
Policy FAQ – JITC Internal v3.0a

Table of Contents

Table of Contents	1
General Information	3
Where do I start?	3
What are NSS and IT Systems?	3
What are the important terms, their formal definitions, and source?	4
What are the buzzwords, acronyms, etc? <i>(Note that in many cases these are the short, practical definitions – not the long formal ones.)</i>	4
Where do I get the basic JITC testing policy and procedures?	6
What are the basic certification processes at JITC?	6
What is a system?	7
Who do I ask about certification, document review, the STP, JIT, ERD, etc?	7
Format and Content	7
What are the most commonly made mistakes?	7
Who signs certification letters?	8
Why does the distribution list change every time I submit a cert letter? ...	9
Why is the system version information so important?	9
Who reviews certification letters?	9
How do I get JITC release authority? What are the procedures for routing the finalized cert letter after incorporating JT4 comments?	9
Related Processes	9
What is an ICTO and what role does JITC play in it?	9

Policy & Guidance	10
Who should sign the coordination sheet for a TEMP?	10
Who decides if standards selected by the Program Manager are in accordance with the DISR?	10
Who approves a program/system standards profile?	10
What is JITC's certification policy?	10
What are the major Interoperability (IOP) DoD/CJCSI directives, instructions, etc.?	10
What is in each of the major IOP DoD/CJCSI directives, instructions, etc.?	11
Where does JITC's authority as DoD's sole interoperability certifier come from?	11
When do certifications expire?	11
What is Information Interoperability?	11
Why certify for Interoperability?	12
When should systems be certified?	12
What does certification involve (i.e., what are the 4 basic steps)?	12
What are the products/actions for an interoperability evaluation?	13
What are the common problems with IOP evaluations?	13
Are there other IOP certifications that other organizations certify?	15
What if the customer wants a preliminary assessment of interoperability?	15
Can I make one call/send one message to evaluate an interface?	15
What is JITC's position on using simulators in IOP testing?	15
Must software system upgrades be fully tested?	16
What if the test environment is not "operationally realistic" – can I still certify?	16
Useful Links	16
General	16
DoD Organizations	17
DoD Info Sources (directives, reg's, etc.)	17
DoD IOP Info Sources	17
Misc Info Sources	17

Dictionary, Abbrev17

Style/Grammar (Follow these at your own risk.).....18

General Information

Where do I start?

A good place to start is to review the [JITC Action Officer's guide](#). In addition, for detailed information concerning JITC's testing process, the JITC Instruction, [380-50-02](#) is a good source of information. [However, please note that the instruction is dated and is currently being updated.] Finally, [CJCSI 6212.01](#) is the source for understanding interoperability and the NR-KPP and how JITC evaluates each element of the NR-KPP.

What are NSS and IT Systems?

From DoDD 4630.05 May 2004, an Information Technology (IT) system refers to, "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)."

From DoDD 4630.05 May 2004, a National Security System (NSS) is "Any telecommunications or information system operated by the United States Government, the function, operation, or use of which:

- Involves intelligence activities.
- Involves cryptologic activities related to national security.
- Involves command and control of military forces.
- Involves equipment that is an integral part of a weapon or weapons system.
- Is critical to the direct fulfillment of military or intelligence missions. This does not include automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance logistics, and personnel management applications)."

What are the important terms, their formal definitions, and source?

Though there is no one single document or source that defines all the appropriate terms. Policy has started a glossary that could be of help (see embedded file). In addition, you can look below in the buzzwords, acronyms section; these are the short, practical definitions, not the formal ones.



Microsoft Word
Document

What are the buzzwords, acronyms, etc? (*Note that in many cases these are the short, practical definitions – not the long formal ones.*)

ATO – *Authorization to Operate* – Information Assurance authority for a system to operate on the GIG/network, granted from the Designated Accrediting Authority (DAA).

Cert – informal abbreviation for *Certification*.

Cert Letter – generic name for a *Certification Memorandum* and associated *Certification Testing Summary* (that is more accurately an Evaluation Summary for IOP Test certs). JITC produces two main types of Cert Letters: *Joint IOP Test Cert* and *Standards Conformance Cert*.

Cert Memo – 1) the “memorandum” portion of a *Cert Letter*, or 2) another way to refer to a *Cert Letter*. [Memoranda to commercial customers take the form of a commercial letter vs memorandum.]

JT4 E-form 9 Review – group that reviews cert / assessment letters , plans and reports, etc. and provides individual comments, and assists in developing JITC testing and certification policy.

C/S/A – Command/Service/Agency.

DT – Developmental Test(ing).

ERD – *Electronic Report Distribution* – JITC system used to electronically distribute (e-mail) the final version of all JITC reports, *Cert Letters*, etc. Complete documents are stored on the *JIT and STP*; only portions of the documents (e.g., the memo portion of *Cert Letters*) are e-mailed. The ERD must be used for the formal distribution of *Cert Letters*– no ERD, no official certification! The *STP* entry must be complete before starting the ERD process.

FOS - *Family-of-Systems* – [DoD 4630 series.] A set or arrangement of independent systems that can be interconnected or related in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation.

IATO – *Interim Authorization to Operate* – A temporary waiver for Information Assurance authority for a system to operate on the GIG/network, granted from the Designated Accrediting Authority (DAA).

ICTO -- temporary waiver from interoperability system testing certification granted by the ITP.

IOP – informal abbreviation for information *Interoperability*.

Interoperability – [DoDD 4630.5] Interoperability is the ability of systems, units or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment.

NR-KPP – [defined/discussed in *CJCSI 3170.01/6212.01*] The NR-KPP is a key performance parameter stating a system's information needs, information timeliness, IA, and net-ready attributes, and standards conformance requirements. It is composed of the following elements: 1) Compliant solution architecture, to include information exchanges, 2) compliance with DOD Net-centric Data and Services strategies, including data and services exposure criteria, 3) compliance with applicable GIG Technical Direction to include DISR mandated IT Standards reflected in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Information Enterprise Architecture and solution architecture system/service views, 4) verification of compliance with DOD IA requirements, and 5) compliance with Supportability elements to include, Spectrum analysis, Selective Availability Anti-Spoofing Module (SAASM) and the Joint Tactical Radio System (JTRS).

Information Exchange Requirements define the information exchanges of a system with other systems; these are in matrix form with sending/receiving nodes, format, criticality, and other items.

ITP – *Interoperability Test Panel*. ITP grants *ICTOs*, resolves IOP testing issues; etc.

IP – *Interoperability Panel* - Chartered to review, develop, recommend, and coordinate studies, reports, and DOD policy for consideration by the Military Communications Electronics Board in the area of data systems interoperability (includes C4I systems operational architectures, operational and procedural standardization issues, and the standardization of data required for C4I information exchange).

IWL – *Interoperability Watch List* – Defined in DoDI 4630.8 & DoD Acquisition Guidebook. List of systems with significant interoperability deficiencies determined to warrant additional attention. Maintained by DOT&E. Systems are only added to the list after the ITP and MCEB fail to resolve issues. Submissions are made to the DOT&E representative of the ITP.

ITWL – *Interoperability Test Watch List (J6)* - ITP maintains an Interoperability Watch List of programs that bear special scrutiny as they progress through the Interoperability certification process.

IUT – *Item under test* - The "item" (system, unit, etc.) being evaluated for interoperability or conformance.

JCPAT-E – DISA system used to coordinate the review of requirements documents. CDDs, CPDs, ISPs, **TISPs**, **ISP Annex**, and TEMP are available on the JCPAT-E (SIPRNET access only).

OT – Operational Test(ing).

Std's – Standards, as in Standards Conformance.

STP – *System Tracking Program* - online database to track systems, testing, and certification status. System & Testing/Activity information must be in the STP before a Cert Letter is released.

System – [See: [What is a "system?"](#)] an information "system" certified by JITC is a stand-alone box with external interfaces. Another practical definition is that a "system" should have a CDD, CPD, ISP, TISP, or TEMP (older systems might have an ORD or C4ISP).

SOS - *System-of-Systems* – [DoD 4630 series.] A set or arrangement of systems that are related or interconnected to provide a given capability. The loss of any part of the system degrades the performance or capabilities of the whole.

SUT – *System Under Test* – The "system" being evaluated for interoperability or conformance.

UUT – *Unit Under Test* – The "unit" being evaluated for interoperability or conformance.

V - Version

Where do I get the basic JITC testing policy and procedures?

The basic policy and procedures can be found in the [JITC Action Officers Guide](#); for a more in-depth explanation, JITC Instruction [380-50-02](#) is recommended. [Note that the instruction is dated and being significantly changed.]

What are the basic certification processes at JITC?

JITC issues two types of certifications: *Standards Conformance* and *Interoperability Test*.

Standards Conformance Certification results from testing a system/component for compliance with standards (for information processing, content, format, or transfer). Compliance is characterized with a matrix (in the certification summary) showing whether an implementation (the hardware/software under test) meets the individual mandatory and optional requirements specified in the standard. Certification is confirmation that the system/component meets – as a minimum - all of the mandatory requirements and that there are no critical discrepancies.

Interoperability Test Certification characterizes the overall interoperability status of a system with respect to the NR-KPP/IERs and other interoperability requirements. It is confirmation by JITC that the system has undergone appropriate testing; that the applicable standards and requirements for interoperability have been met (i.e., standards conformance is a part of IOP); and that the system is ready for joint/combined/coalition use. Certifications are provided in the form of a memorandum with an interoperability status matrix, and a more detailed summary of the IOP evaluation. All JITC joint interoperability test certifications expire upon changes that may affect interoperability or four (4) years from original date of issue.

There are four different types of Joint Interoperability Test Certifications:

Special Interoperability Test Certification is issued for systems or system components that require interoperability test certification, but are not subject to the JICDS process, and generally do not need individual requirements certified by the J6 (e.g., commercial switches being procured to operate in the DSN, in-line encryption devices).

Limited Joint Interoperability Test Certification is issued when a system has adequately demonstrated interoperability for a subset of interoperability requirements (has not met all threshold requirements). A “limited” certification may not be sufficient to allow fielding; if military necessity warrants fielding of the system for the demonstrated capabilities, the system sponsor should contact the J-6 to request an approval for fielding and the MCEB/ITP for an Interim Certificate to Operate (ICTO).

Joint Interoperability Test Certification is issued when a system has adequately demonstrated interoperability for at least all critical threshold requirements pertaining to a specific increment. This system certification attests that the system’s interoperability is sufficient to support a fielding decision.

Interim Joint Interoperability Test Certification issued when a capability module, that will be fielded in an incremental fashion, has adequately demonstrated interoperability for at least all critical threshold requirements identified for the increment. This interim certification attests that the capability’s interoperability is sufficient to support a fielding decision. When the capability is fully mature and meets all critical threshold requirements for the entire module, it may qualify for a Joint Interoperability Test Certification. An Interim Joint Interoperability Test Certification expires whenever the incremental module will be replaced or revised, resulting in changes to NR KPP attributes, but no later than four years from original date of issue.

What is a system?

For practical purposes, an information "system" certified by JITC is a stand-alone box with external information interfaces. Another practical definition is that a "system" should have an CDD, CPD, ISP, TISP, or TEMP, (or ORD, C4ISP). That said, there are differences depending on the type of system. For network infrastructure certifications, it is not practical to certify every component of a large network. In this case, the "systems" certified are actually the network components, usually the equipment at nodes (e.g., switches, routers). However, these components should themselves be stand-alone – don't certify a card for a switch; rather, recertify the switch with additional functionality/interfaces. Platform (e.g., F-15) certifications usually fall in the category of FoS/SoS, meaning they host a number of "systems," each of which could have multiple external interfaces.

Formal definition from *Joint Pub 1-02*: **system**—Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

Who do I ask about certification, document review, the STP, JIT, ERD, etc?

The [JITCNet](#) is one source for POCs. Of particular interest on this web site will be the list of POCs for general guidance, plans & reports, requirements document reviews (JCPAT-E), and certifications.

Other useful POCs:

- [STP](#) and [STP Coordinators](#).
- [JT4 E-Form 9 Review](#) (conformance or interoperability certification) issues.
- [ERD](#) and [ERD Coordination](#).
- [JIT](#) & [JIT Coordination](#).
- [ITP](#) & [Executive Agent](#)
- TechLibrary32 (contact [NetOps](#) to have this system installed on your P.C.)

Format and Content

What are the most commonly made mistakes?

General:

- Left and right margins on the letter should be 1 inch.
- Periods at the end of sentences, paragraph titles, etc. are followed by two (2) spaces, as are colons.
- A comma is used before the last item of a series (e.g., A, B, and C. Not A, B and C, unless logically B&C combined is the same type of item as A.)
- Quotation marks around the title of a document should appear after the punctuation, for example, "This is done correctly," even though syntactically strange. The same type of quotation marks should be used, not a mixture of smart & straight quotes.

Specific:

Subject: Include the system acronym (as well as the full name) in the subject. This aids in searching the JIT and other interoperability databases. (Also applies to USMTF, TADIL, and similar acronyms.) Headers on subsequent pages should match the subject.

List of enclosures: If all of the enclosures are completely defined in the text (i.e., the complete title is used), the enclosure list can be "3 Enclosures a/s." Otherwise, a numbered list of enclosures should be provided.

Acronyms:

DoD – It's DoD, not DOD.

DT – Developmental Test(ing).

NCA – National Command Authorities ; SECDEF discontinued use on 1/11/02.

NIPRNET – Unclassified-but-Sensitive (N) Internet Protocol Router Network.

SIPRNET – Secret Internet Protocol Router Network.

Units of Measure:

Note that the following are not in accord with the [International System of Units \(SI\)](#) (the "metric system"), however, they are in common use and proposed conventions have not been adopted (and you wouldn't like them anyway, especially the prefixes for binary multiples).

kbps – kilobits per second.

Mbps – megabits per second.

Gbps – gigabits per second.

KB – kilobytes (of storage; i.e., 1024 bytes)

MB – megabytes (of storage; meaning varies with context).

[In SI, 1 MB = 1 000 000 B; proposed is 1 MiB = 1 mebibyte = 1 048 576 B.]

GB – gigabytes (of storage).

Gig, Meg, etc. – slang/jargon to be avoided.

Word Usage:

Comprises – X comprises Y, Z, etc. Or use, X consists of Y, Z, etc.

Reference: [JITC certification policy](#). As with the Distribution List, AOs should coordinate with JT4 to ensure they are using the latest version.

Who signs certification letters?

The portfolio/division chief signs all cert letters after incorporation of JT4 comments, except in a couple of situations:

- IOP Test **Non-Certification** letters are signed by the **JITC commander**.

Note that Std's Conformance Non-Certification letters are signed by the portfolio/division chief. IOP non-certifications can create a lot of interest and give us a lot of visibility; therefore, the commander needs to be aware of these potentially politically sensitive situations.

Why does the distribution list change every time I submit a cert letter?

Because it has been updated since the last cert letter you submitted, or you used an old distro list. This usually only happens with IOP Test Certs. The basic distribution list for IOP certs is based on the ITP membership, which changes rather frequently – either personnel change or someone figures out their actual office address. JITC has no control over the ITP membership, so can only pass along the changes as they happen.

Why is the system version information so important?

Systems change rather frequently, especially those using COTS software. Without proper configuration management (CM) on the part of developers and testers, it is not possible to figure out what was tested, what has changed, what works with what, etc. And not all protocols with the same name are compatible or backwards compatible.

If the PM has no CM controls, they should not be developing a system. If we do not know what we tested, we should not be testing and issuing a formal report. There is a difference between testing and playing/demonstrating.

"I don't know/can't find out the version information" is not a good position to be in at the end of a test. If you don't know what you tested, why should anyone believe that the testing was valid?

Who reviews certification letters?

There are a number of reviews that a draft cert letter may go through, and some depend on the particular division/portfolio policy. Consult with the Branch chief.

How do I get JITC release authority? What are the procedures for routing the finalized cert letter after incorporating JT4 comments?

The eForm 9 must be used to obtain release authority for all JITC certification letters. Please note a couple of significant items related to the STP and ERD.

- Policy review of the final version (after comments are received and incorporated) will not be completed until the STP entry is complete and accurate, and matches the information in the certification letter.
- The ERD shall be used for routing and distribution of certification letters.

Related Processes

What is an ICTO and what role does JITC play in it?

An Interim Certificate To Operate (ICTO) is a temporary waiver from interoperability system testing certification. It may be granted by the US MCEB [ITP](#) in special situations based on justifiable circumstances and impacts. An ICTO is not to exceed 1 year.

[Previously, these were known as an IATO - Interim Authority To Operate – issued by the MCEB panel which was called the IPTP.]

JITC reviews the requested ICTO and provides a recommendation back to the DISA representative and/or the [Executive Agent](#) of the [ITP](#) as to whether or not the ICTO should be granted. Recommendations are typically based upon:

- Initial test results
- Assessed impact on the operational systems / networks
- Urgent operational needs
- Plan for future certification

JITC also tracks the status of all ICTOs via the [JITC System Tracking Program \(STP\)](#).

The ICTO process and ITP meeting minutes are located on the [JITC public website](#) under the [ITP](#) menu

Policy & Guidance

Who should sign the coordination sheet for a TEMP?

In general, JITC will be one of the official signatories on the TEMP if we are designated as the Operational Test Agent (OTA) for that program. However, sometimes DISA is asked to sign the coordination sheet for a TEMP when JITC is not the OTA. The DISA office that should sign it should be JITC since we are the one within DISA who is most interested in T&E.

The person within JITC that can sign the TEMP is either the Division Chief, Portfolio Chief, or the Commander.

Who decides if standards selected by the Program Manager are in accordance with the DISR?

All entities that access the Joint C4I Program Assessment Tool (JCPAT), which includes JITC, as part of the requirements document review process, have a say. The Joint Staff is the final approval authority for the entire requirements document process that includes DISR compliance.

Who approves a program/system standards profile?

A Program Manager can request DISA provide analysis support on their selected standards profile. Even if the standards profile is not processed through DISA, it will be approved as a part of the review/approval process of other program documentation.

What is JITC's certification policy?

JITC certification policy and procedures can be found in the JITC Instruction [380-50-02](#).

What are the major Interoperability (IOP) DoD/CJCSI directives, instructions, etc.?

[DoDD 4630.05](#), Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 23 April 2007

[DoDI 4630.8](#), Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

[CJCSI 6212.01](#), Interoperability and Supportability of National Security Systems, and Information Technology Systems, 15 December 2008

[CJCSI 3170.01G](#), Joint Capabilities Integration and Development System, 1 March 2009

[Defense Acquisition Guidebook](#) Hypertext version of IOP dir's, reg's, etc.

What is in each of the major IOP DoD/CJCSI directives, instructions, etc.?

DoDD 4630.05: contains top level DoD directive that establishes IOP policy and authority.

DoDI 4630.8: companion instruction to 4630.5; contains basic IOP policy and direction, plus IWL.

CJCSI 6212.01: details and authorizes types of IOP certifications, JITC's IOP Test Certification and standards conformance certification.

CJCSI 3170.01: defines NR-KPP and IERs, format for CDD and CPD.

Where does JITC's authority as DoD's sole interoperability certifier come from?

The DoD 4630 & 5000 series and CJCSI 6212.01 identify DISA/JITC as the certifier for DoD IOP Test Certifications and Std's Conformance Certifications. However, note that there are other types of certifications and IOP certifications that are performed by other organizations.

When do certifications expire?

Systems are required to undergo periodic IOP evaluation throughout the life-cycle. IOP Test Certifications are issued for a period of four (4) years, or until changes that affect interoperability. It is rare for a system not to be upgraded in four years, even if it is merely the hardware platforms that are changed. Also, changes to interfacing systems or requirements will usually call for another IOP evaluation before the four year limit expires. Even if a system's hardware/software and interfacing systems do not change for a four year period, it is prudent to review the status periodically. If warranted, a new certification can be issued to extend the certification period based on a desktop analysis. This analysis should include feedback from the user community on lessons learned or noted discrepancies.

Standard's Conformance Certifications do not expire – they are good for the specified system and standard versions certified.

What is Information Interoperability?

Interoperability is the ability of systems, units or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment.

Note that there are other definitions from various sources. Joint Pub 1-02 contains a more generic definition that covers more than information interoperability. Other types of interoperability include the compatibility of munitions and other aspects that JITC is not involved in.

Why certify for Interoperability?

Certification assures the Warfighter, the Command/Service/Agency system can interoperate in a joint, combined, and coalition team.

[DoDD 4630.5] 4.1. IT and NSS interoperability and supportability are essential to joint, combined and coalition forces working together seamlessly to enhance operational effectiveness. Attaining IT and NSS interoperability and supportability is a continuous process, addressed as a balance of materiel and non-materiel solutions that is achieved and sustained throughout a system's life. Achieving and sustaining interoperability and supportability is a DoD enterprise-wide responsibility that must be woven into the thread of organizational roles, responsibilities, processes, and resources.

4.2. The Department of Defense shall achieve and maintain information superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining and leveraging interoperable and supportable IT and NSS. IT and NSS interoperability and supportability shall be attained through mission-related, outcome-based processes. Interoperability and supportability requirements shall be balanced with the need for Information Assurance. Joint, combined, coalition, and interagency missions must be supported through interoperable IT and NSS in global operations across the peace-conflict spectrum.

When should systems be certified?

All systems **must** be certified before fielding. Fielded systems must be recertified after changes affecting interoperability, or [every four years](#).

What does certification involve (i.e., what are the 4 basic steps)?

1. Identify **all** of the IOP requirements; verify the requirements, and determine the criticality.
 - Extract IOP requirements from available documents (CPD, ISP, TISP, possibly CDD), architectures, and the operational environment.
 - Requirements should be JS J-6 certified.
 - Requirements/criticality should be verified with the user community.
 - Interfacing systems requirements should be compared for discrepancies.
2. Develop Certification Plan/Methodology.
 - Using the requirements as a basis, determine needs and resources required to meet needs.
 - Map requirements/needs to resources.
 - Determine test schedule.
3. Perform IOP testing (collect IOP data).
 - Gather IOP data from appropriate test events (usually during OT) and other sources.
 - Previous testing, information from exercises, DT, and standards conformance results may provide further input to the analysis.
4. Determine the IOP status of the system and interfaces.
 - Produce the appropriate documentation for the IOP evaluation. Products may include:
 - a. IOP Test Certification Memorandum
 - b. Limited IOP Test Certification Memorandum
 - c. Interim IOP Test Certification Memorandum

- d. IOP Test Non-Certification Memorandum
- e. IOP Assessment Memorandum

What are the products/actions for an interoperability evaluation?

Assuming there is no existing groundwork, the critical items for an IOP evaluation include:

- Identify the system/program; obtain POCs, and coordinate with the system/program PMO.
 - Enter system information into the STP.
 - Educate the proponent on IOP T&E and certification.
 - Develop cost estimates. Get \$\$\$\$.
 - Identify **all** of the IOP requirements.
 - a. The entire system has to be evaluated.
 - b. An assessment may be performed for evaluating partial requirements.
 - c. The PM may only want to pay for limited testing, but all the requirements must be evaluated for a system certification.
 - Validate IOP requirements & criticality with users.
 - Plan.
 - a. Develop an ICEP/IOP Test Plan(s), as needed.
 - b. Develop the system IOP matrix (don't wait until after testing).
 - c. Enter testing information into the STP.
 - Conduct/monitor tests, collect data, analyze, report.
 - a. Perform Std's Conformance Certification (usually during DT).
 - 1. Std's conformance test plans/reports.
 - 2. Std's conformance certification letters.
 - 3. Update STP entries.
 - 4. Review of cert letters; finalization.
 - 5. Enter/update ERD distribution list entry for project.
 - 6. ERD distribution.
 - 7. Verify STP certification entries.
 - b. Perform IOP T&E/Certification (usually during OT).
 - 1. Use all applicable info (e.g., std's conformance results).
 - 2. Perform IOP evaluation on interfaces and system.
 - 3. IOP test plans/reports.
 - 4. IOP test certification letters.
 - 5. Update STP entries.
 - 6. Review of cert letters; finalization.
 - 7. Enter/update ERD distribution list entry for project.
 - 8. ERD distribution.
 - 9. Verify STP certification entries.
 - Continue with next system increment, and continue to monitor status during exercises, contingencies, tests of interfacing systems, etc. throughout the system life-cycle. Perform reevaluation every 4 years, even if no other changes have occurred.
 - a. Analyze changes to system, requirements, configuration, and interfacing systems to determine if new evaluation is required.
 - b. If necessary, perform IOP evaluation, reissue certifications.
- Keep STP system and JITC POCs and other info current.

What are the common problems with IOP evaluations?

- **All of the IOP requirements are not addressed.**
 - An IOP Test Cert must show the overall certification status of the system – all of the external interface requirements must be addressed in the requirements/status matrices, even if they were not tested or were previously evaluated. In the case where more than one cert letter has been issued for a given system version, the

latest cert letter should show the interoperability status of the entire system, not merely the interfaces that were recently tested (i.e., previous cert letters for the same system version are always superseded by the most recent certification; although, a cert letter may indicate the certification status for different versions of the system).

- *"But the PM only paid me to test one interface."* What was paid for or what was tested are not factors in determining what the actual IOP requirements are. An IOP evaluation (excluding IOP assessments) must address all of the external joint/combined interface requirements.
- If you know that there are other requirements, but they have not been formally documented or are otherwise unknown, enter an "other" interface in the requirements/status matrix to show that there are requirements that were not evaluated.
- **An overall interoperability view is not taken.**
 - Interoperability is not merely about one system's (i.e., the SUT's) performance. Interoperability involves at least two systems – both have to work properly to certify the interface.
 - *"But my system works – it's the other system that is broken."* It is the interface that must work. If the required information is not exchanged, there is no interoperability. If the other system is not available (maybe not even developed yet), but is absolutely critical to the SUT working, there is a critical interoperability problem.
 - Do not certify an interface when the interfacing system is broken. Non-certification of an interface is not necessarily an indication that the SUT has deficiencies, merely that there are anomalies in the exchange of information between two interfacing systems. It could even be the case that neither system is at "fault" – the communications path could be the culprit.
- **Version information is not provided.**
 - Version information for the system and each interface must be provided. Without some method for configuration management (i.e., tracking changes), it is impossible to determine exactly what was tested, what works with what, and when something has changed that would require another evaluation and recertification.
 - Every system and every interfacing system should be identified by name and version. Even technical interface requirements (e.g., a protocol such as SMTP or Link 16 should have version identification provided – protocols evolve and are not necessarily backwards/forwards compatible).
 - See "[Why is version info so important?](#)"
- **The interoperability evaluation is incomplete.**
 - Interfaces are individually evaluated, but this is not rolled up to a system level status. The cumulative effect of numerous interface problems may even warrant non-certification of the system. A rationale for certifying or not certifying the entire system needs to be provided, and an overall expected operational impact should be provided for the system.
- **Problems are ignored or buried in the back of the summary.**
 - The status matrix must make note of whether all requirements are met and must identify the expected operational impact of any discrepancies. (If all "critical requirements" are met (meaning that there are probably unmet non-critical requirements), the impact of problems associated with the non-critical requirements must still be mentioned.)
 - Problems mentioned in previous certifications for the same system (perhaps for a different interface than covered in recent testing) must be addressed. If the

problems have not been fixed, they still exist and must be reported, even if previously reported.

[Cert letter problems](#), although related, are addressed separately.

Are there other IOP certifications that other organizations certify?

Yes, that is why it is important to distinguish among the types of certifications that JITC issues and what other organizations produce.

There are a few important types of IOP system certifications.

- J-6 I&S NR-KPP Requirements Certification; certification of CDD, CPD, etc.
- IOP Test and Std's Conformance Certification (JITC).

Note that it has been rather common for some people to refer to requirements certifications as IOP certifications (i.e., my system has been IOP certified by the JS, so why do I need JITC certification?).

In addition to the basic IOP certifications, there may be other required "certifications," depending on the nature of the system. These may include: spectrum, intelligence, security, etc.

What if the customer wants a preliminary assessment of interoperability?

The best action would be to plan for reporting the IOP status with an *Interoperability Assessment* letter, rather than an *IOP Test Certification* letter. Everything is the same as with a normal IOP evaluation, except the results are reported in a slightly different manner.

IOP Assessment letters are *not* certifications, however, they provide the proponent (usually the PM) with the IOP status of the system or selected interfaces. IOP Assessments are also not sent to the JS, so it is less embarrassing if some interfaces or the system flunks (i.e., in an IOP Test Certification they would be formally non-certified).

Assessment results are also useful for reporting to the OTRR on a system's readiness for OT, and as input to an ICTO or waiver request. As a system matures, it should be completely evaluated and an IOP Test Certification issued.

Can I make one call/send one message to evaluate an interface?

It is not wise to exercise any electromechanical or electronic device merely once, then claim that it will work repeatedly. If software (including firmware) is involved, this is even worse. A software function frequently works on the first try – that's how the developer tested it. However, since software can be self-modifying (as can some hardware logic), it can work the first time and fail on subsequent tries. It is best to exercise a capability at least three (3) times before declaring success. This should be considered a bare minimum, not necessarily a statistically significant sample size. Limited resources may preclude obtaining statistically significant amounts of data (at a meaningful confidence level) during IOP testing. However, this is mitigated by the fact that more extensive testing should have been performed during DT, or during previous IOP evaluations. See JITC Test Sample Size training brief for additional info.

What is JITC's position on using simulators in IOP testing?

DoD policy is that interoperability evaluation occur in as operationally realistic environment as possible. However, interoperability evaluation does not necessarily include data from

only one source. Information from simulators (especially simulators that have been validated) could be used to supplement data available from live sources.

The bottom line is that testers/evaluators can use simulators (and environment generators) but not as a surrogate for actual platforms. It is up to the action officer to determine how much data is needed and what the acceptable methods of obtaining that data are.

Must software system upgrades be fully tested?

The requirement to fully test software system version changes is dependent upon the extent of changes. If the changes are minor and do not affect the interoperability of the already certified previous version, all that may be needed is a review of system level test activities and specific changes made to the new version. This review must be conducted by JITC and, based upon the results of the review, an interoperability certification letter may or may not be issued.

What if the test environment is not “operationally realistic” – can I still certify?

Interoperability certification means there is enough evidence to conclude the interoperability requirements can be met in the operational environment. When the test duplicates the operational environment completely this is easy. When it does not, the tester must use judgment to decide if the deviations are serious enough to warrant withholding certification. If there is a realistic risk that a critical requirement will not be met, the system or interface should not be certified. (If this is the case, the tester should warn the customer before the test that no certification can be issued based on it.)

Example: If a radio test does not use typical users, but the radio is simple to use and there are no special procedures required for interoperability with other types of radios, the risk of failure is small enough that certification is appropriate. However if a network switch requires complex configuration to interoperate in a network, the ability of contractor engineers to perform this task in their lab may not be proof that typical military personnel could accomplish it under field conditions. The switch should not be certified without more data to show this.

Useful Links

General

- [Internet Search](#)
- [refdesk.com](#) (General source of information.)
- [Fort Huachuca](#)
- **JITC/Interoperability in the News**
 - [DAU Defense AT&L Magazine](#) (Formerly PM Mag.)
 - [ITEA](#) (International Test and Evaluation Association)
 - [AFCEA Signal Magazine](#)
 - [National Defense Magazine](#)

DoD Organizations

- [DefenseLINK](#) (Links to main DoD sites.)
- [JCS](#)
- [JFCOM](#)
- [JITC Public Website](#)
- [ATEC](#)
- [AFOTEC](#)
- [NATO](#)

DoD Info Sources (directives, reg's, etc.)

- [U.S. Code Search](#)
- [DoDSSP](#) Mil Spec's, Mil Standards, etc.
- [DefenseLINK](#) (Directives are under the Publications menu.)
- [Joint Electronic Library](#) (CJCSI 3170, 6212, ...)
- [DSP](#) (Defense Standardization Program)
- [Defense Technical Information Center](#)
- [Defense Acquisition University](#) DoD 5000 info; good online training programs.
 - [DoD 5000 Series Resource Center](#)
- [USAPA](#) (US Army Publications)

DoD IOP Info Sources

- [DOT&E](#) T&E Oversight List.
- [DISA](#)

Misc Info Sources

- [FAS Search](#)
- [IETF](#) Internet "standards" (TCP/IP, SMTP, ...).
- [ITU](#) (International Telecommunication Union)
- [NIST](#) (National Institute of Standards and Technology)
 - [NIST International System of Units \(SI\)](#)

Dictionary, Abbrev

- [Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms."](#)
- [Acronym Finder](#)
- [DACS Acronyms, Dictionaries, Glossaries & Other Library Resources](#)
- [FAS Acronym List](#) & [FAS Military Lexicon](#) & [FAS News References](#)
- [ITS - Federal Standard 1037C: Glossary of Telecommunications Terms](#)
- [FOLDOC – Free Online Dictionary of Computing](#)
- [Glossary of Parsing Terms](#)

- [Joint Doctrine Encyclopedia](#)
- [NetLingo](#) Internet Jargon and definitions.
- [Webopedia: Online Dictionary for Computer and Internet Terms](#)

Style/Grammar (Follow these at your own risk.)

- [11 Rules of Writing](#)
- [Electronic Reference – Style Manuals](#) (Interesting guides/grammar links, but none official.)
- [English Grammar and Style Theme Page](#)
- [Recursive Adaptable Grammars](#)
- [Refdesk.com – Grammar, Usage, etc.](#)
- [Guide to Grammar and Writing](#)
- [Lynch, Guide to Grammar and Style](#)
- [NIST SI Unit rules and style conventions checklist](#)
- [The Online English Grammar](#)