lead AO to manage test support activities, as required.
- Assign representatives to perform requirements document review duties (described in Chapter 3), as appropriate, and administer requirements document review and comment adjudication.
- When performing the role of a lead division, perform these additional functions:
  - Coordinate with other divisions on programs/systems that cross functional/mission areas.
  - Act as the primary JITC POC for external coordination when necessary to back up the Lead AO.
- When performing the role of a supporting division, perform these additional functions:
  - Provide requested resources (test material, test support, etc.) to lead division in sufficient time to support their particular mission.
  - Provide timely, detailed, and clear document comments and feedback to lead division when requested.

C2.2.8 **JITC Branch Chiefs** will:

- Ensure test, evaluation, and certification information is technically adequate and accurate – interoperability and standards conformance status is determined and reported properly, and that test methodologies and status reporting complies with DoD and JITC interoperability policy and procedures.
- Assist in the development, review, and promulgation of JITC test, evaluation, and certification policy, procedures, and test methodologies.

- Assist Division Chiefs in ensuring AOs receive training and comply with DoD and JITC interoperability policy and procedures.
- Ensure that AOs enter and maintain required information in STP, ERD, and data repositories.
- Ensure review of test plans, reports, and certification products through the Division and Command review process.
- Assist Division Chiefs in ensuring JITC document quality and consistency by following current content and format guidance.
- Assist Division Chiefs in ensuring timely delivery of JITC's formal products to the customers after proper review, approval, and release authorization.
- Assist Division Chiefs in planning and budgeting for testing resources, including tools and necessary infrastructure.
- Assist in resolving test, evaluation, certification, and interoperability issues within JITC.
- Assist Division Chiefs in ensuring all assigned personnel are responsive to interoperability status inquiries, document review requests, interoperability status reporting requirements, ICTO and Waiver to Policy review requests, and generation of related products. Ensure assigned personnel supporting these various tasks coordinate with other Divisions and AOs on a timely basis, as needed.

C2.3 **JITC Action Officers.** AOs can have widely varying roles and responsibilities depending on the nature of their assigned test program(s). Because of this, AOs are expected to coordinate with their Branch Chiefs to determine which of the items below are suitable for their particular situation.

C2.3.1 **Basic Knowledge Requirements.** AOs must have a working knowledge of fundamental test, evaluation, and certification policy guidance, as well as be cognizant of the following, as appropriate for their assignments:

- JITC IPG.
- DoD interoperability policies.
- DoD Architecture Framework (DoDAF), which defines Architecture Viewpoints that are essential to NR KPP interoperability certification.
- Requirements Review Processes, e.g., the Global Information Grid Technical Guidance Federation (GTG-F) Interoperability and Supportability Assessment Module (IAM) which provides an automated process for staffing, providing comments, and adjudicating the Information Support Plan (ISP). (See Chapter 3.)
- JCAs, Universal Joint Task Lists (UJTLs), UJTL to JCA linkage, etc.
- Joint Capabilities Integration and Development System (JCIDS) Manual. Also see Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 (JCIDS) and

CJCSI 5123.01 (Joint Requirements Oversight Council (JROC) Charter), which further detail the NR KPP process.

- Unified Capabilities (UC). DoDI 8100.04, UC Approved Products List (APL) Process Guide, Unified Capabilities Requirements (UCR), and JITC Distributed Testing UC Implementation Guide. (See Chapter 8.)

- JITC Action Officer's Guide.

C2.3.2 **Specific Roles and Responsibilities.** The AO's primary role is to understand the program, system, or system components sufficiently to provide the PMO/Sponsor a technically sound interoperability evaluation. Additionally, the AO should support the PMO/Sponsor in navigating the process by providing information and direction on interoperability policies and procedures. Detailed duties encompass the following activities:

- Review system capability/requirements documents. Ensure the sufficiency and testability of measures in the NR KPP, associated architecture viewpoints, and other interoperability requirements (i.e., traceable, measurable requirements).
- If attempts to resolve a critical requirements-related issue with the PMO/Sponsor have been unsuccessful, coordinate with the Strategy and Policy Branch (JT4A) for assistance in coordinating among the various parties.
- Prepare and execute an appropriate test planning document such as an Interoperability Test Plan (ITP) or provide input to other test planning documents, as appropriate.
- Ensure the PMO/Sponsor understands that JITC will perform an interoperability evaluation based on Joint Staff-certified NR KPP and approved architecture viewpoints. Evaluation results are used to determine the appropriate interoperability (IOP) T&E product (JIC, Joint Interoperability Assessment, etc.).
- Prepare and staff plans and reports, including status reports, assessments, certifications, and related correspondence, in accordance with this instruction, the JITC Guide to Test Documentation, and other guidance referenced in this instruction.
- Create/update STP entries and maintain ERD recipient distribution lists.
- Ensure all JITC formal products go through the designated review process (see Chapter 6) and use the ERD for softcopy distribution. Any product that warrants special handling, e.g., a classified or For Official Use Only document requires insertion of a "placeholder" file for ERD processing.
- Support ICTO reviews and Waiver to Policy requests, coordinating with other Divisions and AOs.
- Adhere to approved JITC policies and procedures, in coordination with the Lead AO, when establishing a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) with the PMO/Sponsor.
- Be accountable for the quality of all final products. Ensure that all products are carefully screened and properly marked for classification or special handling and processed in accordance with policy.

- Be prepared to assume the responsibilities of Lead or Support AO.

C2.3.3 **Lead Action Officer.** The Lead AO has oversight for all test-related activities for a particular program/system to include the following actions:

- Serve as the single JITC POC to coordinate all issues involving requirements, testing, evaluation, certification, and funding. This includes responsibility for developing any Plans of Actions and Milestones (POA&Ms) and MOAs/MOUs in coordination with the PMO/Sponsor. The Lead AO confirms that necessary test methodologies, test tools and associated procedures, and support systems are available or developed.
- Coordinate early with the Business Operations Branch on any work involving foreign customers to address matters concerning funding, material transfer, etc.
- Ensure validation of test tools and procedures pertaining to interoperability and standards conformance testing, including those developed by other organizations.
- Conduct periodic In-Progress Reviews (IPRs) to brief JITC management and the PMO/Sponsor on the status of the program/system under test.
- In coordination with the customer and JT4A, determine the appropriate test, evaluation, and certification documentation required.
- Prepare documentation following this instruction and referenced guidance and resolve specific questions with JT4A.
- Coordinate documents through division and JT4A reviews, as appropriate, and obtain approval from the Division Chief before publication and distribution.
- Ensure the program's overall JITC T&E and certification strategy is technically sound and thoroughly evaluates the system's capabilities and requirements.
- In support of an Operational Test Readiness Review (OTRR) or Milestone C decision, the Lead AO will coordinate with appropriate division management to produce a consolidated JITC recommendation.
- Ensure test data used to support evaluations are archived in designated central storage areas.
- As part of the reporting process, assess the expected operational impact of any discrepancies or unmet critical test requirements.
- Be accountable for security matters and product quality.

C2.3.4 **Support Action Officer.** The Support AO is responsible to the Lead AO in performance of the following tasks:

- Coordinate all funding and scheduling matters involving test, evaluation, and certification efforts with the Lead AO.
- Provide technical support and expertise to the Lead AO on document review and test planning, execution, analysis, and reporting.

C2.4 **Supporting JITC Elements.** The paragraphs below list the responsibilities of the command elements involved in developing and managing JITC interoperability policy and procedures.

C2.4.1 **Business Operations Division (JT2).** Division duties cover a wide range of test support activities including:

- Operate a 24/7 hotline to provide JITC test experience and resources to resolve real-time interoperability issues. Coordinate hotline requests with the appropriate Division for resolution.
- Coordinate JITC/Combatant Command support activities with the applicable DISA field offices and DISA desk officers.
- Develop and maintain system interoperability exercise planning and reporting instructions.
- Perform initial processing of JIC recertification request forms.
- Maintain JITC public website. This site contains JITC testing, DoD policy references, contact information, etc. It also includes Hotline Support forms for initial contact with customers needing assistance.

C2.4.2 **Chief, Information Management Branch (JT2F).** This branch is responsible for development and management of the STP, ERD, JITC Automated Workflow Service (JAWS), JITC Data Management Tool (JDMT), JITC Information Sharing Tool (JIST), and JITC Industry Toolkit (JIT); JIT includes the Electronic Report Library (ERL) and other related tools. Specific duties include the following tasks:

- Review and approve access requests.
- Assist users in STP, ERD, JAWS, JDMT, JIST, and JIT operation.
- Approve and oversee system modifications and updates.
- Manage the STP:
  - Respond to data calls to support other JITC Divisions, the Commander, historical reporting requirements, performance metrics, etc., that require special STP reports/queries.
  - Provide periodic STP statistical summaries to JITC Senior Staff.
  - Develop STP training material and provide training to the workforce.
  - Develop and maintain the STP Users' Manual.
- Manage the ERD process, to include:
  - Develop and maintain the ERD and associated tools.
  - Assist users in ERD operation.
  - Provide ERD training to the workforce.

- Facilitate use of the JIT. Specific actions involve developing and maintaining the JIT online site and maintaining the JIT server, assisting users in JIT operation, and providing JIT training to the workforce.
- Facilitate use of JAWS, JDMT, and JIST.

C2.4.3 **Test Operations Division (JT3).** Division duties cover a wide range of test support activities which will:

- Provide space, facilities, network, and security services in hosting DISA, DoD, government, and vendor development, integration, and test activities.
- Provide JITC with a consolidated cybersecurity support team.

C2.4.4 **Chief, Strategy, Plans, and Engineering Division (JT4)** will:

- Coordinate with the JITC Senior Staff to establish and promulgate JITC test, evaluation, and certification policy, procedures, and processes.
- Represent JITC to resolve interoperability-related issues between external organizations and JITC when elevated above the Chief, Strategy and Policy Branch.
- Oversee all JITC T&E and certification policy development, associated publications, and related training programs, to include the JITC IPG, as per DoDI 8330.01. This includes review and approval of deviations from policy or established best practices within functional/mission area testing methodologies developed by the Divisions and Branches and JITC input to DoD interoperability-related directives, instructions, policy, and procedures.
- In coordination with JITC Command staff, respond to data calls relating to general interoperability and certification-related issues in support of the Government Accountability Office (GAO), the DoD CIO and ISG, Joint Staff, Inspector General, and DISA.
- Oversee the execution of JITC Executive Agent duties (see Chapter 3).

C2.4.5 **Chief, Strategy and Policy Branch (JT4A).** As directed by the Chief, Strategy, Plans and Engineering Division, the JT4A Branch Chief will:

- Implement a JITC quality control program to establish quality standards, templates and enforce best practices across the command to ensure consistency and clarity of test plans, test reports, requirements reviews, and certification products.
- Develop and maintain policies and procedures for JITC certification and related processes.
- Maintain current interoperability T&E and certification information at the following locations:
  - JIST – T&E Pad. JIST T&E pad serves as the policy share site that contains training briefings; DoD interoperability policy and architecture information;

document review material; example JITC test, evaluation, and certification products; etc.

- JITC JT4A SharePoint Website. This site contains notices on interoperability testing, DoD policy references, and current JITC certification statistics.
- JITC NR KPP Helpdesk. This site supports the Helpdesk function.

- Manage the administrative ERD processes associated with JITC test and certification documents.
  - Process and disseminate test and certification documents through the ERD.
  - Ensure all distributed products and related metadata, are entered into STP. This includes interoperability administrative details and related status information.
  - Ensure ERD Interoperability Certification Letter Core (distribution) List and (Standards) Conformance Certification Letter Core (distribution) List are current and updated, as needed.
- Manage formal document reviews. Staff documents and coordinate JITC comments to the GTG-F IAM or the Knowledge Management/Decision Support (KM/DS) tool, as applicable, in coordination with the respective Lead Division and AO. Designate an Executive Agent, Lead Assessor or Assessor POC, and alternates to be responsible for the following:
  - Identify the Division responsible to review documents.
  - Provide technical assistance and coordinate publication using GTG-F IAM or KM/DS, as applicable.
- Process and disseminate Waiver to Policy recommendations.

# C3. CHAPTER 3. REQUIREMENTS GENERATION

C3.1 **Overview.** This chapter provides policy and guidance for reviewing requirements documents for JIC. Certification is based upon meeting requirements set forth by the Joint Staff-certified NR KPP and approved architecture viewpoints or alternate approved forms of requirements (e.g., for platform and business systems) as established in the IPG.

C3.2 **Net-Ready Key Performance Parameter.** The NR KPP attributes are the foundation for an interoperability evaluation. The three attributes, as shown in Figure 3-1, specify the joint mission(s), operational tasks (mission activities) supported by the systems; the networks (transport); and the supporting information exchanges; all with applicable measures critical to assessing interoperability. The primary DoD policy and guidance for the NR KPP are the CJCSI 3170.01 series, the companion JCIDS Manual, and the Content Guide for the NR KPP website (formerly Joint Staff NR KPP Manual) located at https://intellipedia.intelink.gov/wiki/Content_Guide_for_the_Net-Ready_KPP.

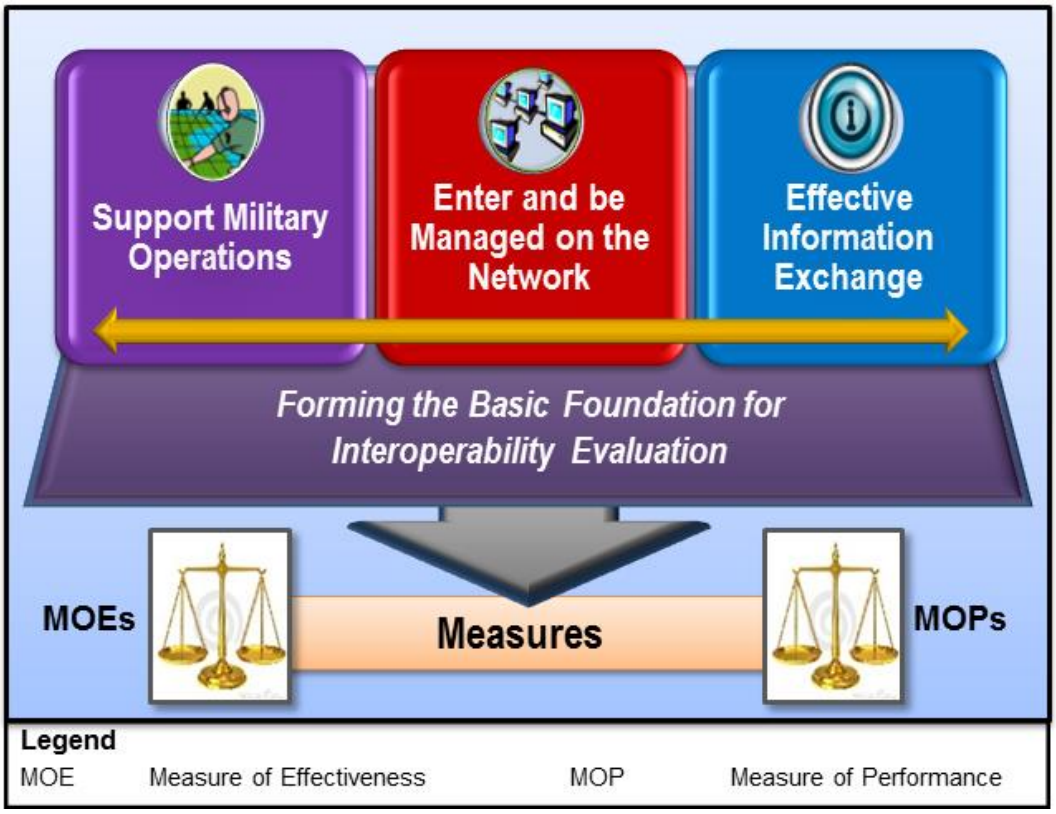



**Figure 3-1. NR KPP's Three Attributes**

Testable and traceable measures, to include appropriate conditions and criteria, are derived from applicable architecture viewpoints and used to evaluate compliance with the NR KPP attributes. JT4A developed the JITC NR KPP Evaluation Guidebook, Requirements Document Review Process, to help the AO conduct the formal IOP requirements review and extract test requirements from the Joint Staff-certified NR KPP and approved architecture viewpoints. Use of

a requirement traceability matrix, such as the Integrated Architecture Traceability Matrix (IATM) described in the evaluation guidebook, during document review is strongly recommended.

C3.3 **Information Support Plan.** The ISP documents a program's information infrastructure support and information interface requirements, to include the Joint Staff-certified NR KPP and architecture viewpoints, which are required for a JIC. DoDI 8330.01, "Interoperability of Information Technology (IT), including National Security Systems (NSS)," and DoDI 5000.02, "Operation of the Defense Acquisition System," require systems have an ISP so it is a good source for IOP requirements; however, the final, complete ISP is not required for a JIC.

The PMO/Sponsor develops the ISP using the GTG-F. The GTG-F comprises the following and is available at https://gtg.csd.disa.mil/iam/home.html:

- Program Management Portal (PM-P): Provides PMOs/Sponsors with the means to manage ISP, NR KPP, and architecture information during document development, assessment, comment adjudication, and approval.
- Global Information Grid (GIG) Technical Profiles (GTP) provides a simple wizard to create a Standards Viewpoint (StdV).
- DoD IT Standards Registry (DISR): Used to build StdV-1, StdV-2, and GTP lists.
- Enhanced Information Support Plan (EISP): The EISP submission wizard compiles program information into an ISP and GTP data for assessment.
- IAM: Provides management and workflow capabilities for the assessment of ISPs, NR KPPs, and architectural viewpoints.

The PMO/Sponsor submits the document to the Component Executive Agent (EA) for a component-level review. After the component review is completed, the Component EA submits the document to the appropriate organizations for a joint assessment.

Reviews conducted in the IAM follow a role-based policy for ISP reviews. The roles applicable to JITC's review process are:

- DoD Component EA: Staffs the ISP, reviews and submits comments, staffs to other Components, approves the ISP (or delegates this authority), and provides a certification/approval memorandum.
- JITC EA: The JITC EA manages IAM document assessment. This role is executed by JT4A.
- Lead Assessor: The Lead Assessors assign Assessors to review documents, approve Assessors' comments, and make recommendations. The JITC Lead Assessors are the Branch Chiefs of the test divisions.
- Assessor: The JITC Assessors are the AOs who review and assess the ISP, NR KPP, and the architecture viewpoints for testability, traceability, and completeness.

Figure 3-2 provides an overview of the ISP development and review process. The interoperability requirements are the combination of the NR KPP table and associated architecture information. The technical detail portion of an ISP, if available, may also be useful for planning.

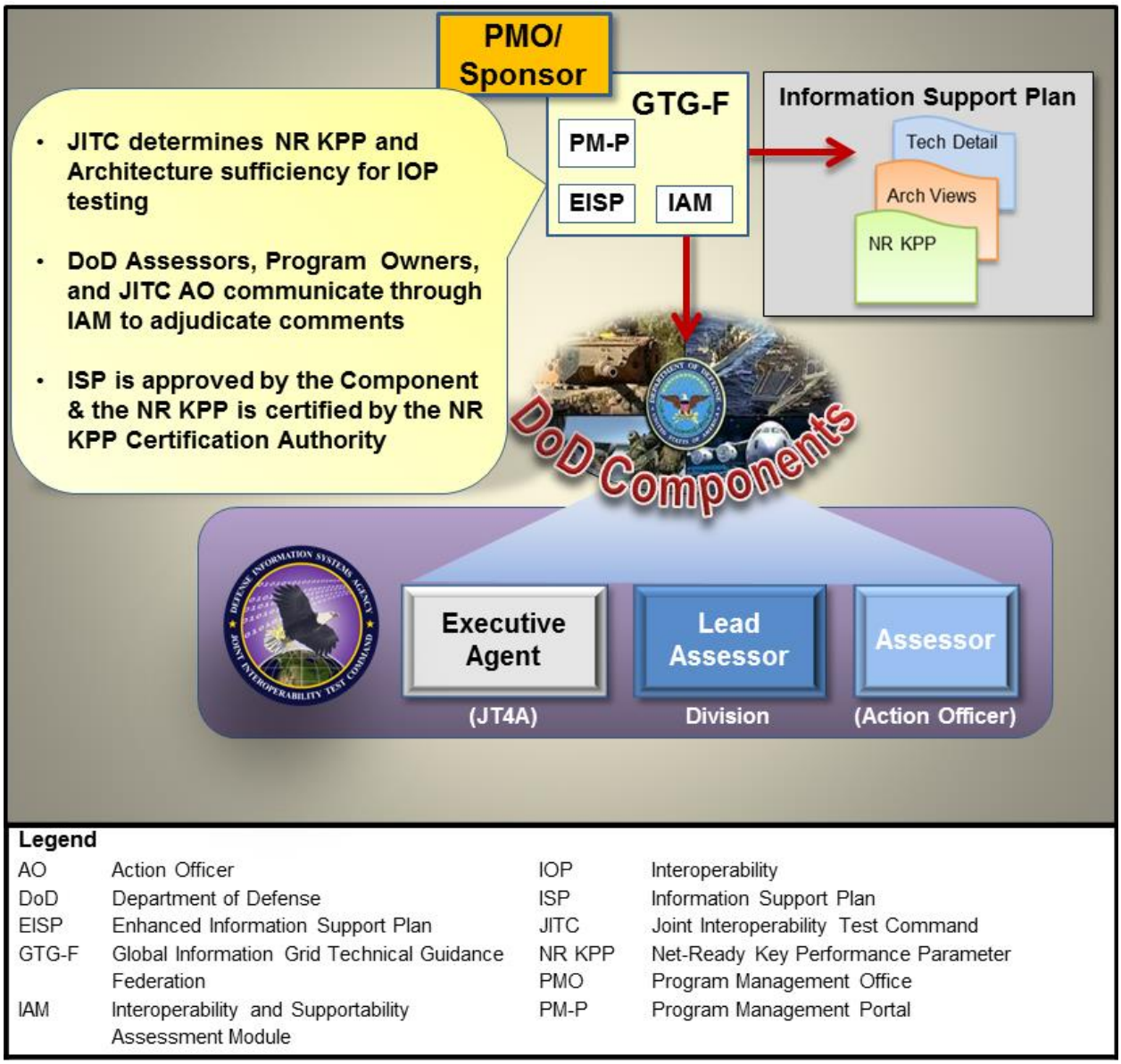



**Figure 3-2. ISP Review Process Using GTG-F IAM**

C3.4 **JCIDS Documents.** The JCIDS process provides the baseline for documentation, review, and validation of capability requirements at all classification levels across DoD. The authoritative source for JCIDS information is CJCSI 3170.01, "Joint Capabilities Integration and Development System (JCIDS)," and the "Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)."

The JCIDS documents that JITC regularly assesses include:

- Initial Capabilities Documents (ICDs) and Information System Initial Capabilities Documents (IS-ICDs). An ICD provides initial documentation of capability gaps.
- Capability Development Documents (CDDs) and Information Systems Capability Development Documents (IS-CDDs). A CDD specifies capability requirements in terms of developmental performance attributes.
- Capability Production Documents (CPDs). A CPD specifies capability requirements in terms of production performance parameters.

JITC sometimes assesses Joint Doctrine, Organization, Training, materiel, Leadership and education, Personnel, and Facilities – Policy (DOTmLPF-P) Change Recommendations (DCRs) that recommend partially or wholly mitigating one or more identified capability requirements and associated capability gaps with non-materiel capability solutions.

The PMO/Sponsor develops the JCIDS documents in accordance with instructions in the JCIDS Manual and submits the document to the Joint Staff Gatekeeper through the KM/DS system. The Joint Staff Gatekeeper identifies the lead and supporting FCBs, assigns the Joint Staffing Designator (JSD), and determines the Certification/Endorsement Authority. The Joint Staff Gatekeeper then initiates the assessment. Both the CDD and CPD contain the NR KPP and associated architecture viewpoints that can form the basis of an interoperability evaluation.

C3.5 **Review Rules.** Observe the following rules for a comprehensive requirements review:

- Treat each review as the only opportunity to improve the requirements.
- Use the requirements review checklists focusing on requirements testability, traceability, and completeness based on the joint interoperability evaluation framework.
- Assess traceability of requirements in the NR KPP and associated architecture viewpoints. A requirements traceability matrix (e.g., IATM) is useful for this assessment.
- Administrative comments should not be included unless necessary to understand the requirements.
- Every comment must be complete, unambiguous, and specific.
- Every comment must describe exactly what the problem is, how to correct it, and why the correction is needed.
- Recommendation must agree with the comment(s).
- Coordinate with the PMO/Sponsor when making critical comments, in addition, coordinate with Joint Staff J-6 before making critical comments on the NR KPP.
- The PMO/Sponsor is required to adjudicate critical comments.

- Comments posted after the suspense date may not be considered by the program.
- Refer to the NR KPP Evaluation Guidebook for checklists and IATM guidance.

C3.6 **Requirements Document Review.** The review process is similar for both IAM and KM/DS; the commonalities and differences are listed below. The AO is responsible for following the specific instructions provided in the requirements review tasking email. JT4A maintains a Requirements Review checklist (see the JITC NR KPP Evaluation Guidebook) and reviews requirements documents on select programs ("Requirements Head Start Review," see C4.6.1) to assist the AO with the formal interoperability requirements review and to extract test requirements from the Joint Staff-certified NR KPP and approved architecture viewpoints.

### C3.6.1 IAM and KM/DS Review Process Commonalities

- The Doc Review team (JT4A) receives a tasking email.
- The Doc Review team sends an email to the lead and support divisions and cc's the other divisions.
- The Division or Branch Chief assigns the assessment to an AO who will serve as an IAM assessor or KM/DS reviewer. Branch Chiefs will provide the AO's contact information to the Doc Review team as soon as possible.
- The AO reviews, comments, and determines the recommendation for the document.
- JT4A may review and provide AO with inputs to assist with his/her review.
- The Branch Chief reviews and approves.
- The Division Chief reviews and approves, as appropriate; for example, when there are critical issues.
- JT4A reviews as the EA (checks consistency and criticality of comments).
- If the test division does not provide the Doc Review team or submit to GTG-F any comments by the suspense date, then the Doc Review team will post "Concur with No comments."

### C3.6.2 Specific to IAM Review Process

- Assessors and Lead Assessors require an IAM account.
- The IAM sends tasking email to all Assessors (ignore these emails). AOs will receive an email from their respective Division Chief, Branch Chief, or the Doc Review team when they are the designated assessor.
- The AO must enter the comments into the IAM in the proper section, and obtain approval from the Lead Assessor. Guidance on using the comment and adjudication functions in the IAM is located at https://gtg.csd.disa.mil/uam/support/userDocument/list. Input only UNCLASSIFIED comments to IAM.

- For any JITC critical comments, even those generated by multiple substantive comments, the comments must be discussed with the original author (document sponsor) and documented (name, phone number, and date contacted). For final reviews, any JITC comments or non-concurs must be discussed with the original author.
- Assessors should review previous comments to ensure their current submissions are consistent with earlier JITC and other organization's comments.
- IAM will generate notifications when PMO/Sponsor adjudicates comments; JITC must accept or reject proposed adjudications.
- Assessors will update the STP as needed in order to keep the entry up-to-date to support accurate metrics and reporting.
- The Component EA may send out a document for multiple assessments to try to gain complete concurrence.

### C3.6.3 **Specific to KM/DS Review Process**

- Reviewers require a KM/DS and SECRET Internet Protocol Router Network (SIPRNet) account (KM/DS resides on SIPRNet).
- Appropriate security measures for the SIPRNet must be followed.
- The JITC Doc Review team will download the document to be assessed and any supporting documentation into a shared folder that is identified in the tasking email. (Note: Remote users will have different procedures because of access restrictions.)
- All comments must be entered into the provided comment resolution matrix (CRM) in the KM/DS. A different or modified CRM will not upload into the KM/DS and the comments will have to be entered manually.
- Action officers should review previous comments to ensure their current submissions are consistent with earlier JITC and other organization's comments. To non-concur because of multiple substantive comments, include a critical comment that says so. KM/DS automatically sets the "concur with comments/non-concur" field based on the highest criticality comment received. Any classified comments must include derived-from and downgrading statements.
- For any JITC critical comments, even those generated by multiple substantive comments, the comments must be discussed with the original author (document sponsor) and documented (name, phone number, and date contacted). For Final/FCB Draft reviews, any JITC comments or non-concurs must be discussed with the original author.
- Reviewers will update the STP as needed in order to keep the entry up-to-date to support accurate metrics and reporting.

- Send comments via SIPRNet email to the individuals indicated in the tasking email, providing:
  - Recommendation (Concur, Concur w/Comments, Non-Concur):
  - Reviewer:
  - Division/Portfolio Chief concurrence:
  - Notes: e.g., STP entry has been made or updated; document sponsor contacted for non-concur.
- Once the comments and recommendation are approved, notify the Doc Review team via Nonsecure Internet Protocol Router Network (NIPRNet) email at disa.huachuca.jitc.mbx.doc-review@mail.mil and they will upload the CRM and recommendation into KM/DS.
- Joint Staff J-8 uses a single review cycle for JCIDS documents.

C3.7 **Classified Document Considerations.** The IAM is on the NIPRNet, and the KM/DS is on the SIPRNet. Generally, the types of documents processed on the IAM are unclassified. The KM/DS documents generally are unclassified or SECRET. Table 3-1 explains how each of these systems handles unclassified and classified documents to ensure appropriate security controls.

**Table 3-1. Classified Document Considerations**

| Document Classification | IAM | KM/DS |
|---|---|---|
| Unclassified | Review and comment on the NIPRNet. | Review and comment on the SIPRNet. |
| SECRET | The IAM will have a placeholder document instead of the actual document. The placeholder should have instructions on how to access the document and what to do with your comments. Review and comment according to the placeholder instructions. | |
| Above SECRET | Same instructions as for SECRET documents. Review and comment according to the placeholder instructions. | The KM/DS will have a placeholder document instead of the actual document. The placeholder should have instructions on how to access the document and what to do with your comments. Review and comment according to the placeholder instructions. |

**Legend**

| | | | |
|---|---|---|---|
| IAM | Interoperability and Supportability Assessment Module | NIPRNet | Nonsecure Internet Protocol Router Network |
| KM/DS | Knowledge Management/Decision Support | SIPRNet | SECRET Internet Protocol Router Network |

C3.8 **Minimum Set of Architecture Information**. JITC, in coordination with the ISG, identified the minimum set of DoDAF architecture viewpoints necessary to evaluate joint interoperability for a JIC based on the NR KPP attributes. The IPG defines the minimum set of architecture viewpoints and related elements.

C3.9 **Alternate Interoperability Certification Requirements.** The IPG contains a provision for PMO/Sponsors to use other requirements documents, in lieu of a certified NR KPP and approved architecture viewpoints, with the concurrence of the DoD CIO, Joint Staff, and JITC. Examples include requirements for Defense Business Systems (DBS) and the Platform Integration Information Table (PIIT).

- The overarching framework for the planning, design, acquisition, deployment, operations, maintenance, and modernization of DBS was called the Business Capability Lifecycle (BCL). Although the concept continues, the term BCL is no longer used in more recent policy. The Business Enterprise Architecture (BEA) is the enterprise architecture for all DoD DBS and capabilities and reflects the DoD business transformation priorities; the business capabilities required to support those priorities, and the combinations of enterprise systems and initiatives that enable those capabilities.
- The PIIT simplifies the identification of NR KPP requirements under special conditions involving platforms. In this context, a platform is defined as a vehicle, air, sea, or surface, structure, or person that carries, contains, or includes multiple information systems. The JCIDS Manual contains a Content Guide that allows PMOs/Sponsors, in coordination with Joint Staff J-6, to substitute the PIIT for the NR KPP table.
- UC requirements are specified differently than DoDI 8330.01 NR KPP requirements. (See Chapter 8.)

# C4. CHAPTER 4. PLANNING

C4.1 **Overview.** The primary goals of the Planning Phase are to develop a rigorous evaluation approach (i.e., evaluation planning) and to ensure AOs are prepared to collect the data they need from anticipated tests or other sources (i.e., test planning).

This chapter establishes the activities and artifacts required during the Planning Phase of the joint interoperability T&E process, which covers the period from initial engagement with a program to the start of test (i.e., includes products from requirements generation). Figure 4-1 shows an overview of the joint interoperability T&E process.

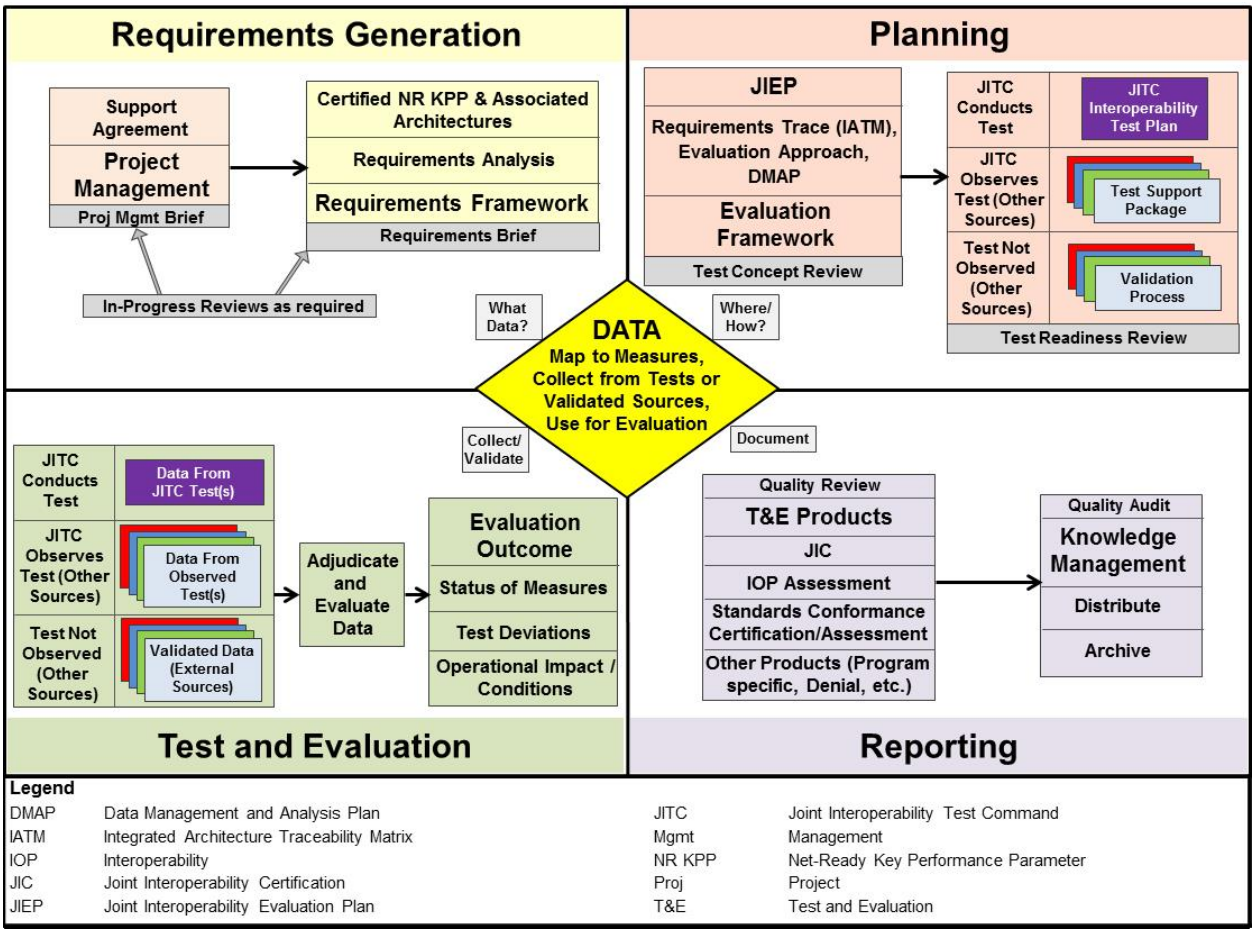
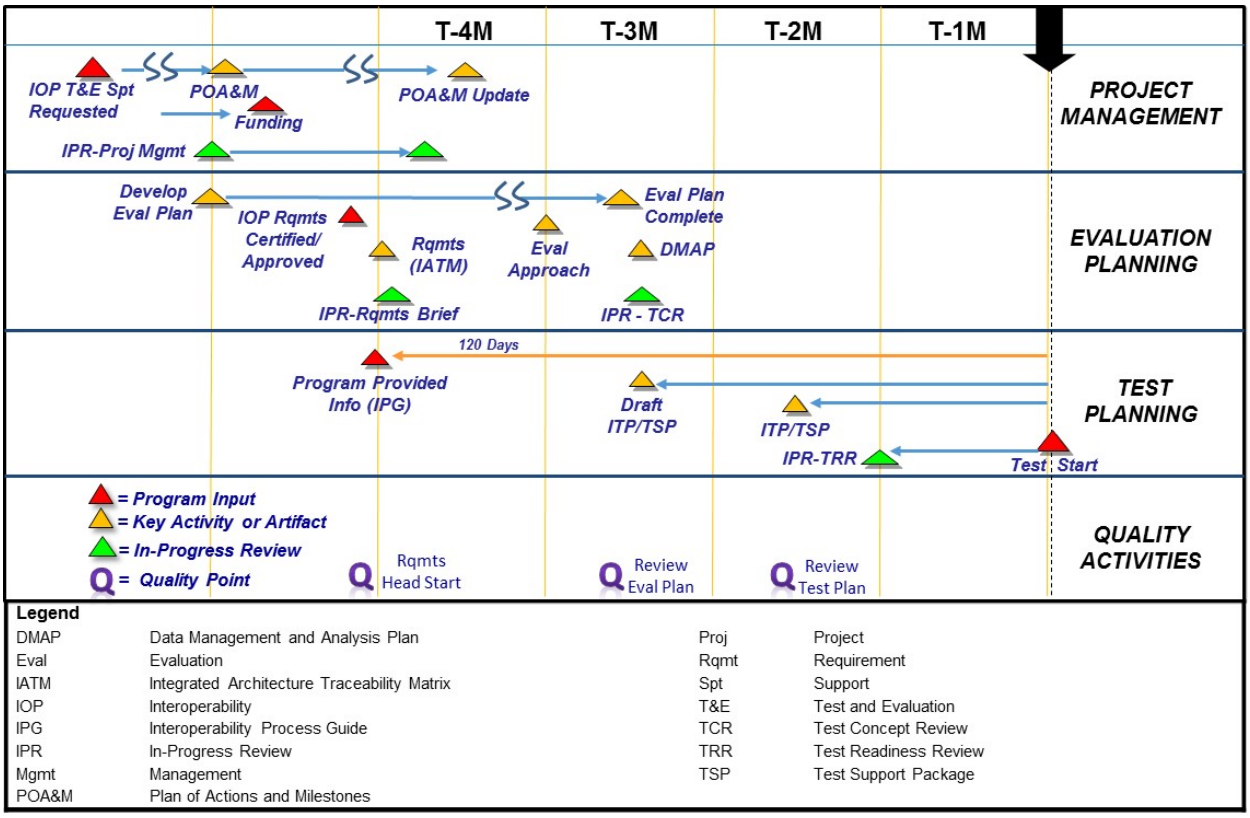



**Figure 4-1. Joint T&E Process Overview**

Figure 4-2 depicts an example timeline presenting significant activities and artifacts associated with the Planning Phase (Pre-test) in four lanes of effort: Project Management, Evaluation Planning, Test Planning, and Quality Activities. A planning timeline is part of the IPR.




**Legend**

| | | | |
|---|---|---|---|
| DMAP | Data Management and Analysis Plan | Proj | Project |
| Eval | Evaluation | Rqmt | Requirement |
| IATM | Integrated Architecture Traceability Matrix | Spt | Support |
| IOP | Interoperability | T&E | Test and Evaluation |
| IPG | Interoperability Process Guide | TCR | Test Concept Review |
| IPR | In-Progress Review | TRR | Test Readiness Review |
| Mgmt | Management | TSP | Test Support Package |
| POA&M | Plan of Actions and Milestones | | |

**Figure 4-2. Example Joint Interoperability T&E Planning Schedule**

Figure 4-3 depicts the products required during the joint interoperability T&E Planning Phase and the associated IPR briefs (for Commander's Watch List (CWL) systems). These align with the activities and artifacts in Figure 4-2. When required, the AO will coordinate and present IPR briefs to Senior Staff in accordance with the systems joint IOP T&E planning schedule.

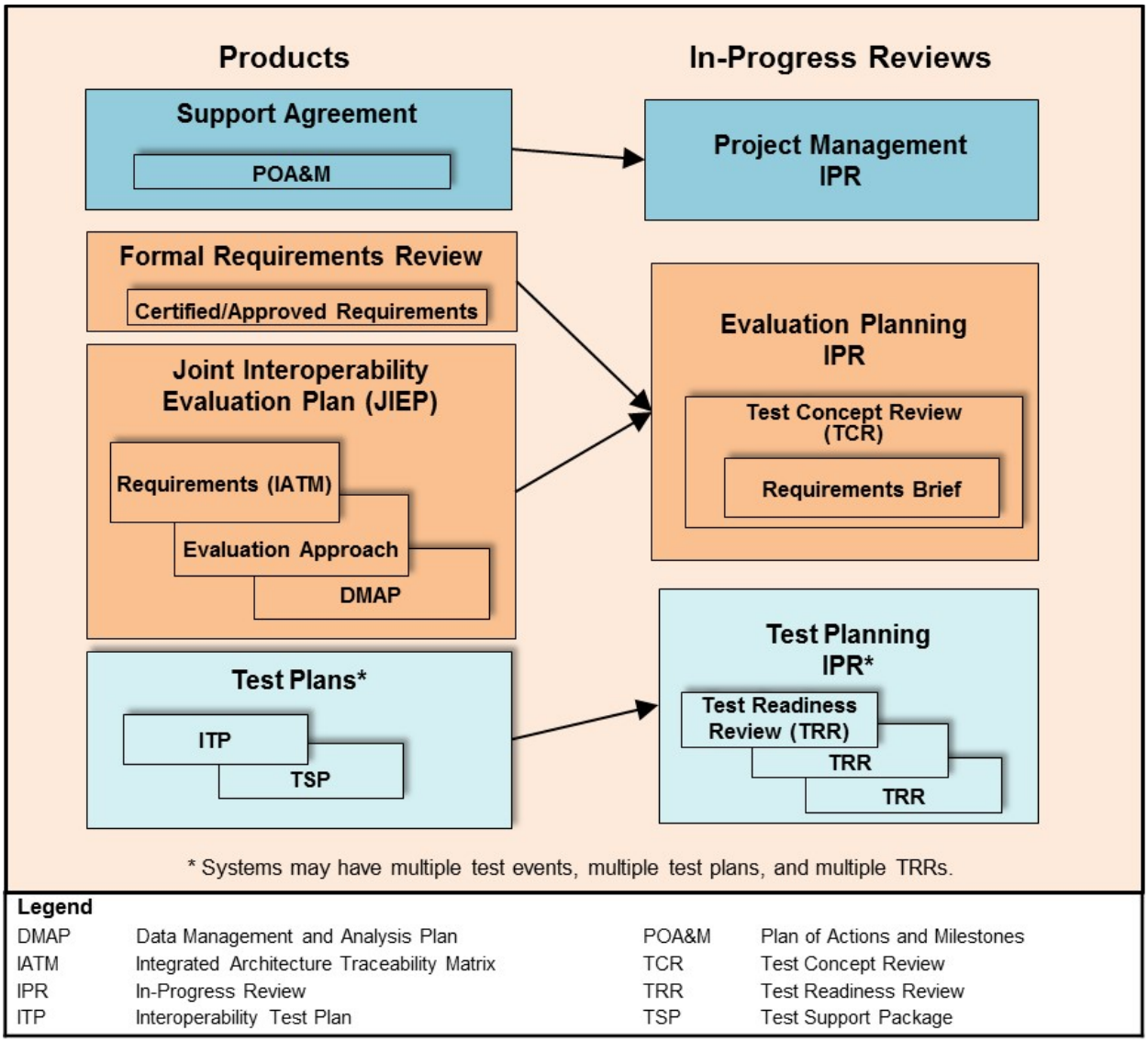



**Figure 4-3. Planning Products and In-Progress Reviews**

C4.2 **Project Management.** Project Management refers to the business-related requirements associated with providing joint IOP T&E support. This instruction addresses only the interdependencies between joint IOP T&E and developing a Support Agreement, which is required when JITC provides reimbursable support.

C4.2.1 **Support Agreement.** A support agreement (e.g., DD Form 1144) is an agreement between JITC and the customer that details the responsibilities of both parties and is required for JITC to provide reimbursable support. The agreement contains a POA&M that provides the technical information for the support. In this instruction, support agreements in general, whether an 1144 or only a POA&M, are referred to as POA&Ms.

The AO is responsible for developing the POA&M in coordination with the PMO/Sponsor. If details are not available to cover the entire T&E effort when the initial POA&M is drafted, then the AO should plan on updating the POA&M to address support through the final certification or assessment as T&E objectives and requirements become clearly defined.

An agreement should be completed in sufficient time to obtain funding to support the T&E effort. When using contracted support, the goal is to complete the POA&M 75 days before support is needed. The actual lead time varies with the scope and complexity of the support required.

There are multiple formats for the support agreement that are available in the JT2B Public Library on DEPS under the JT2B - MRTFB Program Controls Branch (https://disa.deps.mil/org/JT2/JT2B/_layouts/viewlsts.aspx?BaseType=1). Contact JT2B for timelines and questions regarding support agreements.

C4.2.2 **Program Documentation.** According to the IPG, the PMO/Sponsor is required to provide the following information no later than 120 days before the start of test. The AO includes these items in the POA&M.

- Joint Staff-certified NR KPP
- Architecture Information
- Interface Documentation
- Documentation of Standards Conformance
- Cybersecurity Documentation
  - System Cybersecurity Configuration
  - Refer to IPG for additional details
- Version Identification
  - System or system components to be certified
  - Interfacing capabilities and enterprise components
- Approved PMO/Sponsor and designated test organization test plans and planning documents
- Program Security Classification Guide (SCG)

C4.2.3 **Joint IOP T&E IPR-Project Management.** Applicable administrative business information is presented in the Project Management portion of the Joint IOP T&E IPR. See C4.5 for Joint IOP T&E IPR discussion.

C4.3 **Evaluation Planning.** Evaluation Planning is the process of developing the strategy and approach to evaluate whether or not a system meets the requirements based on the T&E goals (e.g., JIC or Joint Interoperability Assessment). The Joint Interoperability Evaluation Plan (JIEP) and the Evaluation Planning portion of the Joint IOP T&E IPR are the primary activities and artifacts of evaluation planning.

C4.3.1 **Joint Interoperability Evaluation Plan.** The JIEP defines the strategy and approach to evaluate whether the system meets the IOP requirements. It is required for all CWL programs. The JIEP contains program information (e.g., system identification, stakeholders, etc.), the IATM, Evaluation Methodology, and Data Management and Analysis Plan (DMAP), or at least links to those documents. The JIEP should be completed approximately 75 days before the start of test. For non-CWL programs, the test division may tailor the JIEP content to balance cost and integrity of the interoperability evaluation goals. The JIEP follows the test documentation guidance in NR KPP Evaluation Guidebook posted on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad.

C4.3.1.1 **Requirements.** The first section of the JIEP addresses adequacy (traceability and testability) of the joint interoperability requirements. Traceability is documented in an IATM, or similar construct, and must provide the requirements traceability information required for the JIEP. The primary output of an IATM is the data requirements and traceability for an IOP evaluation. An IATM is also useful to analyze and understand a system's architecture data. Guidance to develop the IATM is provided in the NR KPP Evaluation Guidebook posted on the JIST T&E pad.

C4.3.1.2 **Evaluation Approach.** The primary outputs of the evaluation approach are the data requirements, how the data will be collected, and the test events where the data can be collected. The first step in developing an evaluation approach is to review and analyze the system's interoperability requirements. The next step is to review the available test events in the program's test schedule and determine which of the required data will be available from each of the test events. A matrix can be used to correlate the required data and the planned test methods, key test resources, and facility or infrastructure needs. The discussion of an evaluation approach should also identify major risks or limitations to completing the evaluations. The Evaluation Approach will also contain a process to validate data when JITC does not observe collection. Guidance to develop the evaluation approach is provided in the NR KPP Evaluation Guidebook posted on the JIST T&E pad.

C4.3.1.3 **Data Management and Analysis Plan**

The management portion of the DMAP comprises several elements: principles, practices, and processes that enable the management of digital (and hardcopy, as appropriate) product and program artifacts. The fundamental data management processes are:

- Identification and Definition

- Acquisition and Preparation
- Control
- Disposition/Distribution
- Archival/Retention

The fundamental data management processes also provide a basis for data validation.

The analysis portion of the DMAP provides detailed procedures for the collection, reduction, collation, and analysis of data gathered to support determination of a system's interoperability. The analysis plan is a planning tool to ensure procedures are in place for assessing data collected upon completion of test execution. The analysis plan should include the purpose of the data analysis, data sources (including a description and any limitations), key variables to be used, and the analysis methods. Guidance to develop the DMAP is provided in the NR KPP Evaluation Guidebook posted on the JIST T&E pad.

C4.3.2 **Joint IOP T&E IPR – Test Concept Review with Requirements Brief.** The Evaluation Planning portion of the Joint IOP T&E IPR is the Test Concept Review (TCR). The TCR addresses the evaluation approach, which includes a joint interoperability Requirements Brief that can be presented as part of the test concept or as a stand-alone brief. Due to the importance of requirements in the planning process, a Requirements Brief should be presented early in the planning process and whenever there is a significant requirements change (i.e., that impacts the evaluation approach). See C4.5 for Joint IOP T&E IPR details.

C4.4 **Test Planning.** Test planning refers to the actions of coordinating and developing the Interoperability Test Plans (ITPs) and Test Support Packages (TSPs). These products provide the detail needed to conduct, or participate in, specific test events and collect the data identified in the interoperability evaluation plan (e.g., the JIEP). Perform test planning in coordination with the PMO/Sponsor and the service component test agencies, as applicable.

An ITP or TSP is required for test events supporting joint interoperability evaluation of systems on the CWL. They are subject to a formal quality review and must be signed before the applicable test activities begin. For non-CWL programs, the test division may tailor the test plan products as appropriate to ensure valid data collection.

ITPs and TSPs ensure data collected from events JITC conducts or observes, respectively, are valid for the T&E objectives. In cases where JITC does not observe an event, the Lead AO is responsible for developing guidance and criteria to validate data used are sufficient for the T&E objectives and documenting the process in the evaluation plan. Guidance for data validation is provided in the NR KPP Evaluation Guidebook posted on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad.

Refer to Chapter 6 for appropriate ITP/TSP staffing and approval authority.

C4.4.1 **Interoperability Test Plan.** An ITP is intended for use when JITC is conducting the test. The ITP describes the system to be tested, test objectives, and detailed test procedures for an interoperability test. An ITP is required for each JITC-conducted test event. The ITP details the testing, data collection, and analysis procedures that apply to that event. Guidance to develop the ITP is provided in the NR KPP Evaluation Guidebook posted on the JIST T&E pad.

C4.4.2 **Test Support Package.** A TSP is used when JITC collects data from a test conducted by another organization. Therefore, the TSP should provide sufficient explanation to ensure the right data is collected. Guidance to develop the TSP is provided in the NR KPP Evaluation Guidebook posted on the JIST T&E pad.

C4.4.3 **Joint IOP T&E IPR – Test Readiness Review.** The Test Planning portion of the Joint IOP T&E IPR is the Test Readiness Review (TRR). The TRR addresses details related to test execution such as test environment, data collection, instrumentation, and automation. A TRR should be presented about 30 days prior to the test event. See C4.5 for Joint IOP T&E IPR discussion.

C4.5 **Joint Interoperability T&E In-Progress Review (Joint IOP T&E IPR).** In-progress reviews are required for systems on the CWL and highly encouraged for all systems to provide situational awareness and a venue to request assistance. The purpose is for the AO to brief the chain of command on the status of interoperability T&E, in as much detail as possible. The IPR consists of three main sections: Project Management, Evaluation Planning, and Test Planning. For non-CWL programs, Division Chiefs may require parts of the IPR for any program that belongs to their division. Follow the content and format guidance in the Joint IOP T&E IPR Guide posted on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad.

C4.5.1 **Project Management**. The Project Management portion of the IPR provides a high-level description of the system, the anticipated JITC support, and additional details of business-related activities and artifacts, as required. The Business Operations Division (JT2) manages the content of this section.

When an IPR is required, the relevant Project Management information should be presented before the POA&M is completed and must be presented before participating in any test events. The AO should coordinate with business operations regarding requirements to update the POA&M if scope or funding requirements change. Action Officers are responsible for coordinating and scheduling IPRs with JT2.

The Project Management portion can be presented with other portions of the IPR or as its own stand-alone brief.

C4.5.2 **Evaluation Planning**. The Evaluation Planning portion of the IPR addresses the requirements and evaluation approach.

C4.5.2.1 **Test Concept Review.** The TCR is the Evaluation Planning portion of the system's Joint IOP T&E IPR. The TCR is required for systems on the CWL or as directed by the Technical Advisor. It focuses on test design, to include requirements

status. When required, the TCR will be presented 30 days prior to completion of the JIEP or the first test event, whichever comes first. The TCR can be combined with the TRR if appropriate (Division Chief's discretion). The Joint IOP T&E IPR Guide outlines the content for the TCR and is posted on the JIST T&E pad.

C4.5.2.2 **Requirements Brief.** The Requirements Brief is part of the Evaluation Planning portion of the system's Joint IOP T&E IPR. The Requirements Brief is required for systems on the CWL or as directed by the Technical Advisor. The purpose is to influence requirements early in the planning phase and provide leadership the status of requirements with regards to supporting a joint interoperability evaluation for a certification decision. Division Chiefs may request a Requirements Brief for any program that belongs to their division. The brief, if required, should be prepared in time to influence the requirements (before or during the formal review) but not later than 10 days after completion of the formal requirements review. See Chapter 3 for the formal interoperability requirements review process discussion. The Joint IOP T&E IPR Guide contains a template for the Requirements Brief and is posted on the JIST T&E pad.

C4.5.3 **Test Planning.** The TRR is the Test Planning portion of the system's Joint IOP T&E IPR. The TRR is required for systems on the CWL. The purpose of the TRR is for the AO to demonstrate they are prepared to test. One or more TRRs shall be presented to address all test events. Multiple TRRs can be presented for a single test event (i.e., complex events). The TRR should be presented no less than 30 days before start of test, earlier if needed to execute corrective actions. Division Chiefs may request a TRR for non-CWL programs. The Joint IOP T&E IPR Guide contains a template for the TRR and is posted on the JIST T&E pad.

C4.6 **Quality Activities.** Quality activities are the steps taken to ensure JITC IOP products are consistent, comprehensive, and correct. In the planning phase these steps include support provided to AOs during interoperability requirements development and quality reviews of T&E products as listed below.

C4.6.1 **Requirements Head Start Review.** The Requirements Head Start Review addresses traceability between attributes, completeness of measures, and other characteristics related to the quality of the requirements. Under this review, JT4A will conduct an initial interoperability requirements document review on new requirements for CWL systems, as resources permit. The goal is to provide the AO review results 5-10 work days from receipt of review tasking from the owning EA. This JT4A review does not relieve AOs from the responsibility of conducting a thorough review of the joint interoperability requirements.

C4.6.2 **Review Evaluation Plans.** The JIEP is subject to a Quality Review or Quality Audit. Refer to Chapter 6 for review and staffing requirements.

C4.6.3 **Review Test Plans.** The ITPs and TSPs are subject to a Quality Review or Quality Audit. Refer to Chapter 6 for review and staffing requirements.

# C5. CHAPTER 5. TEST AND EVALUATION

C5.1 **Test & Evaluation Overview.** As the designated DoD Joint Interoperability Certification Authority, JITC is empowered by the DoD CIO to certify whether or not a system meets its joint interoperability requirements. The AO must perform thorough and independent evaluation to verify the system meets technical requirements and confirm that critical interfaces and interfacing systems interoperate and do not impact the interoperability environment, which will ultimately lead to certification.

C5.1.1 **Joint Interoperability Requirements.** JITC evaluation is based on clearly defined requirements. Valid requirements must meet three criteria: 1) They must include a Joint Staff-certified NR KPP and approved architecture viewpoints; 2) They must be traceable and testable (measurable); and 3) They must allow for testing of joint critical tasks (mission activities), information exchanges, networks (transport), and interfaces in an operationally realistic environment.

If a system does not have testable or measurable requirements or other substantive requirements issues are discovered, the AO must coordinate (via their chain of command) with the PMO/Sponsor and the Joint Staff J-6 in sufficient time to resolve before testing. Changes to certified/approved joint interoperability requirements require coordination with the Joint Staff and the Component Acquisition Executive (or delegated authority). The JIC addresses all the joint interoperability requirements in the certified NR KPP and approved architecture viewpoints. The PMO/Sponsors cannot "move" a requirement to a later increment (e.g., spiral/block) without following the requirements approval process. Consult the Strategy and Policy Branch (JT4A) for issues regarding policy and when assistance is needed.

A system without a Joint Staff-certified NR KPP and approved architecture viewpoints would not normally be eligible for a JIC. JITC cannot issue a JIC without Joint Staff-certified NR KPP and approved architecture viewpoints (or equivalent). However, JITC may still perform an evaluation of interoperability and publish test reports or Joint Interoperability Assessments. The AO can use available documentation to determine requirements and then work with user communities to ascertain requirements criticality. Refer to Chapter 3 for alternate requirements documents.

C5.1.2 **Test Plans and Execution.** An approved ITP or TSP is required prior to conducting testing when JITC is the lead or when participating in another organization's test event, respectively. Changes in test configurations or system requirements, architecture, or concept of operations may occur that require modification to test plans. Coordinate any changes with JT4A to determine the level of approval needed.

The AO must follow preferred practices when testing:

- Verify that system and network configurations used in testing are representative of an operationally realistic environment, to include cybersecurity characteristics of that environment.

- Comply with the Program SCG to ensure that all JITC products are marked properly and handled appropriately.
- Coordinate as necessary with JT4A, the PMO/Sponsor, and Joint Staff J-6.
- Enter/update system information into the STP, including test activities, test-related documents, and document tracking information, to include test start/end and last test activity dates.

When JITC conducts the test, the AO:

- Must use an approved ITP/DMAP.
- Must carefully document the test configuration, cybersecurity configuration, and maintain configuration management (CM).
- Must document any deviations during the test. If deviation was discovered prior to testing start, if feasible (i.e., time allowed), it is highly recommended that the approved test plan be modified to reflect the changes. If that is the case, then coordination with the AO's chain of command and JT4A (if a CWL system) is required. The test plan will be appropriately staffed and sent out using the ERD tool so that an official copy can be kept in the JIT/STP. Reviewers will focus the review on the changed sections. The test report and certification letter will document the deviation, and the test configuration will accurately reflect what was tested.
- Must document any anomalies discovered.
- Must verify the test environment will support the T&E needs (relevant to what is being evaluated).
- Ensure system has the appropriate cybersecurity accreditation to connect to the test environment (e.g., a test network, an operational network, etc.).
- Ensure the data integrity (collection, reduction, analysis, archiving, etc.) and adjudication of the test data process.
- Must store raw test data in a designated central storage area, such as the JDMT (follow guidance provided by the JDMT instruction for the database structure). Refer to current JITC Records Management (RM) policy for additional guidance.
- Must follow the guidelines provided in this instruction, JITCI 380-50-02, to issue the appropriate JITC interoperability product.

When JITC witnesses rather than conducts a test, the AO:

- Must use an approved TSP/DMAP.
- Must validate the Responsible Test Organization's (RTO's) test design is implemented per RTO's test plan.

- Must validate the RTO's test configuration and conditions, making sure such configuration and conditions are based upon any early mutual agreement.
- Must be ready to provide answers to any clarification questions, whether technical or procedural, asked by any test participant/observer.
- Provide formal in-brief or de-brief prior to and after the start of a test as required.
- Depending upon agreement with the test director (e.g., test plan, test procedures), provide input concerning deficiencies that occur during the test.

C5.2 **Testing Timeline.** Figure 5-1 depicts the testing timeline and some of the major steps toward completing a successful test.

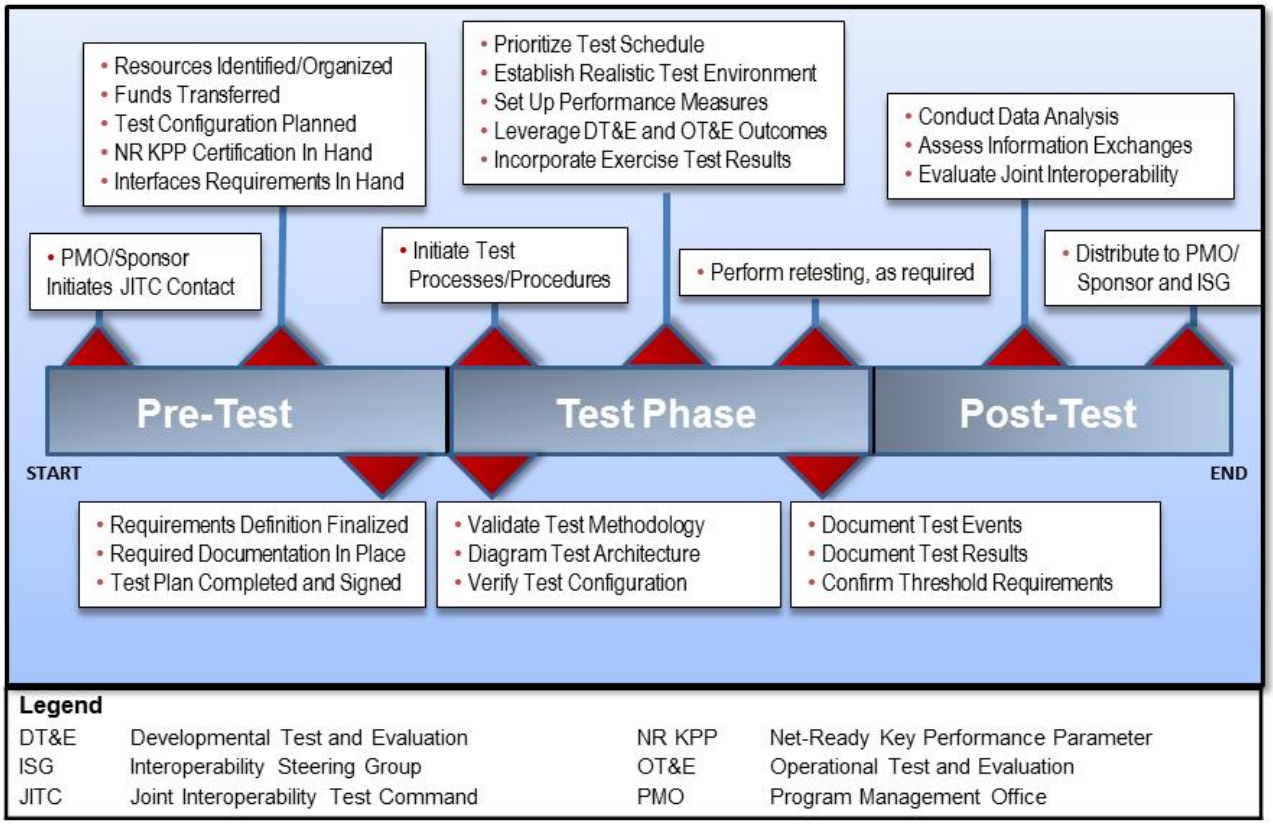



**Figure 5-1. Testing Timeline**

Since test data may be derived from multiple events, the AO is responsible for ensuring data collection and analysis is based on valid data from reliable sources that contribute to the eventual evaluation. Valid data is acceptable from standards conformance testing, developmental testing (DT), operational test and evaluation (OT&E), or other reliable sources such as military exercise events.

C5.3 **Life-Cycle Certification Processes.** Once JITC certifies a system and while it is fielded, the need for follow-up review and possible retesting and recertification continues. Figure 5-2 outlines a typical system certification process. If significant changes or modifications occur to the system or to its interoperability environment that potentially affect joint interoperability, the status must be reviewed. Otherwise, after four (4) years, the cycle begins anew with a review of interoperability requirements and status.

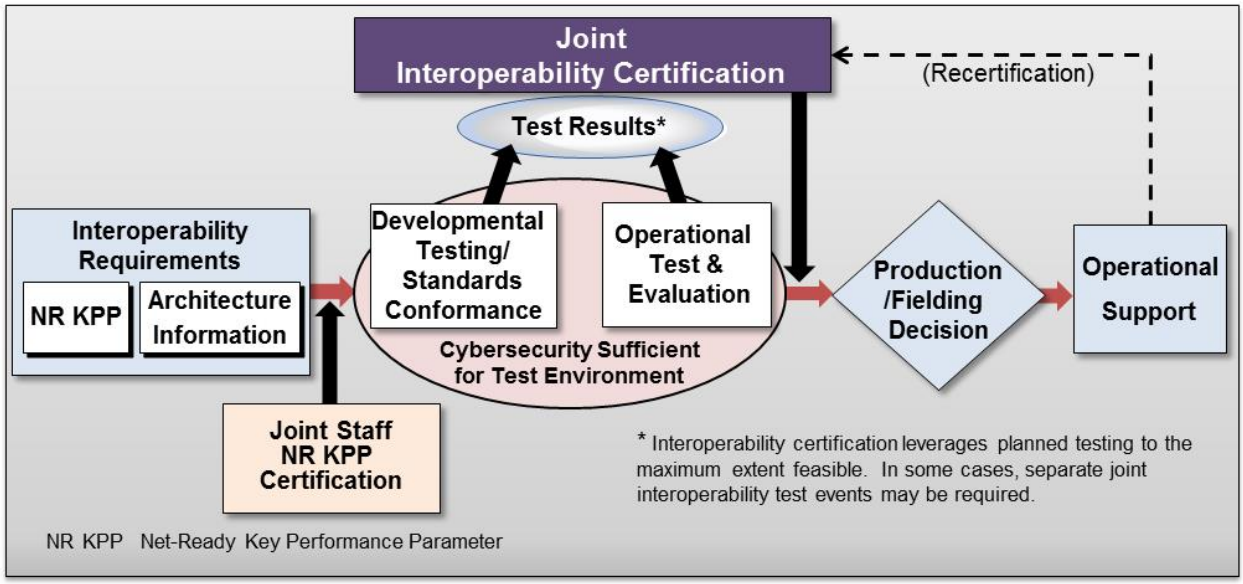



**Figure 5-2. System Life-Cycle Certification Process**

C5.4 **Lead Action Officer.** The Test Division Chief will direct the designation of a Lead AO to be the program/system POC. The Lead AO is responsible for managing the system's entire testing and certification effort, which includes the cost estimate; entering and updating the system information in STP; system requirements assessment and validation; and test and certification products. The Lead AO will establish a test team consisting of the Lead AO, support staff, and representatives of all test support organizations.

The Lead AO's Division has responsibility for ensuring an effective and efficient test program. Other divisions may play a supporting role in conducting test activities in coordination with the Lead AO. The Lead AO retains responsibility for test team actions and represents JITC to the PMO/Sponsor. Typically, the Lead AO's Division issues the appropriate certification and supporting test product(s).

Test and certification products (test reports, certifications or assessments, etc.) will identify the Lead AO and Division. If a supporting division issues a certification product, the Lead AO will review the product.

C5.5 **Interoperability T&E and Certification Products.** This section describes the principal interoperability-related products that JITC develops to document its joint T&E and certification activities. JT4A provides guidance, such as templates and instructions, for developing test plans and reports, and certifications. Variations of these products are not authorized without prior coordination with JT4A. This stipulation ensures JITC products are consistent with DoD policy and properly implemented in accordance with command guidance.

C5.5.1 **Joint Interoperability Certification.** A JIC is the primary JITC product based on an evaluation of joint interoperability requirements. The purpose of a JIC is to document a system's interoperability to support a fielding decision. A system must have a Joint Staff-certified NR KPP and approved architecture viewpoints to receive a JIC.

C5.5.2 **Joint Interoperability Certification With Conditions.** JITC may issue certifications with conditions (limitations) when only subsets of the requirements are met. Conditional certifications provide the interoperability status for cases where useful capabilities are provided, despite not meeting all threshold requirements, and there are no expected critical operational impacts or adverse effects on the joint interoperability environment. Conditions are based on expected operational impact of discrepancies and limit the operational use of the system to only those capabilities that were adequately demonstrated. A PMO/Sponsor may submit the system for additional interoperability evaluation in order to have conditions removed.

C5.5.3 **Joint Interoperability Assessment.** In circumstances where full system certification is not achievable, practicable, or desirable, preliminary interoperability status may be available in the form of a Joint Interoperability Assessment. An assessment can be particularly useful in cases where requirements documents have not been finalized or high-risk areas warrant early feedback. In these cases, an assessment may prove useful in providing constructive feedback concerning interoperability strengths and weaknesses.

Joint Staff-certified requirements are not required to conduct an assessment. In addition, not all requirements need to be evaluated to provide an assessment. Distribution of an assessment report may be limited to the PMO/Sponsor and other designated parties. Any system, United States (U.S.) or non-U.S., is eligible for a Joint Interoperability Assessment, and almost any test or exercise venue may be used. Note that DoDI 8330.01 requires an interoperability certification be granted (not an assessment) before fielding a new IT capability or upgrade.

C5.5.4 **Denial of 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 the DoD CIO, Joint Staff, Milestone Decision Authority (MDA), and PMOs/Sponsors notification of problems that warrant immediate attention.

C5.6 **Other JITC Interoperability T&E and Certification Considerations**

C5.6.1 **Recertification of Joint Interoperability Certification.** Interoperability status can change over time. Standards, interfacing systems, and even cumulative minor upgrades have the potential to impact the ability of systems to interoperate. Each factor must be carefully monitored throughout a system's lifecycle. Thus, interoperability certification for a specific

increment (i.e., version) must be renewed periodically or when system, interoperability environment, or performance requirement changes occur that affect joint interoperability. The IPG Section 5.c. details the recertification process.

C5.6.2 **Expired Certifications.** JITC should be contacted by the PMO/Sponsor at least six (6) months prior to the scheduled expiration date. Note that the PMO/Sponsor is responsible to notify JITC regarding incremental upgrades and other changes affecting interoperability. IPG Section 5.c details the certification process for expired (or expiring) certifications.

Among the actions the AO must consider are the current set of requirements and their certification status, as well as examine all interfacing systems to ensure no change in interoperability status, requirements, or the interoperability environment. Presuming all necessary conditions are met, a new JIC (or certification with conditions) may be issued without additional interoperability testing.

C5.6.3 **Certification Extensions.** The original certification may be extended (to another system version, not the expiration date) if it is determined that 1) any system modification has not affected interoperability, 2) interfacing systems are essentially unchanged, and 3) the operating environment remains unaltered. IPG Section 5.b.(5) details the extension process. Figure 5-3 illustrates this process.

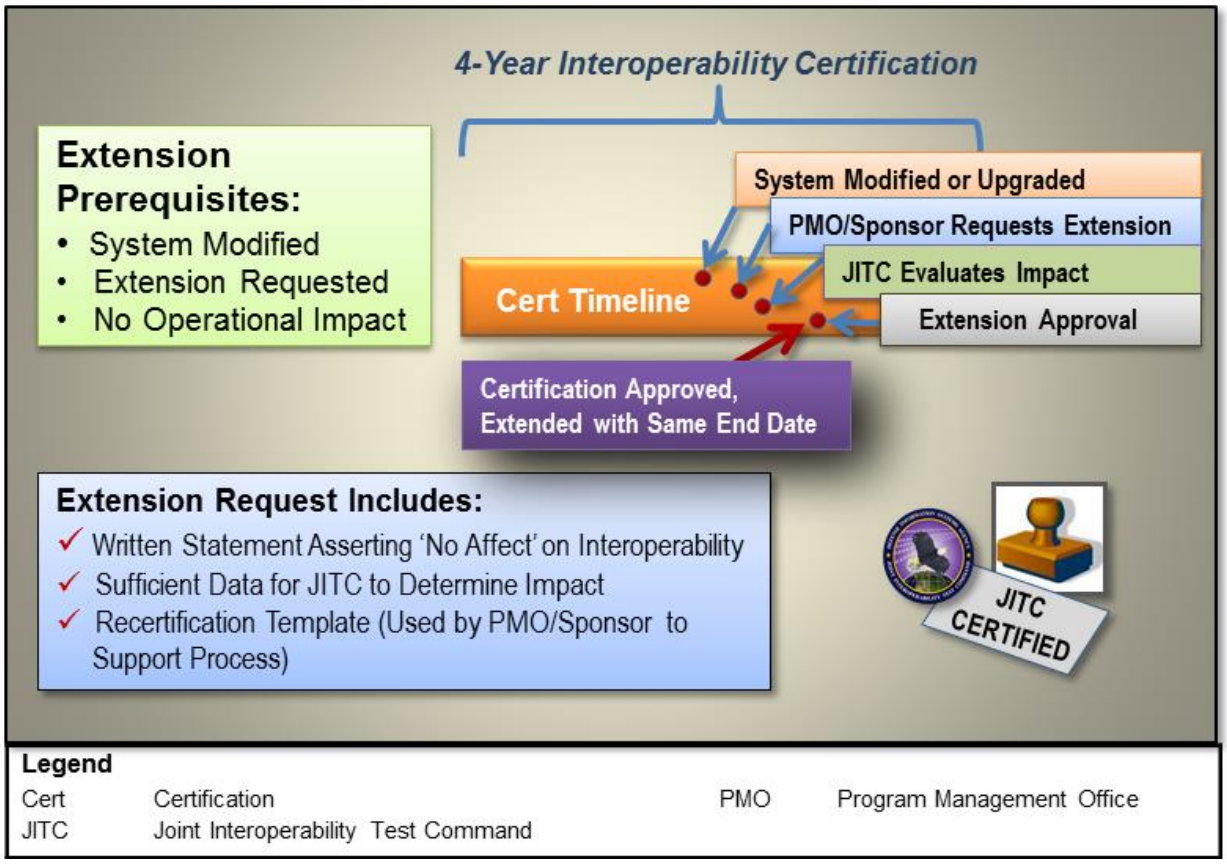



**Figure 5-3. Certification Extension Process**

C5.6.4 **Revocation and Re-issuance of Certifications.** JITC may rescind, revoke, or reissue JICs. See IPG Section 5.b(4) for details. The AO will notify all parties who received the original JIC, and will ensure status updates are posted on the STP. Revocations and Re-issuances are infrequent, contact JT4A for assistance.

C5.6.5 **Configuration Management.** Use of formal CM processes is fundamental to sound test management. The system configuration must be described in detail, and hardware and software (including firmware) version identification must be identified in all JITC test documentation. This includes test reports, assessments and certifications, and status letters. When formal CM processes are not specified in support of a test program, AOs will follow instructions contained in JITCI 280-50-01, "Configuration Management."

C5.6.6 **Testing Foreign Systems.** JITC may be tasked to conduct foreign systems interoperability testing. The IPG section 9.b. details the testing of foreign systems.

The AO will first coordinate with JT2 in all cases involving a foreign national customer. Typical issues that may be encountered involve potential funding issues or conditions such as security or material transfer that must be conducted in accordance with special guidelines that stipulate how JITC must perform when dealing with foreign entities.

C5.6.7 **Homeland Security Support.** JITC provides interoperability assessments and standards conformance certifications, as appropriate. JITC typically does not issue JICs for Homeland Security-sponsored systems due to the lack of Joint Staff-certified requirements. The IPG section 9.c. details support to Homeland Security systems.

C5.6.8 **Stimulators/Simulators and Training Systems.** Stimulators/simulators and training systems are authorized for use throughout JITC to support testing activities. The IPG section 9.d. details the use of stimulators/simulators and training systems.

JITC may certify stimulators, simulators, and training systems in the same manner as operational systems if they have Joint Staff-certified requirements. However, systems cannot be certified by JITC as representing an accurate model of any particular environment. Accordingly, certification memoranda should contain wording to the effect: *"This is a certification of system conformance to interoperability standards or system interoperability [tailor to fit situation]. It is not a certification of system performance adequacy as stimulator or simulator in any specific environment or application."* The AO should carefully tailor the wording, as appropriate.

C5.6.9 **Validation of Test Tools and Standards.** Test tools (and any associated test suites) and standards/standards profiles must be validated before T&E use. JITC may contribute to the validation as requested by a standards body. In this situation, validation takes place under the authority used to establish a JITC testing program.

C5.6.10 **Test Execution and Interoperability Status.** Interoperability testing may be accomplished by JITC or other designated test organizations. When possible, testing is performed in conjunction with other designated test organizations to conserve resources and achieve greater testing efficiencies. A test scenario should include a message mix, traffic loading that reflects normal and wartime modes, and operation in benign and hostile environments.

JITC (i.e., the Lead AO) must meet the delivery goals for JIC as specified in Section 5 of the IPG. The AO must maintain close coordination with the PMO/Sponsor and the designated test organization to ensure prompt receipt of all relevant test data, reports, and system/test configuration and version identification information. This includes details about interfacing systems, test data, trouble reports, and analysis of any discrepancies noted.

An interoperability assessment may be issued based on Developmental Test and Evaluation (DT&E), OT&E, acceptance testing, interoperability exercises, or similar test venues. The PMO/Sponsor coordinates with the JITC POC (generally the Lead AO) to establish specific needs and documentation requirements.

For systems fielded in increments, a JIC may be issued for each increment. IPG section 5.b.(1)(b) details policy and procedures on handling system increments.

Additional requirements subject to evaluation include those that do not appear in the integrated architecture products, for example, a capability to communicate on two channels simultaneously. Any change affecting the increment or the criticality of a requirement is a modification to the requirements that may prompt Joint Staff re-certification action.

C5.6.11 **Additional Test Execution Guidelines.** Ensure respective Division guidelines are adhered to before coordinating with Joint Staff J-6 to resolve T&E-related issues. Inform JT4A of coordination efforts when feasible.

Interoperability evaluation must substantiate that interoperability requirements are met. Information exchanges and operational usage must be confirmed, including those attributes pertaining to accuracy, completeness, timing, and security. Meeting these criteria means the system under test not only functions correctly, but the interfacing systems also perform as required and that the network infrastructure provides the necessary reliability, bandwidth, response times, and security for effective information exchange.

Certification status may be verified during exercises and deployments throughout the system's lifecycle. If serious interoperability problems are observed, evaluations should be performed to confirm and update system status. Results will be reported as follows: existing certifications may be confirmed (no action required), extended to minor system releases (extension issued), or revoked. Interoperability status memoranda will be issued as appropriate.

C5.7 **JITC Reporting and Certification Determination.** Interoperability T&E quantifies the degree to which a system interoperates with other systems. Successful certification signifies the system is interoperable and ready for use in a joint/combined/coalition operational environment. Certification letters state what was tested, the scope of testing (test coverage, including testing limitations), and the interoperability status of each joint interface.

Interfaces may be derived from the NR KPP table or architecture information. These sources usually contain a textual or tabular list and a graphical representation of external interfaces in the architecture products, such as Operational Viewpoint (OV)-1/2 and Systems Viewpoint (SV)-1/2.

C5.7.1 **Interoperability Determination.** Joint interoperability certification is based on a Joint Staff-certified NR KPP and approved architecture viewpoints, the criticality of the requirements, and the expected operational impact of any deficiencies. Certification applies to the overall system. Interoperability certification represents the extent to which a system is interoperable with respect to the requirements in the NR KPP table, architecture information, standards conformance, and other stated interoperability requirements.

Deficiencies with critical operational impacts are grounds for denying certification. A Denial of Joint Interoperability Certification may also result from the cumulative impact of less severe problems or failed non-critical requirements. Because of the complex factors determining interoperability, atypical situations must be handled on a case-by-case basis. For example, a failed critical interface may result in either a Joint Interoperability Certification with Conditions or Denial of Joint Interoperability Certification. Situations where most critical requirements are met with no critical adverse effect on the interoperability environment will usually result in a Joint Interoperability Certification with Conditions. In other situations where the requirements or interoperability status preclude issuing a JIC, an assessment may be issued to inform the PMO/Sponsor.

C5.7.2 **Joint Interfaces.** Interoperability of joint interfaces is a key factor in determining whether a system meets requirements and whether joint systems are "interoperable." This is not necessarily an indication that the system under test does or does not contain any faults. Although it is desirable to isolate faults to a particular test item, the overall system interoperability status should reflect whether the interoperating systems meet their mutual requirements. In other words, faults impacting interoperability must be assessed, regardless if the faults exist in the system under test, an interfacing system, or the supporting communications infrastructure.

JITC categorizes the degree of interoperability of systems and interfaces based on performance and the expected operational impact of any interoperability deficiencies. Consequently, the AO must work closely with the user community when assessing the risk of operational impact directly attributable to a discrepancy. Weighing the operational impact of each discrepancy and the cumulative effect of all discrepancies is critical in determining whether or not to certify a system.

C5.8 **Operational Test Readiness Review Interoperability Statement.** A formal review is conducted to ascertain whether or not a system can proceed into operational testing (OT) with a high probability of success. This review examines the system's progress against critical technical parameters, risks, and other entrance criteria. When requested, JITC may provide an assessment of a system's joint interoperability to include in the OTRR. (See IPG section 3.h.(4).) Figure 5-4 shows this review.

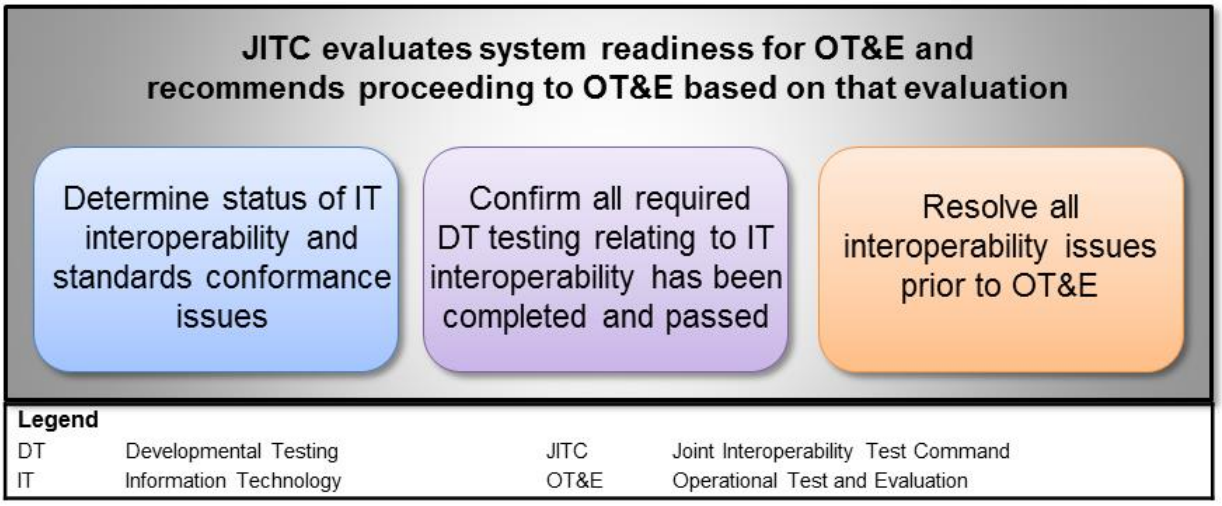



**Figure 5-4. JITC OTRR Readiness Evaluation**

When JITC is requested to provide OTRR input, the Lead AO will produce an interoperability statement memorandum that has been coordinated with other appropriate divisions to ensure a consolidated JITC position. Upon completion, distribution is made to the PMO/Sponsor-specified ERD recipient list and ERD Interoperability Certification Letter Core (distribution) List.

C5.9 **Test Environment: Cybersecurity Assessment.** JITC will evaluate cybersecurity or portions of cybersecurity requirements when requested, and will document any known cybersecurity issues as part of assessing the interoperability status of a given system.

Joint interoperability certification is based on T&E of production systems in as realistic an operational environment as practicable, including an authorized cybersecurity configuration. Accordingly, pre-test activities by JITC will include verifying that system and network configurations used in testing are representative of an operationally realistic environment, to include cybersecurity characteristics of that environment.

Cybersecurity requirements may not be able to be assessed fully until JITC interoperability certification is concluded. However, cybersecurity issues uncovered during testing which have potential critical operational impact may result in JITC being unable to certify the system.

The PMO/Sponsor should provide cybersecurity information to JITC at least 120 days prior to any T&E activity supporting a JIC. This documentation is essential to establish the authorized cybersecurity configuration that sufficiently recreates an operationally realistic testing environment. This includes applying all applicable cybersecurity controls. An improper configuration may result in invalid test results, thus requiring additional testing.

The early test planning stage is the best time to define a suitable interoperability environment for both the system under test and for interfacing systems. One exception, a PMO/Sponsor seeking to develop an enterprise application or service that is wholly dependent upon the enterprise infrastructure for security and access control may request a waiver from a requirement for security certification by the sponsor's Authorizing Official.

C5.10 **Operational Test and Evaluation.** JITC serves as the OTA for many systems. As the OTA, JITC provides test directors and test personnel to support operational test events. The primary purpose of OT&E is to determine whether systems are operationally effective, suitable, and survivable for the intended use by representative users in an operationally realistic environment before production or deployment. Refer to the Operational Test and Evaluation Guidebook posted on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad under the OT&E Products tab.

(This page intentionally left blank)

# C6. CHAPTER 6. REPORTING
# (Staffing, Distribution, and Archiving)

C6.1 **Overview.** This chapter covers internal JITC staffing and routing procedures used to process JITC T&E and certification products for review. Specific business practices may differ based on the nature and type of JITC product and the associated level of command attention involved.

The command's review process, as shown in Figure 6-1, maintains the quality and consistency of certification and test products. All products for CWL systems, unless the product is Exempt, must undergo Division and Command review. The Strategy and Policy Branch (JT4A) oversees and manages the certification and test product review process. The internal Interoperability Product Review Process, instructions, and e-Form 9 templates are posted on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad.

JITC products fit into three categories of review:

- Certification and test products for CWL systems
- Certification and test products for non-CWL systems and CWL Exempt products
- Denials of Certification

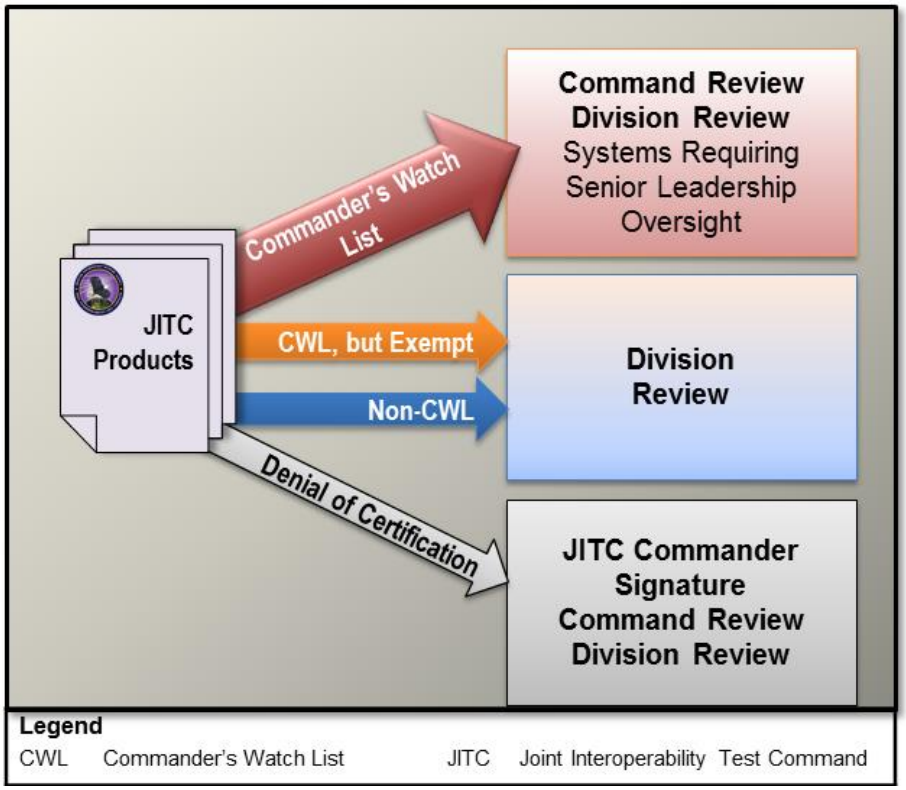



**Figure 6-1. JITC Staffing and Review Process**

C6.2 **Commander's Watch List.** The CWL identifies systems needing an additional level of oversight. The CWL serves as an internal JITC management tool to process and review selected certification and test products – those that warrant special attention prior to product release.

A system that meets one of the following four criteria will be placed on the Commander's Watch List:

- Has a DISA Responsible Organization
- Acquisition Category (ACAT) I (and variants such as ACAT IAM)
- On the Director, Operational Test and Evaluation (DOT&E) Oversight List
- Any system the JITC Commander deems to be deserving of special attention

A Division Chief may recommend a system CWL status change. Recommendations are submitted via JT4 to the Commander for approval. If circumstances change, JT4 can recommend putting the system back on the CWL.

The JITC STP View System page provides the CWL status.

C6.3 **Joint Interoperability T&E Products Review.** T&E products are reviewed to ensure the information they possess is true, correct, complete, and contain representative results of a sound technical approach aligned to existing guidelines and policies. Reviews focus on multiple aspects of a T&E product, ranging from technical content and rigor to grammar and format. The goal is to produce an authoritative product using a rigorous approach that accurately and objectively represents T&E outcomes.

C6.3.1 **Reviewing Responsibility.** Products for a CWL system require Division, Quality (JT4A), and Command (Technical Advisor) review. Products for non-CWL and CWL-Exempt systems are reviewed at the Division level only.

The staffing process, instructions, and e-Form 9s are located on the JIST T&E pad. In lieu of e-Form 9s, the AO can use JAWS.

A Denial of Certification differs from other products in that the JITC Commander, not the Division Chief, ultimately signs the document.

C6.3.2 **Quality Review.** Quality Reviews are formal, independent checks of JITC's T&E products conducted by JT4A. Quality Reviews are required for specific T&E products generated for systems on the CWL (see list below). The reviews are a means to ensure JITC's official T&E products are technically correct, complete, consistent, and compliant with DoD and JITC policies. Reviews are based on command guidelines for content, traceability and coverage (of joint requirements), rigor in T&E approach, clarity of information, grammar, and formatting. Quality Reviews are conducted as part of the formal review (staffing) process established for T&E products. Quality Reviews start after products are reviewed by the owning Branch Chief and are completed before products are approved for official release (i.e., before ERD).

For systems on the CWL, the following products require a Quality Review:

- Joint Interoperability Evaluation Plans (JIEPs)
- Interoperability Test Plans
- Test Support Packages
- Test Reports (when generated)
- Joint Interoperability Certifications (includes certifications with conditions)
- Joint Interoperability Assessments
- Standards Conformance and Compliance Certifications
- Denials of Certification
- Others if directed by Technical Advisor

Other T&E products can be submitted for a courtesy Quality Review. These reviews will be conducted when time and resources are available. Examples of products submitted for courtesy Quality Reviews include:

- Joint IOP T&E products for systems not on CWL (plans, certifications, etc.)
- Quick Look Reports

C6.3.3 **Quality Audit.** Quality Audits are independent reviews of JITC's T&E products conducted by JT4A after they are distributed via the ERD to intended recipients. Quality Audits are performed on specific T&E products generated for non-CWL systems and CWL-Exempt products. The audits serve as a quality check of T&E products not subject to a Quality Review. JT4A will randomly select products from each test division to be audited. The Quality Audits use the same guidelines as the Quality Reviews for CWL products stated in the previous section. Audit results will be provided to the test divisions and made available to the Command Staff for feedback and action as appropriate.

Joint IOP T&E products subject to a Quality Audit:

- Test Plans and Reports (when generated)
- Joint Interoperability Certifications (includes certifications with conditions)
- Products as directed by the Technical Advisor

C6.3.4 **Commander's Watch List Review Exemption**

Selected JITC products determined to be "low risk" may be "exempt" from the CWL reviews (referred to as CWL-Exempt). This means JT4A reviewed the requirements, test methodology, tools, and sample certification letter and determined this specific type of product has a low risk of having administrative and content errors and is not required to go through the CWL formal review process.

UC products on the CWL are exempt from the CWL review requirements (i.e., Command and Quality Reviews). The UC products will be reviewed using the non-CWL process. The exemption status can be removed if conditions or circumstances for T&E change (e.g., revised

requirements or test procedures), products are assessed as being sub-standard, or if an item is of particularly high interest/visibility to the Commander. The UC products will follow the established CWL review process if the exemption status is removed.

A list of CWL exempt products is available in the STP Insert Document Tracking page.

C6.3.5 **Operational Test and Evaluation.** JITC serves as the OTA for many systems. Quality Reviews are required for select OT&E products. Refer to the Operational Test and Evaluation Guidebook posted on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad.

C6.4 **Document Staffing, Distribution, and Archiving Tools.** JITC IOP T&E products go through a formal review process to ensure they are complete and correct. The final products are then officially distributed. As shown in Figure 6-2, there are multiple tools used to facilitate processing, storing, and distribution of the joint IOP T&E products. These tools serve to notify intended reviewers that a product is available for review, provide a mechanism to route the product, and store record copies for reviewers through final organizational release. After release, JITC products are maintained in a repository for many reasons, to include:

- Ease of finding and sharing of information.
- Reference for future informed decisions.
- Authoritative and authentic information that can be trusted.
- Readily available information for reuse.
- Serving as proof of record of decisions and actions taken in the event of legal challenges.

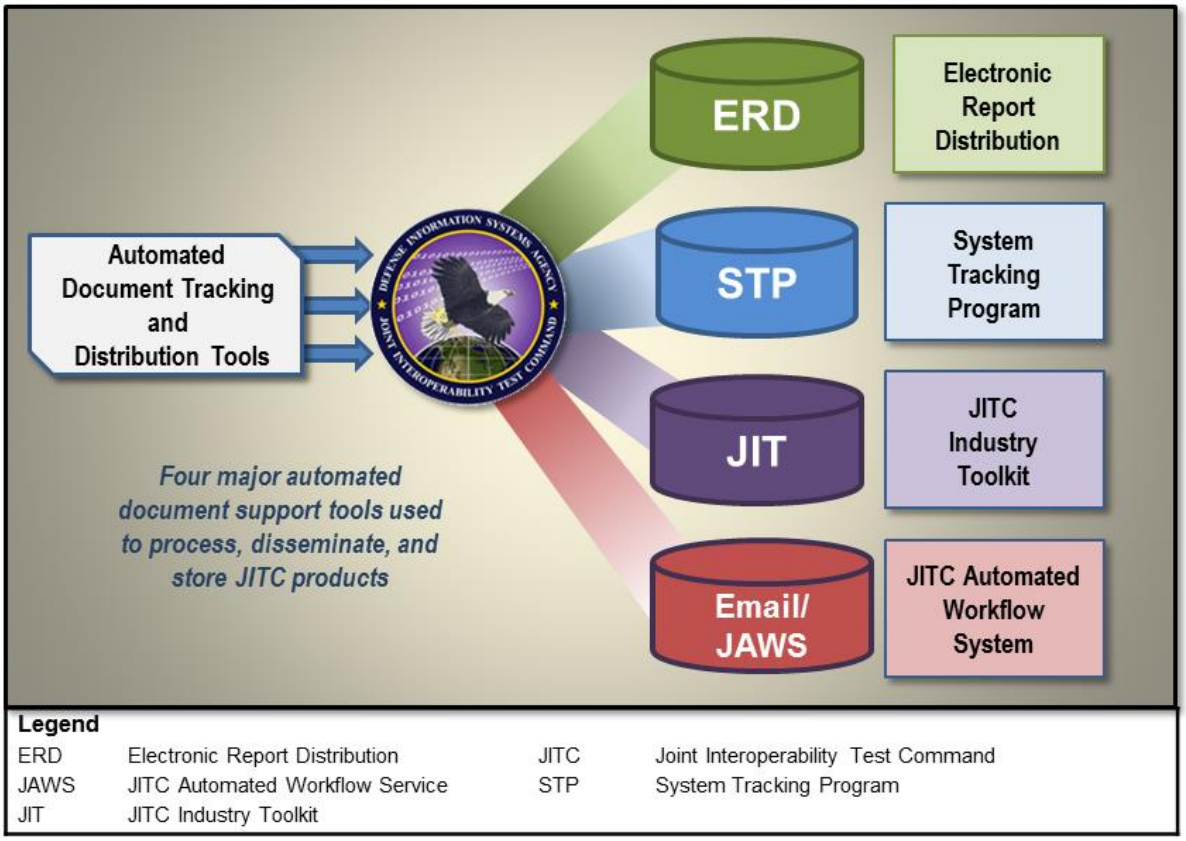



**Figure 6-2. Document Management Toolsets**

C6.4.1 **Email.** The e-Form 9 is a PDF soft copy of the paper Form 9 that JITC uses in internal document routing (aka via email) for review and approval. The required product reviewers (recipients) are determined by the associated system's CWL or Non-CWL status. Products associated with a CWL system warrant review by recipients outside the division level, to include JT4A, Technical Advisor, and, when necessary, the Commander.

C.6.4.2 **JITC Automated Workflow Service.** As an alternative to email, JAWS can be used for internal document review, tracking, routing, and approval/concurrence. JAWS automates the product review process. It automates notification to review alerts and hands off review responsibility to the next reviewer. Click on https://jitcnet.fhu.disa.mil/scripts/dr/pageDirectory.asp to access this tool. Click on https://jitcnet.fhu.disa.mil/scripts/dr/pageHelp.asp for instructions and help files on its use.

C6.4.3 **Electronic Report Distribution.** The ERD tool automates and standardizes the process of delivering formal products to internal and external recipients. The ERD tool also generates a record of products released to include when it was distributed and to whom it was addressed. It is the command's only authorized system for distributing approved final documentation. Click on https://jit.fhu.disa.mil/tools/erd/index.aspx to access this tool.

JT4A conducts a final check for all joint interoperability and standards certifications submitted to the ERD, with the exception of UC certifications, to verify specific administrative information, such as the document is signed, the correct version is uploaded for distribution, a certified NR KPP exists for JICs, and that STP metadata is accurate. After a product is released for distribution, the ERD tool generates an email with the product attached, the location of the product on the JITC's online Electronic Report Library, and the testing agent information. The email is addressed according to the interoperability and standards conformance core distribution lists, as applicable, and the AO-generated recipients list. A copy of the product is placed on the JIT for reference, and the official record copy is filed on the STP. Classified documents or documents with special handling (i.e., proprietary and For Official Use Only (FOUO)) are not emailed via ERD. Instead, a special processing procedure is used where a placeholder attachment is sent (i.e., cleared for open release) to notify recipients with access instructions.

C6.4.4 **System Tracking Program.** The STP is JITC's web database that tracks a system's progress toward joint or combined interoperability certification. The STP also serves as the command's authoritative database repository for joint interoperability T&E products.

STP is used to track the lifecycle of IT/NSS from requirements document validation to testing to certification status. It provides access to system, testing, and interoperability certification information, to include direct links to certification letters and test reports. STP also provides user-friendly custom and standard report/query generation and printing. Located on the NIPRNet, this unclassified database is mirrored on the SIPRNet. Access to STP requires a user account and Common Access Card (CAC) authorization. Click on https://stp.fhu.disa.mil/ for instructions/help and to access STP.

C6.4.5 **JITC Industry Toolkit.** The JIT is a web-based set of JITC tools used to quickly access JITC products distributed by the ERD. Click on https://jit.fhu.disa.mil/index.aspx to access this tool. Click on http://jitc.fhu.disa.mil/organization/serviceCatalog/tools/index.aspx for JIT access instructions.

## C6.5 Summary of Tools Supporting Joint IOP T&E

- Email (Electronic Mail)
  - E-Form 9
- GTG-F (Global Information Grid Technical Guidance Federation)
  - IAM (Interoperability and Supportability Assessment Module)
  - PM-P (Program Management Portal)
  - DISR (DoD IT Standards Registry)
  - GTP (GIG Technical Profiles)
- JAWS (JITC Automated Workflow Service)
- JDMT (JITC Data Management Tool)
- JIST (JITC Information Sharing Tool)
- JIT (JITC Industry Toolkit)
- J-RAD (JITC Risk Assessment Database)
- KM/DS (Knowledge Management/Decision Support)

- SharePoint (web portal for Knowledge Management) – JT4A SharePoint (https://disa.deps.mil/org/JT4/JT4A/default.aspx) website
- STP (System Tracking Program)
- Repositories (local networked shared drives)

External repositories for requirements, standards, status, and other information used during the joint IOP T&E process:

- AFAR (Air Force Architecture Resource)
- ArCADIE (Army Capability Architecture Development and Integration Environment)
- DITPR (DoD Information Technology Portfolio Repository) *****
- MARS (Marine Corps Architecture Registry Service)
- NEAR (Naval Enterprise Architecture Repository)
- SADIE (SYSCOM Architecture Development & Integration Environment)
- WMA-AFIP (Warfighter Mission Area Architecture Federation and Integration Portal)

***** The DITPR is a DoD-level tool used for maintaining DoD compliance with Clinger-Cohen management and reporting requirements. DITPR is located online at https://ditpr.dod.mil/. DITPR is an important resource for the following functions:

- Understanding how systems relate to each other from a programmatic perspective. (What is a subsystem of something else? Where does one system stop and another begin?)
- A source for information such as the system ACAT level.
- A record of determinations that have been made, or of PMO/Sponsor intentions regarding any requirement to perform interoperability testing and certification.
- Being able to properly answer the mail when JITC is asked about the interoperability status of a system by outside agencies viewing it from the perspective of how it is defined in DITPR. Being aware of the differences in system definitions is especially important when a program may be defined as several systems in STP. (There are also cases where STP will have a smaller number of more inclusive entries than the same topics in DITPR.)

System DITPR identification and related information, such as ACAT level, are recorded in STP to provide traceability between STP and DITPR. STP and DITPR identification numbers, when available, are referenced in JITC certifications.

(This page intentionally left blank)

# C7. CHAPTER 7. STANDARDS CONFORMANCE CERTIFICATION PROCESS

C7.1 **Standards Conformance Certification Overview.** DoD Instruction 8310.01 defines IT standards policy as shown in Figure 7-1. It identifies DISA as the DoD Executive Agent responsible for identifying and proposing DoD IT standards. Further, JITC is the organization responsible for carrying out standards implementation and compliance verification as an integral part of the overall IT/NSS interoperability process.

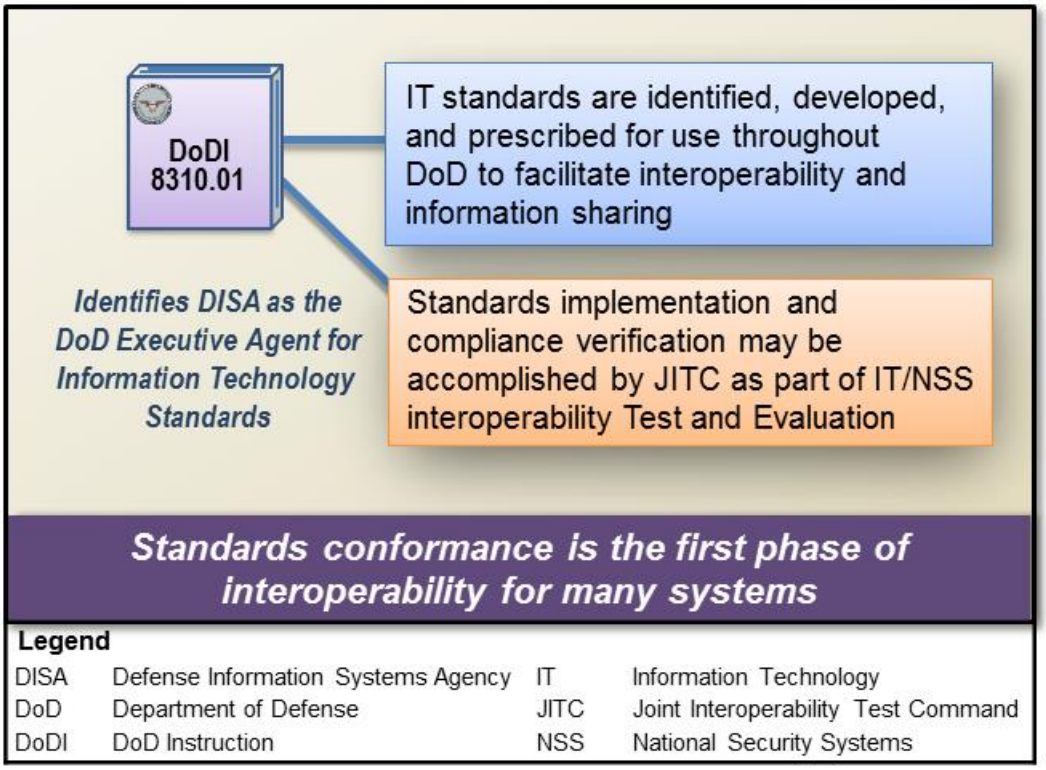



**Figure 7-1. DoD Standards Policy**

The DoDI 8310.01 requires IT standards and standard profiles be identified, developed, and prescribed to promote interoperability, information sharing, reuse, portability, and cybersecurity within the DoD, as well as with federal agencies and multinational partners.

Since standards conformance is the first step of interoperability for many systems, the AO must consider various factors when determining where standards conformance certification is required and decide what actions are needed to verify, through testing, its proper implementation. While standards conformance promotes interoperability, it is not sufficient to ensure interoperability.

This chapter reviews what is meant by certification, reviews the differences between standards conformance and standards compliance, identifies the various reporting products used by JITC, and recaps the resources available to JITC personnel to research and select a particular standard or set of standards appropriate for testing a particular system. Figure 7-2 defines some key standards terms of concern to JITC testers.

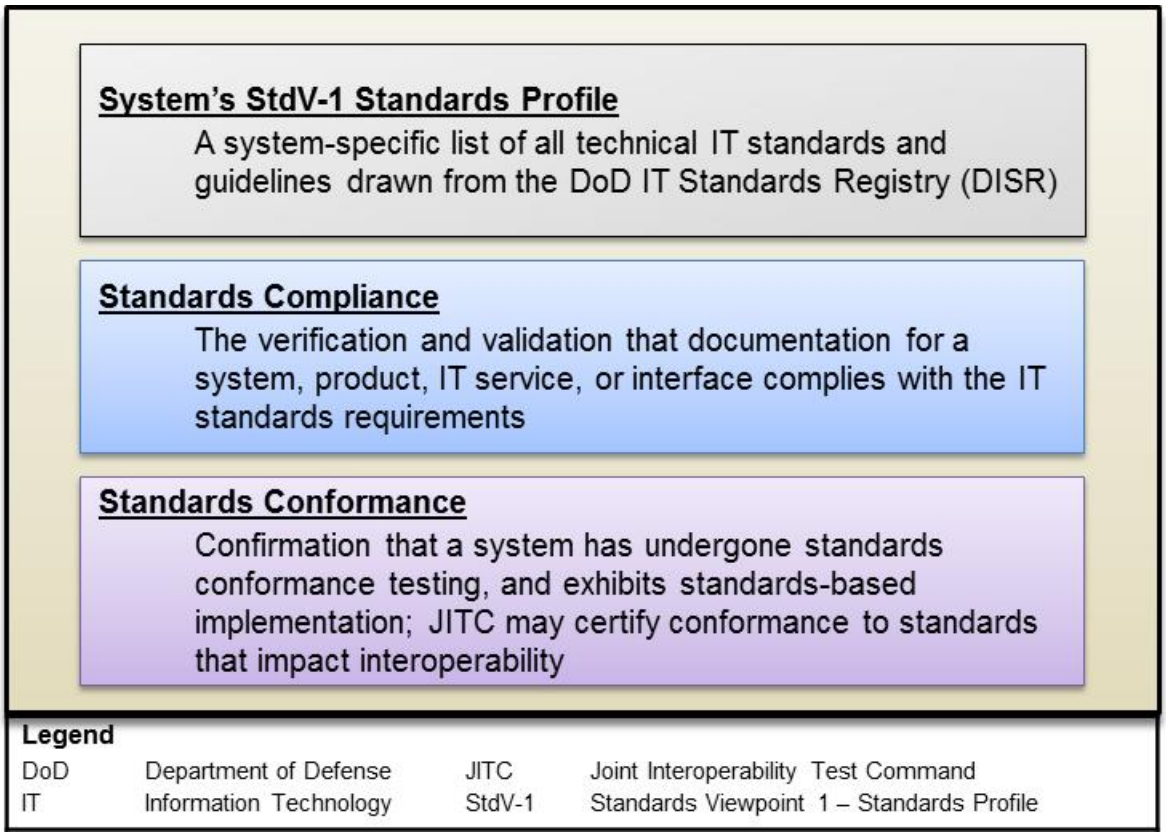



**Figure 7-2. Key Standards Terms**

C7.2 **Characteristics of Standards Conformance and Standards Compliance Testing.** Standards conformance and compliance testing may be conducted as part of interoperability T&E to affirm standards described in system documentation and architectures meet interoperability requirements.

Standards conformance testing programs have formal standards/standards profiles, a documented testing methodology, validated test suites and tools, and implementation conformance statements and associated reports. Standards conformance discrepancy reports associated with individual protocol elements may be generated at some point in the evaluation process. If test cases are not detailed enough to provide test coverage at the level of protocol elements, then testing is probably not sufficient for determining standards conformance.

Standards compliance test activities, on the other hand, are often limited in scope and may not examine all protocol items nor test each one for specific values and boundary conditions. Test parameters may vary as to minimum and maximum values or length of data, as

well as weigh any use of invalid data to determine if behavior under error conditions is correct. Further, testing that involves sending a message and verifying its receipt without examining the data content would preferably be reported in an interoperability assessment or standards compliance letter rather than a standards conformance certification.

C7.3 **Standards Policy.** DoD-approved and adopted standards are required for all new IT systems and for changes to fielded IT systems to promote interoperability. The DISR lists DoD-approved IT standards.

DISA operates and maintains the DISR, which consists of approved IT standards, technical guidance resources, and standards profiles to support programs. The PMO/Sponsor uses the DISR in developing interoperable IT capabilities and products. The resulting StdV-1 Standards Profile forms the actual basis for determining what technical standards must be successfully implemented when evaluating a particular system.

Many acquisition programs and network authorities require standards conformance certifications before issuing an approval to connect. This requirement is explicitly called out in many commercial and DoD development and acquisition instructions. Standards conformance certifications are also required by vendors seeking to sell technology, such as a tactical switch or radios, to North Atlantic Treaty Organization (NATO) countries where conformance must be certified using standardization agreements (STANAGs) as the basis for verifying technical interoperability.

JITC performs standards conformance testing and certification to determine whether a system or system component conforms to a specific standard/standards profile that could possibly affect interoperability. Conformance testing may be conducted by JITC, other test organizations, or a combination thereof. Also, tests may involve U.S. or non-U.S. equipment; both are eligible for a standards conformance certification.

In practice, the AO will confirm that test documentation and requirements associated with a system identify specific IT standards/standards profiles (DISR mandates) required for IT standards compliance. The AO must detail JITC-approved standards conformance testing events and procedures in interoperability test plans and, subsequently, verify IT/NSS conformance with the particular DISR-cited standards during interoperability testing.

The DoD IT military standards (MIL-STDs) and military specifications cited in the DISR can be reviewed in the Defense Standardization Program (DSP) Acquisition Streamlining and Standardization Information System (ASSIST) database.

C7.3.1 **DoD IT Standards Registry.** The DISR is a DoD registry of standards and standards profiles for IT/NSS systems. See Figure 7-3 below.

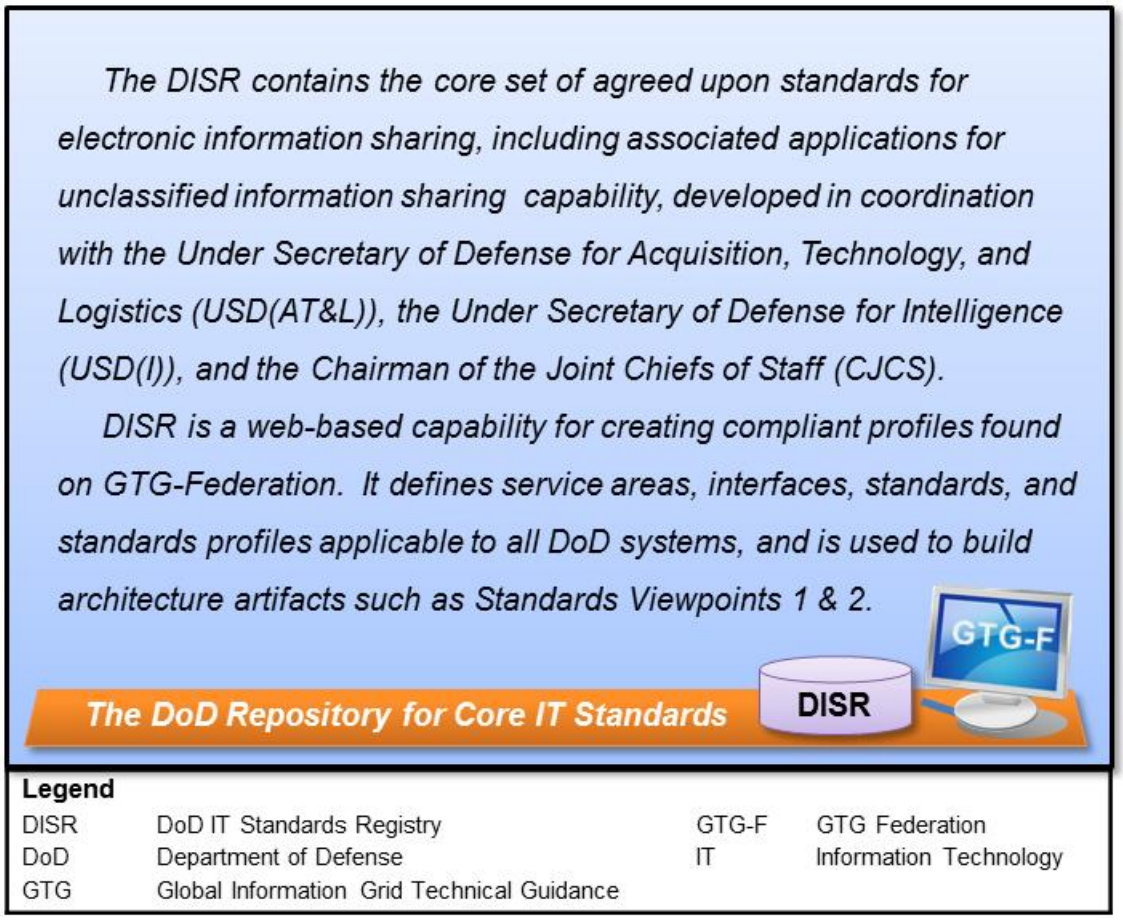



**Figure 7-3. DoD IT Standards Registry**

DISR does not contain standards. Rather, it defines the service areas, interfaces, standards (the DISR registry elements), and standards profiles applicable to DoD systems. Use of the registry is mandated for the development and acquisition of new or modified fielded IT systems throughout DoD.

The Joint Enterprise Standards Committee (JESC) maintains and populates the DISR. JESC replaced the Information Technology Standards Committee (ITSC) for adjudicating IT standards issues and publishing a baseline of Emerging and Mandated IT standards for DoD. The JESC provides close coordination with the Intelligence Community which results in a single standards baseline. DoD Instruction 8310.01, "Information Technology Standards in the DoD," codifies specific authorities, roles, and responsibilities.

DISR-related information can be found on the GTG-F online portal (https://gtg.csd.disa.mil). The GTG-F is a DISA web-based toolset that includes support for standards processes. GTG-F tool capabilities and GIG Technical Profiles are used to identify DISR standards and to develop and publish StdV-1 and StdV-2 for a program's solution architecture.

C7.3.2 **JITC Risk Assessment Database.** A complementary tool to DISR is the J-RAD, a JITC risk analysis tool for researching, determining, and analyzing standards and their associated risks, as depicted in Figure 7-4. In fact, conformance testing is focused on high-risk standards. This is why AOs estimate the value of risk factors for standards implementations in context with the system under test. It also enables test teams to identify known issues and consider the potential implications for system failure and the impact of failure.

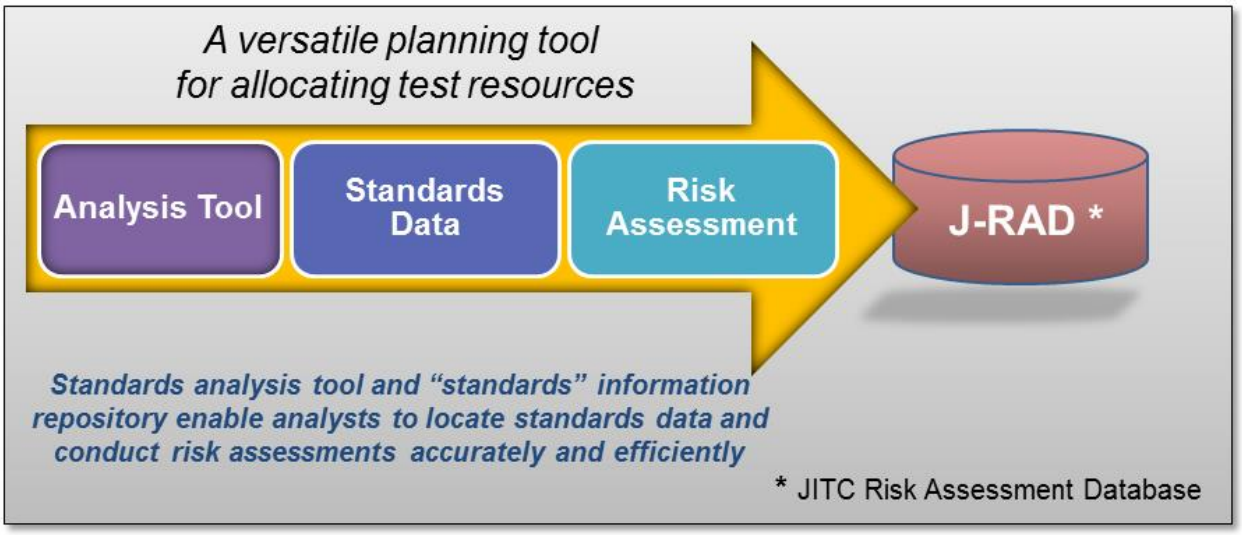



**Figure 7-4. A Tool to Research and Analyze Standards and Risks**

The AO can use J-RAD, in conjunction with the OV-3 and SV-6, to identify high-risk standards for specific conformance test planning. J-RAD enables analysts to locate standards data and conduct risk assessments accurately and efficiently. It serves as a standards analysis tool and an unclassified standards information repository built on a Microsoft Access database.

C7.3.3 **JITC Standards Research (JSR) Team.** The JSR Team was formed in response to inconsistencies across the command in determining risk level for standards. Today, the JSR Team maintains the J-RAD to provide IT standards testing information to PMOs/Sponsors and JITC personnel to support interoperability testing and certification efforts. Figure 7-5 illustrates the services provided by the J-RAD Team.

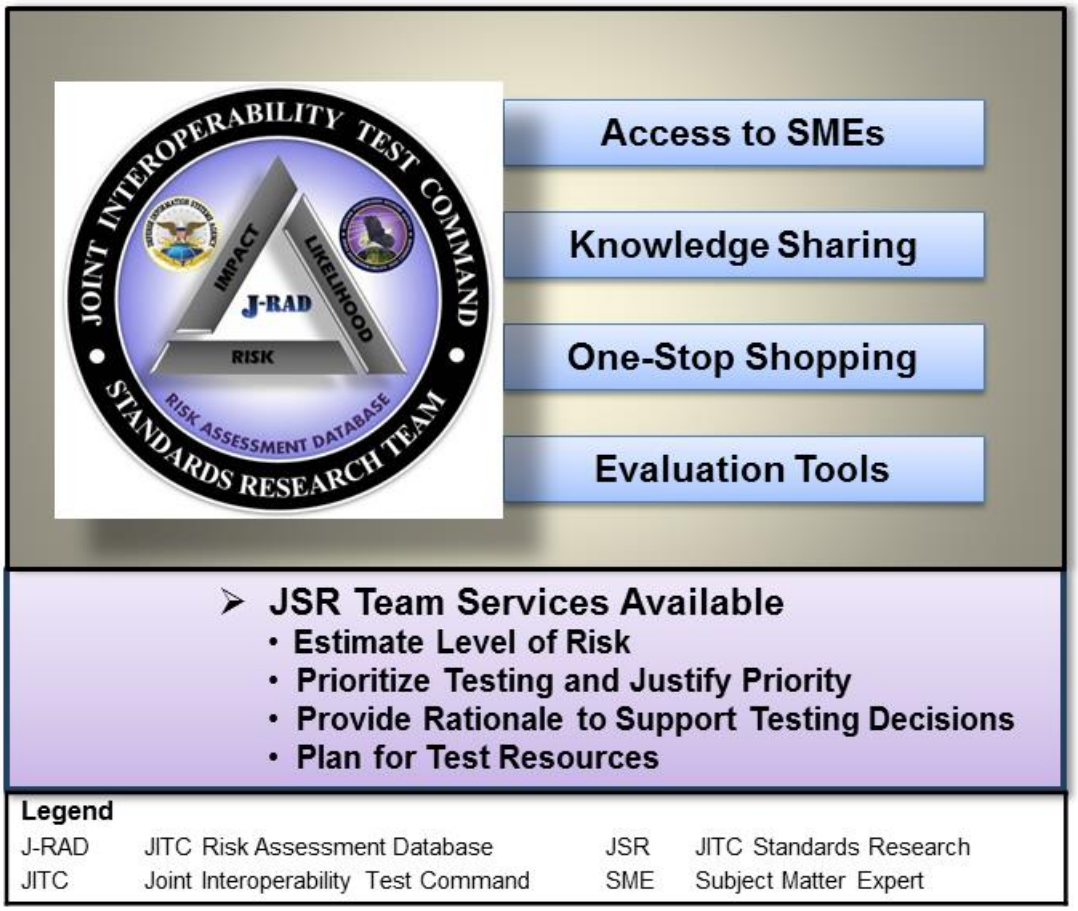



**Figure 7-5. JITC JSR Team Supports Standards and Risk Assessment**

In the event the tester elects not to use the self-service J-RAD or their risk assessment is complicated, the tester can submit a full-service request to the JSR Team. The full-service support offers the added benefit of dedicated assistance to the tester throughout the risk assessment process. For additional details, refer to http://jitc.fhu.disa.mil/projects/jsr/index.aspx.

C7.4 **Sources of Standards.** Within both industry and government, the authority to issue a standard normally derives from the various U.S. and international standards bodies. With potentially hundreds of standards to select from, they are usually grouped by priority.

- The first priority is given to treaty-based standards. The NATO STANAGs are prime examples.
- The second priority usually encompasses the International Non-Governmental Standards with the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunication Union (ITU), and European Telecommunications Standards Institute (ETSI).
- Third priority goes to the U.S. National Consensus Standards with examples such as the American National Standards Institute (ANSI) and Institute of Electrical and

Electronics Engineers (IEEE) (essentially all of the professional societies fall under ANSI).

- The fourth priority consists of the technical consortia such as the Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Organization for the Advancement of Structured Information Standards (OASIS), and Object Management Group (OMG).
- Remaining categories are typically combined to make a "military unique" grouping.

In practical terms, the standards groups of primary interest to JITC are the military unique standards, MIL-STD and STANAG, plus those listed below.

- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- National Institute of Standards and Technology (NIST)
- European Telecommunications Standards Institute (ETSI)
- Organization for the Advancement of Structured Information Standards (OASIS)

Figure 7-6 depicts an overview of the major standards organizations.

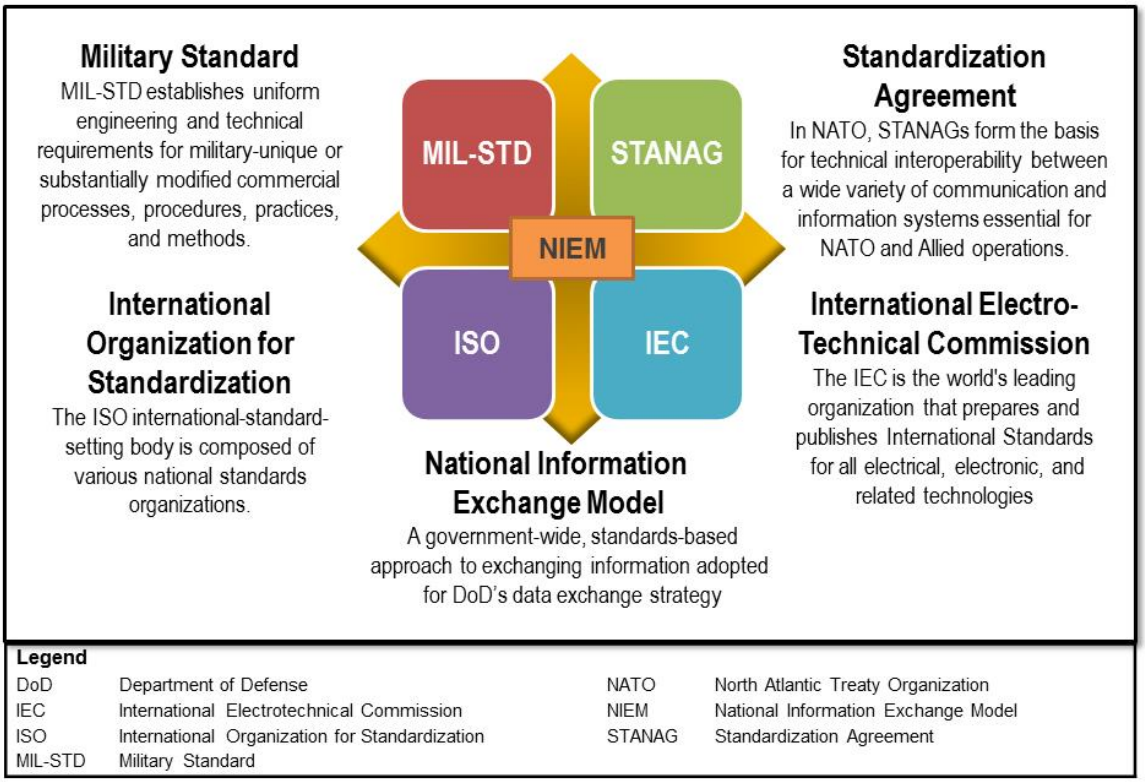



**Figure 7-6. Major Standards Organizations**

C7.5 **National Information Exchange Model (NIEM).** NIEM is a government-wide, standards-based approach to exchanging information. It provides a baseline for creating information exchanges so the sender and receiver of information share a common, unambiguous meaning across various communities, thus allowing interoperability.

NIEM consists of content, guidance, and tools that are part of a national effort to transition current data exchange standards, specifications, and policies to a NIEM standards-based framework for sharing information. It directly supports the DoD data strategy, the Joint Information Environment (JIE), and emerging government data sharing guidance.

DoD organizations first consider NIEM for their information sharing solutions when deciding which data exchange standards or specifications meet their mission and operational needs. The "NIEM First" policy applies when organizations are developing a new information exchange requirement or working an update to an existing information exchange. This means that NIEM is considered "first" for every new and modified data exchange. It does not mean that NIEM is always used. Nor does it require reworking existing data exchanges to make them use NIEM. The AO should consider this when reviewing standards information in requirements.

C7.6 **Reporting Test Results.** Standards conformance testing programs serve as a foundation for overall joint interoperability evaluation and should be conducted prior to joint interoperability testing. The PMO/Sponsor should coordinate with the JITC AO during the planning of standards conformance testing to ensure interoperability evaluation needs are adequately addressed. This will allow the AO to leverage planned testing for the system's JIC process and minimize additional testing. Figure 7-7 depicts the overall standards certification process.

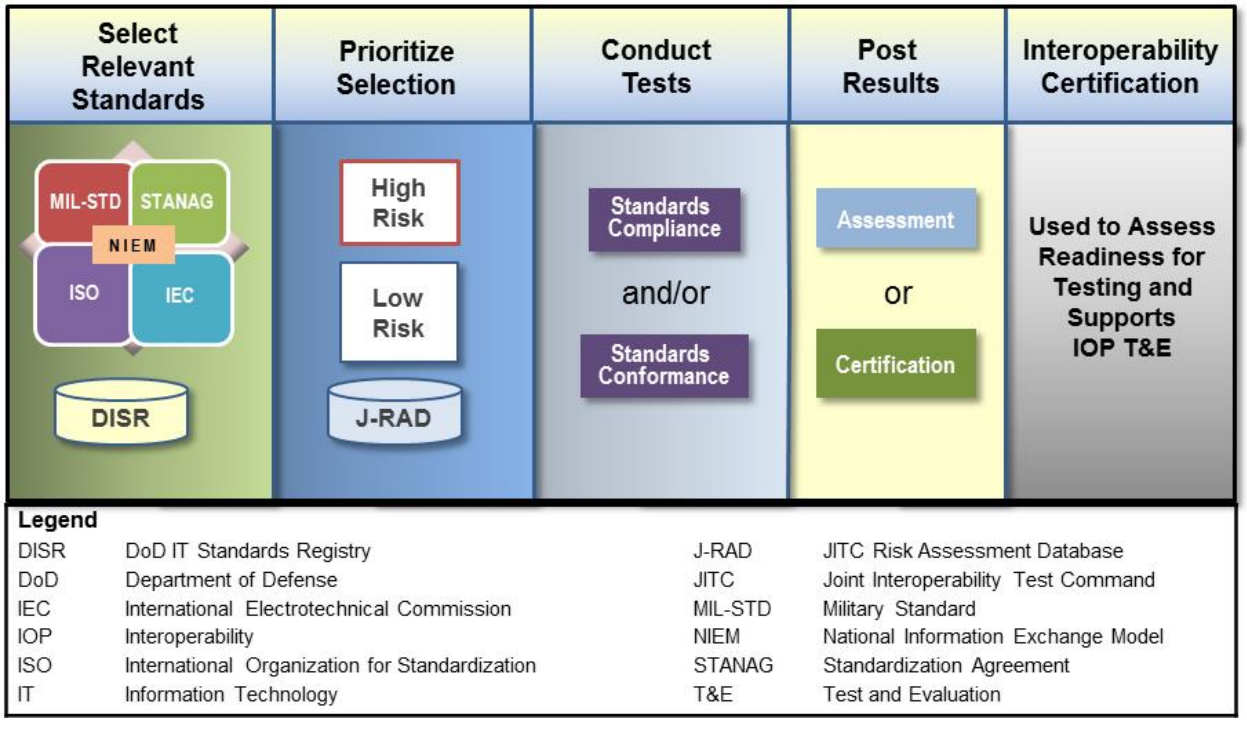



**Figure 7-7. Standards Certification Process**

Results of standards certification testing are evaluated on a pass/fail basis. Successful testing usually leads to formal standards conformance or compliance certification, which is reported via a memorandum or a commercial letter if a vendor is involved. Locally, the AO posts test results on the STP (via the ERD/STP processes).

Standards certifications must be based on testing that covers all protocol elements or other specified requirements. Standards conformance certification means that all mandatory items, and all implemented optional items, are correctly supported.

DoD Components are required to assess systems standards compliance requirements as a part of the ISP review and approval process. To promote interoperability, PMOs/Sponsors must use the applicable IT standards in the DISR. AOs can expect to receive DoDAF-compliant standards viewpoint data, along with appropriate systems and services viewpoint data to show where these standards are used. If significant negative impacts to cost, schedule, performance, or cybersecurity are identified, a system PMO/Sponsor may submit a waiver request to use other than DISR designated "active" standards.

JITC maintains repositories for standards conformance testing performed by JITC. With appropriate coordination, standards conformance test products may be shared with other organizations.

Common issues associated with standards evaluation include lack of formal methodology and accepting results from external sources. For example, standards conformance testing requires a formal methodology. Use the ISO/IEC 9646 standard as the basis for determining appropriate local processes. In addition, AOs need to ensure results received from external sources are valid and sufficient to issue a standards conformance certification. For example, vendor provided self-certification results may lack adequacy or validated data.

With complex standards, full (100 percent) conformance to all specifications in the standard is rarely obtained; therefore, reports may quantify results when a system is less than fully conformant. Reports should consider implementation requirements (mandatory items) and criticality when available. Assessments with little analytical detail, application of less stringent rules for passing, or that allow numerous non-conformance issues should be documented in something other than a conformance certification, using instead a conformance assessment or compliance letter.

For further information regarding Standards Conformance Policy, refer to the JITC IPG. Additional information on JITC standards capabilities can be found at http://jitc.fhu.disa.mil/organization/serviceCatalog/services/complyConform/index.aspx

C7.7 **Standards Conformance Testing Products.** Standards conformance test results may be documented in several different formats depending on the scope and nature of the test. The following paragraphs discuss these types of reports in greater detail.

C7.7.1 **Standards Conformance Certification.** Standards conformance certification occurs through testing to confirm that a product or system adheres to a defined standard, standards profile, or specification. Standards conformance testing typically occurs very early in the development process. Although such testing represents an important first step toward establishing an interoperability status, it is not sufficient by itself to support a fielding decision. Additional testing may be required to determine conformance with multi-standard profiles or compliance with other technical requirements mandated by policy or procedure.

Standards conformance certifications are issued at the conclusion of technical testing against a published standard, standards profile, or specification that describes the degree of conformance attained. A system's standards profile must be monitored throughout its lifecycle since system updates or requirements changes may impact system status.

C7.7.2 **Standards Conformance Assessment.** Conformance assessments may be issued following technical testing against standards/standards profiles/specifications to describe the degree of conformance when a standards conformance certification is not appropriate.

C7.8 **Standards Compliance Products**

C7.8.1 **Standards Compliance Certification.** A standards compliance certification is conveyed through a memorandum or commercial letter. Compliance certification indicates an implementation complies with the set of standards/standards profiles required, rather than strictly conforming to specific items in a standard. The certification must clearly identify what is meant by compliance, either directly or by reference to testing methodology documentation. Compliance may be verified through analysis, inspection, demonstration, or testing. Test results may reflect data obtained from multiple sources.

C7.8.2 **Standards Compliance Assessment.** Compliance assessments document test results when a formal certification cannot be justified (for example, where analysis detail is insufficient).

# C8. CHAPTER 8. UNIFIED CAPABILITIES PROCESSES

C8.1 **DoD Approval to Use Commercial Technology.** Unified Capabilities (UC) policy establishes a process to leverage commercial-off-the-shelf (COTS) technology to meet DoD's mission requirements. UC are defined as the integration of voice, video, and data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities (includes equipment and software).

DoDI 8100.04 is the overarching policy covering UC product certification, supplemented by the UC Approved Products List (APL) Process Guide. The DoD UC Requirements (UCR) specifies functional requirements, performance objectives, and technical specifications for certification of products to be used in DoD networks. The UCR provides UC products' features, standards, and requirements to support DoD mission-critical needs, to include test, certification, acquisition, connection, and operation of these devices.

DISA maintains the DoD UC APL, a list of products that have been certified for interoperability and cybersecurity and are approved to be acquired or operated by DoD Components. The APL represents the products recommended for use by all military services and defense agencies to acquire communications and information technology equipment approved for connection to the DoD Information Network (DoDIN). DoD Components are encouraged to use UC-certified products in developing acquisition programs. See DoDI 8100.04 and DoDI 5000.02 for additional guidance.

JITC plays a key role in this process, as JITC is the sole interoperability certifier for UC APL products and services.

C8.2 **Unified Capabilities Distributed Testing.** Within DISA, the Unified Capabilities Certification Office (UCCO) manages the UC Distributed Testing and Certification Process. DISA/JITC uses its distributed test capability for testing and certification of voice, video, and data products to evaluate the UCR. Refer to the JITC Service catalog for additional information regarding UCR test capabilities.

JITC certification enables a commercial vendor to have its UC products placed on the DoD UC APL. In practice, products may be tested via multi-vendor test events, demonstrated via conduct of enterprise product solutions at DoD test laboratories, or implemented using planned UC pilot T&E activities. In addition to in-house facilities, the distributed test sites most often used by JITC are those operated by the Services' major test organizations. These are the Army Information Systems Engineering Command – Technical Integration Center (ISEC-TIC), the Space and Naval Warfare Systems Command (SPAWAR) Systems Center – Atlantic, and the Air Force's 677th Cyberspace Wing.

JITC collaborates with all parties concerned to analyze interoperability test results and provides appropriate certification recommendations for individual UC products seeking to attain DoD UC APL status. The DoD CIO makes the final decision for certification and placement of the UC product on the APL taking into consideration DISA and JITC recommendations.

C8.3 **Strategy for Acquiring Unified Capabilities and Support Services.** Typically, the DoD sponsor works closely with the vendor (product or service provider) to ensure the test submittal application is completed properly, with the appropriate interoperability and cybersecurity information, and is submitted to the UCCO. Any DoD Component user of the DoDIN with acquisition or management-level responsibilities of equipment can sponsor a product for testing.

The UCCO manages the DoD UC APL process. This process covers both mature products (APL and post-APL) and technology insertion products that are evaluated via assessment testing in DoD test laboratories and validated for deployment.

Subsequently, the UCCO routes tasking to the designated JITC Division (JTE – Networks/Communications and UC Division) to initiate formal commercial product evaluation. The JITC Strategy and Policy Branch (JT4A) oversees and manages the certification and test product review process. The internal JITC review processes and UC procedures are detailed in the JITC NR KPP Evaluation Guidebook, JITC UC Processes, and can be accessed on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad.

# C9. CHAPTER 9. INTERIM CERTIFICATE TO OPERATE (ICTO)

C9.1 **ICTO Overview.** An ICTO permits a system to be fielded for operational use without a JIC. This is a temporary authorization, normally up to one year. An ICTO is the authority to allow operational use while the PMO/Sponsor continues to pursue JIC.

JITC AOs play a key role in this process. Requests for ICTOs must be submitted and processed in accordance with the JITC IPG and additional instructions that may be found on the ISG Resource website, http://jitc.fhu.disa.mil/projects/isgsite/index.aspx.

C9.2 **ICTO Approval Guidelines.** The basic criterion for pursuing an ICTO requires one of two conditions. The operational chain of command and the Joint Staff have validated an urgent operational need requiring fielding of the system prior to JIC. Or, an ICTO may be granted in the event JITC or other DoD Component test laboratories have been unable to assess all joint critical requirements for the system undergoing joint interoperability evaluation. In either case, the system PMO/Sponsor must engage with JITC and pursue full JIC.

C9.3 **ICTO Approval Process.** The ISG members vote to approve or disapprove the ICTO, having taken JITC's recommendation into consideration. The DoD CIO has the final authority to grant an ICTO.

C9.4 **JITC's ICTO Role.** The ISG Secretariat will contact the appropriate JITC Division, Branch Chief, or AO to obtain JITC's position on an ICTO request. Figure 9-1 provides an overview of the JITC review process.

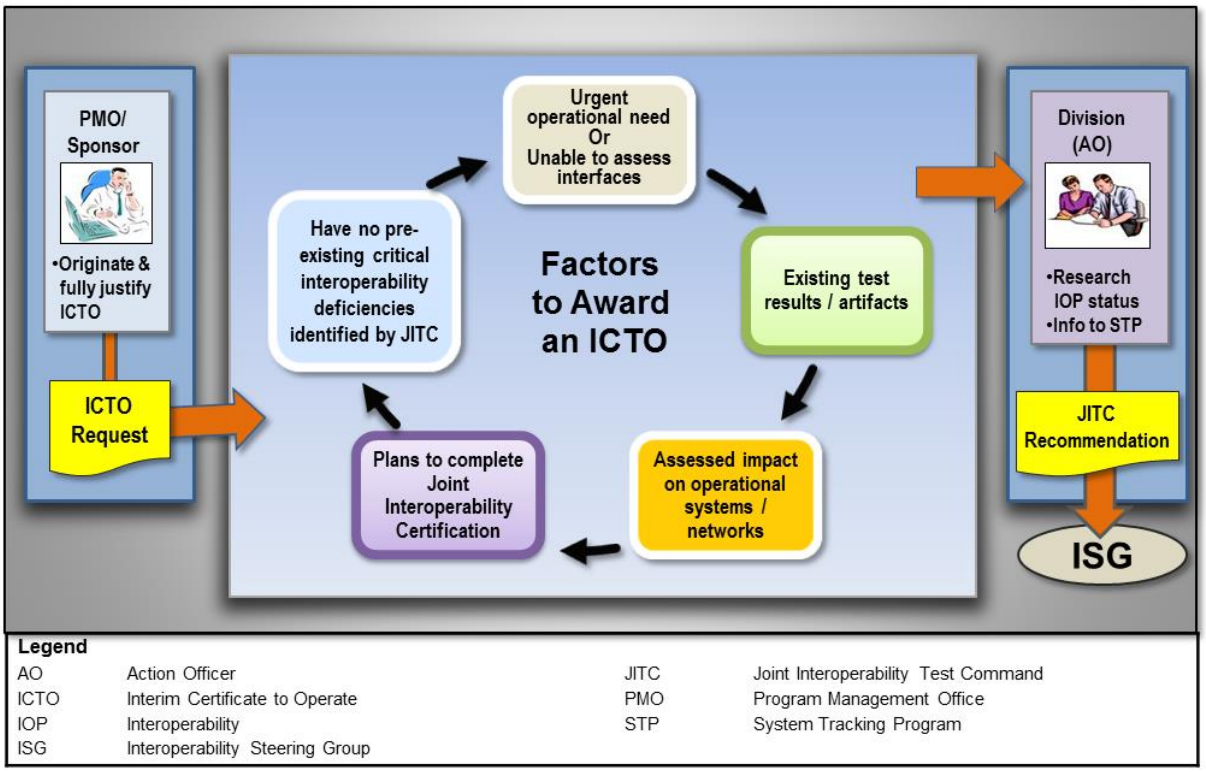



**Figure 9-1. JITC Considerations for ICTO**

The AO coordinates with their respective Branch Chief and Division Chief in determining the final JITC recommendation. The AO then notifies the ISG Secretariat. System ICTO information is also entered into the JITC STP (https://stp.fhu.disa.mil).

C9.5 **ICTO Request Procedures.** The PMO/Sponsor initiates an ICTO request using forms from the ISG Resource website (http://jitc.fhu.disa.mil/projects/isgsite/ictoreqs.aspx). Additional instructions regarding ICTO procedures, ISG meeting minutes, and ISG POCs are also located on this website. The PMO/Sponsor works with their ISG representative who, once the request is reviewed and validated, forwards the request to the JITC AO.

C9.6 **JITC ICTO Processing.** Initially, the JITC AO verifies the request has an associated STP system entry. If needed, the AO creates an entry. Next, the AO reviews the submission and begins gathering information. AO actions are conducted either In-Cycle during a scheduled ISG meeting bi-monthly (i.e., January, March, May, July, September, and November) or Out-of-Cycle (OOC) via the web-based ISG Management Console. Details are spelled out at http://jitc.fhu.disa.mil/projects/isgsite/index.aspx .

- If processed In-Cycle, the JITC AO's input is essential for the ISG voting members to determine whether or not a system obtains an ICTO during the ISG meeting. The AO should be ready to discuss the ICTO request and associated issues during the ISG meeting.

- If processed OOC, the ISG representative forwards the ICTO request through the ISG Secretariat to JITC by email via the ISG Management Console. This notification prompts the appropriate JITC AO to provide comments/recommendations. The JITC AO is required to update the five STP ICTO questions within three (3) business days. The questions are located on the "View System" page in the STP. The JITC AO's input to the STP "ISG Questions & Answers" are required before the ICTO request can be opened to ISG members for their recommendation to approve or deny the request.

- The JITC AO thoroughly researches the system interoperability status to determine if an ICTO should be recommended. The STP is a prime source used by the AO to determine previous testing and certification status. As needed, the JITC AO coordinates with other AOs if the system missions cross over to other Divisions or if additional expertise is required.

- Once the JITC "package" is assembled, including AO input and recommendation, it is submitted to the ISG representative, who forwards the annotated ICTO request to the ISG Secretariat. The ISG Secretariat may follow up with the JITC AO regarding any outstanding programmatic issues, as well as clarification of interoperability testing status or recommendations made pertaining to the ICTO request.

- JITC (under the direction of the ISG Secretariat) posts all ICTO letters (including disapproval letters) in the STP and uses it in monitoring the expiration dates. The STP automatically generates an "Expiring ICTO Alert," which provides a list of ICTOs that have expired or will expire within 90 days. This prompts dialog between the ISG Secretariat and ISG representative.

(This page intentionally left blank)

# C10. CHAPTER 10. WAIVER TO POLICY PROCESS

C10.1 **Waiver Process Overview.** Not all IT/NSS need to be tested and certified for joint interoperability. DoD policy allows systems to be granted a "Waiver to Policy" provided certain specified conditions are met.

Waivers are prescribed by guidance issued by the DoD CIO (see DoDI 8330.01 and the IPG). These documents detail policy and procedures for processing waiver requests. The documents and additional instructions may be found on the ISG Resource website, http://jitc.fhu.disa.mil/projects/isgsite/index.aspx.

JITC plays a special role in this overall waiver process. The internal JITC processes and procedures are detailed in the JITC NR KPP Evaluation Guidebook and can be accessed on the JIST (https://jitcnet.fhu.disa.mil/scripts/jist3x/index.aspx) T&E pad.

C10.2 **Waiver to Policy Criteria.** A "Waiver to Policy" is a formal action that seeks exclusion from JIC or related interoperability policy. Waivers may be either permanent or have an expiration date, at the discretion of the DoD CIO, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the DOT&E, and Chairman of the Joint Chiefs of Staff (CJCS). These waivers do not apply to other DoD CIO requirements, such as system survivability or cybersecurity. A waiver request must meet strict criteria; at least one of the three conditions shown in Figure 10-1 must be present.

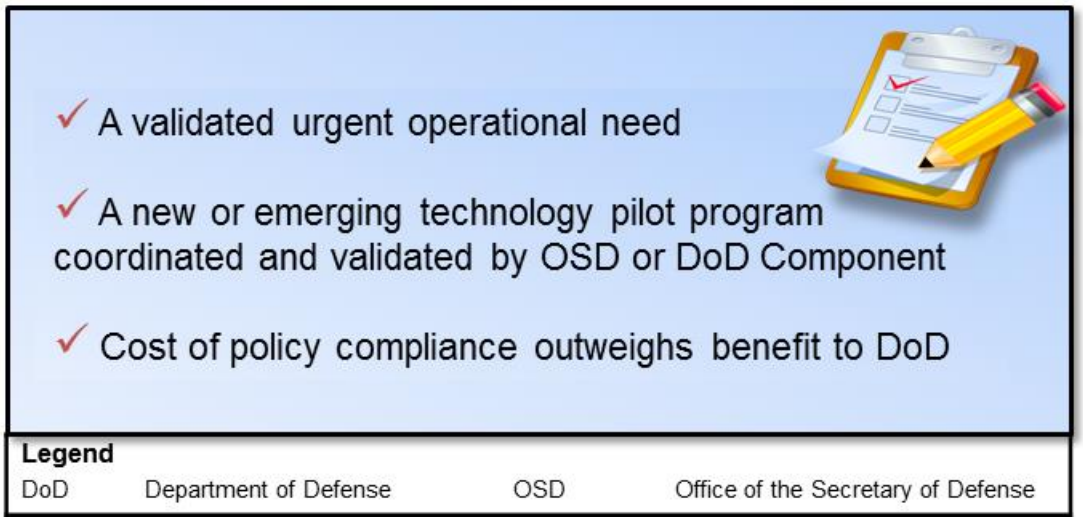



**Figure 10-1. Conditions to Grant a Waiver to Policy**

C10.3 **Waiver Request Overview.** The PMO/Sponsor is responsible to make the business case when initiating a waiver request. It is up to the PMO/Sponsor to work with their ISG Representative to determine if a Waiver to Policy is the right choice for the program/system, and that the request form is complete and valid. After favorable review by the ISG Representative, the request is forwarded to JITC for further action.

JITC reviews the request, identifying interoperability issues, if any, and then forwards the waiver request to the ISG Tri-Chair members (DoD CIO, USD(AT&L), and CJCS) with accompanying recommendation.

The DoD CIO, in coordination with USD(AT&L), DOT&E, and CJCS, evaluates the request and considers granting a Waiver to Policy. Although the ultimate decision to grant the waiver rests with the DoD CIO, this decision is weighted heavily on JITC's technical evaluation. If approved, the system is waived from the JIC requirements of the policy cited in the request.

C10.4 **JITC Internal Review.** JITC AOs play an important role throughout the waiver request process. The AO is expected to complete the review process within the allotted timeframe; typically, the assigned AO will have four (4) working days to review the draft recommendation that has been prepared by JT4A. The AO is responsible for coordinating with the PMO/Sponsor to obtain additional information, if needed, to fulfill the task. If the system spans more than one Division's area of expertise, the lead AO will coordinate with the other divisions, as appropriate.

C10.5 **Unified Capabilities Waiver Requests.** For policy information on waivers on UC components, refer to DoDI 8100.04. For additional details, refer to the UC APL Process Guide at https://aplits.disa.mil. The DISA UCCO maintains the official database used to track the status of UC waivers.