



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MAR 27 2012

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY, AND LOGISTICS
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
CHIEF INFORMATION OFFICERS, MILITARY DEPARTMENTS

SUBJECT: Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)

Reference: "Memorandum of Understanding Between the Joint Staff J8 Directorate and the Department of Defense Chief Information Officer for Transfer of Functions and Associated Resources," August 26, 2011

Reference transferred specific functions from the Joint Staff (J8) to the DoD CIO to include responsibilities for interoperability of IT and NSS previously performed by the Joint Staff (J6). The purpose of this memorandum is to provide interim guidance for the review and approval of Information Support Plans (ISPs), and interoperability certification of IT and NSS. This interim guidance memorandum does not alter existing DoD authorities or command relationships.

The DoD CIO point of contact for this action is Mr. Kris Strance, kris.strance@osd.mil, 571-372-4670.

A handwritten signature in black ink, appearing to read "Teresa M. Takai".

Teresa M. Takai

Attachment:
Interim Guidance for Interoperability of IT and NSS

Interim Guidance for Interoperability of IT and NSS

- References:
- (a) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004
 - (b) "Memorandum of Understanding Between the Joint Staff J8 Directorate and the Department of Defense Chief Information Officer for Transfer of Functions and Associated Resources," August 26, 2011
 - (c) Memorandum, OASD(NII), "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 (hereby superseded)
 - (d) Memorandum, OUSD(AT&L), "Improving Milestone Process Effectiveness," June 23, 2011

1. **GENERAL**. The following provides amplifying guidance for responsibilities and procedures contained in Reference (a) to implement functions transferred to the DoD Chief Information Officer (CIO) in Reference (b). Applicability, definitions, and policy in Reference (a) still apply.

2. **RESPONSIBILITIES**. In addition to those responsibilities specified for DoD Components in Reference (a), the following amplifying responsibilities are required:

a. The DoD CIO shall:

(1) Provide direction and oversight, in coordination with other DoD Components, for:

(a) Interoperability test and certification of IT and NSS.

(b) Adjudicating waivers of policy and requests for an Interim Certificate to Operate (ICTO).

(2) Establish, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Director of Operational Test and Evaluation (DOT&E), and the Chairman of the Joint Chiefs of Staff, process, procedures, format, and content guidance for developing and submitting Acquisition Category (ACAT) and non-ACAT Information Support Plans (ISPs).

(3) Establish, in coordination with the USD(AT&L), the DOT&E, and the Chairman of the Joint Chiefs of Staff, overarching process and procedures to verify, assess, and certify, through testing, IT and NSS interoperability throughout a system's life (per Reference (a), formerly a Chairman of the Joint Chiefs of Staff responsibility).

(4) Establish and oversee the DoD-wide process for review of ISPs.

(5) Establish an IT and NSS Interoperability Steering Group (ISG), subordinated to an appropriate DoD CIO Executive Board (EB) forum. This replaces both the existing Interoperability and Interoperability Certification Panels. Representatives from the DoD CIO, the USD(AT&L), and the Joint Staff (J8) shall tri-chair the ISG.

(6) Ensure DoD Components establish an ISP review process to support joint reviews.

(7) Adjudicate critical comments in joint ISP reviews that cannot be resolved at the DoD Component level.

b. The Director, Defense Information Systems Agency (DISA), under the authority, direction, and control of the DoD CIO, shall:

(1) Conduct the Joint IT and NSS Interoperability Assessment, Test, and Evaluation Program, in collaboration with the other DoD Components.

(2) Direct the DISA Joint Interoperability Test Command (JITC) to:

(a) Evaluate joint IT and NSS interoperability for the Department of Defense.

(b) Serve as the Joint Interoperability Certification Authority for the DoD. Certify all joint IT and NSS for interoperability, using the Net-Ready Key Performance Parameter (NR-KPP), when applicable, as the basis for test.

(c) Establish, in coordination with the DoD CIO, the USD(AT&L), the DOT&E, and the other DoD Components, procedures to verify, assess, and certify, through testing, joint IT and NSS interoperability throughout a system's life.

(d) Publish and maintain an Interoperability Process Guide (IPG), outlining all procedures and documentation required to support joint interoperability testing, certification, and waiver submissions.

(e) Accept and review all requests for waivers of DoD CIO interoperability policy (except as specified in paragraph 2.c.(2) for ISPs), analyze those requests, and provide recommendations for DoD CIO approval/disapproval.

(3) Operate and maintain the GIG Technical Guidance - Federation (GTG-F) online portal and associated processes supporting the preparation, submission, verification, assessment review, and approval of ISPs (<https://gtg.csd.disa.mil>).

(4) Participate in all joint reviews of ISPs, and nominate for DoD CIO ISP Special Interest oversight those programs affecting DoD enterprise strategic initiatives.

c. The DoD Components shall:

(1) Ensure that:

(a) ISPs for all ACAT and non-ACAT acquisitions and procurements are submitted and approved using the procedures specified in paragraph 3 of this memorandum.

(b) The DoD Component, Milestone Decision Authority (MDA), or cognizant fielding authority (must be above the program manager (PM) level) reviews, assesses, and

approves all ISPs. Final approval of all ISPs must be published using the GTG-F or Secret Internet Protocol Router Network (SIPRNet) Joint C4I Program Assessment Tool - Empowered (JCPAT-E), as appropriate.

(c) Processes and procedures exist for conducting review (including joint review) and assessment of ISPs for all ACAT and non-ACAT programs.

(d) Joint reviews are performed for all ACAT and non-ACAT ISPs as described in paragraph 3.a.(2) of this memorandum.

(2) When appropriate, approve waiver requests for requirement of an ISP for DoD Component-unique (i.e., no joint interfaces) IT and NSS. Upon approval, the DoD Component will provide the DoD CIO with copies of the waiver request and approval memorandums.

(3) Submit all other waivers or requests for exceptions to Reference (a) of this memorandum in accordance with paragraph 3.d.. Statutory requirements may only be waived if the statute specifically provides for doing so.

d. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) shall provide a tri-chair to the ISG.

e. The Chairman of the Joint Chiefs of Staff shall:

(1) Establish policy and procedures for developing, coordinating, and certifying the NR-KPP, in coordination with the USD(AT&L), the DOT&E, and the other DoD Components.

(2) Provide specific guidance on preparation, format, content, timelines for submission, and review of the NR-KPP.

(3) Certify that the NR-KPP is sufficient, both in scope and content, to describe a system's interoperability requirements in a measurable and testable manner. NR-KPP Certification must occur prior to interoperability test and certification.

(4) Provide a tri-chair to the ISG.

3. PROCEDURES

a. Review and Approval of ISPs. The Information Support Plan (ISP) process is defined in Reference (a). This interim guidance memorandum amplifies and updates elements of the ISP review process described in Enclosure 4 of Reference (a) and supersedes Reference (c).

(1) ISP Content

(a) Unclassified ISPs shall be created, submitted, and approved using the DISA-managed GTG-F (<https://gtg.csd.disa.mil>). ISP formatting and content requirements shall be specified in the GTG-F. Deviations from these requirements require DoD Component approval.

(b) Secret ISPs shall be submitted and approved using JCPAT-E until GTG-F is available on the SIPRNet. Top Secret ISPs shall be submitted using a staffing notification to the appropriate classified network that includes the location of the document on the Joint Worldwide Intelligence Communications System (JWICS) and the program's points of contact.

(c) Classified ISP documents may also still be developed following the 13 steps in Reference (a), Enclosure 4. ISP documents submitted using the above process shall reference applicable GTG-F generated GIG Technical Profiles (GTPs) and DoD Information Technology Standards Registry (DISR) standards, as appropriate.

(d) ACAT II and below, as well as Non-ACAT ISPs, may be tailored based on a system's scale, complexity, and available resources with the approval of the DoD Component.

1. DoD Components may only approve a tailored ISP using the following categories: legacy programs in sustainment with no plan of upgrade, non-ACAT programs with limited resources, or programs with a scheduled date of retirement in the near future.

2. At a minimum, the tailored plan will provide an explanation of the program's Concept of Operations (CONOPS) and will provide IT supportability analysis of the CONOPS.

3. Additionally, the following set of integrated architecture viewpoints is required: an AV-1, OV-5a, either OV-5b or OV-6c, either SV-5 or SvcV-5, either SV-6 or SvcV-6, and StdV-1. The PM shall coordinate with the DoD Component point of contact to determine if any additional viewpoints will be required. The final DoD Component tailored ISP will be submitted to the GTG-F for review and assessment.

(2) ISP Review Process

(a) The DoD Components shall lead the review of all ISPs regardless of ACAT level. If a program meets the criteria for a joint review listed below, the DoD Component shall coordinate the review with the joint community (including DISA).

1. For ACAT II and below programs, the owning DoD Component shall select the appropriate additional DoD Components for the joint review; however, the review shall include at a minimum the Joint Staff and DISA.

2. For all ACAT I and DoD CIO ISP Special Interest programs, the ISP shall be staffed to all DoD Components as part of a DoD-level joint review. The DoD CIO shall participate in ACAT I and DoD ISP Special Interest ISP reviews, and shall provide concurrence, concurrence with comment, or non-concurrence with the ISP for consideration by the DoD Component, MDA, or cognizant fielding authority for final approval.

3. The Joint Staff will no longer conduct Joint Interoperability and Supportability Certification for DoD Component IT and NSS. Final approval of an ISP undergoing joint review as outlined below satisfies the requirement for Joint Interoperability and Supportability Certification (paragraph 5.9.9 of Reference (a)).

(b) Joint reviews shall be conducted for all IT and NSS ISPs that:

1. Have a Joint Staffing Designator (formerly Joint Potential Designator (JPD)) of Joint Requirements Oversight Council (JROC) Interest; Joint Capabilities Board (JCB) Interest; or Joint Integration with an NR-KPP.

2. Implement information exchanges across DoD Component boundaries.

3. Implement a web service with the explicit or implicit intention to share information across organizational boundaries.

4. Have received a DoD Component determination that a joint review is necessary.

(3) DoD Components shall establish processes to facilitate the review of unclassified ISPs within the GTG-F (<https://gtg.csd.disa.mil>). DoD Components are encouraged to conduct concurrent joint and internal Component reviews as often as possible. DoD Components (specifically DoD Agencies), that do not have a mature ISP review process will coordinate with the DoD CIO to ensure joint reviews are conducted.

(4) ISP reviews in the GTG-F will result in a set of comments for the PM to adjudicate. The PM will adjudicate critical comments by actively engaging with the organization and person who made the comment to ensure adequate resolution. For critical comments that cannot be resolved, the issue will be elevated through the owning DoD Component for resolution by the DoD CIO. Critical risks and issues identified through ISP reviews shall be briefed by the PM in Integrating Integrated Product Team and Overarching Integrated Product Teams, as appropriate.

(5) Figure 1, "ISP Submission Timeline," illustrates when ISPs must be submitted to the GTG-F (<https://gtg.csd.disa.mil>) for joint reviews. All joint ISP reviews will be staffed for thirty calendar days. Programs not governed by the Defense Acquisition System (non-ACAT) may have different milestone events than as shown in Figure 1. Those programs should follow the described process to build toward a Final ISP of Record by determining equivalent milestone events to the Defense Acquisition System process, and conducting ISP submissions and reviews accordingly.

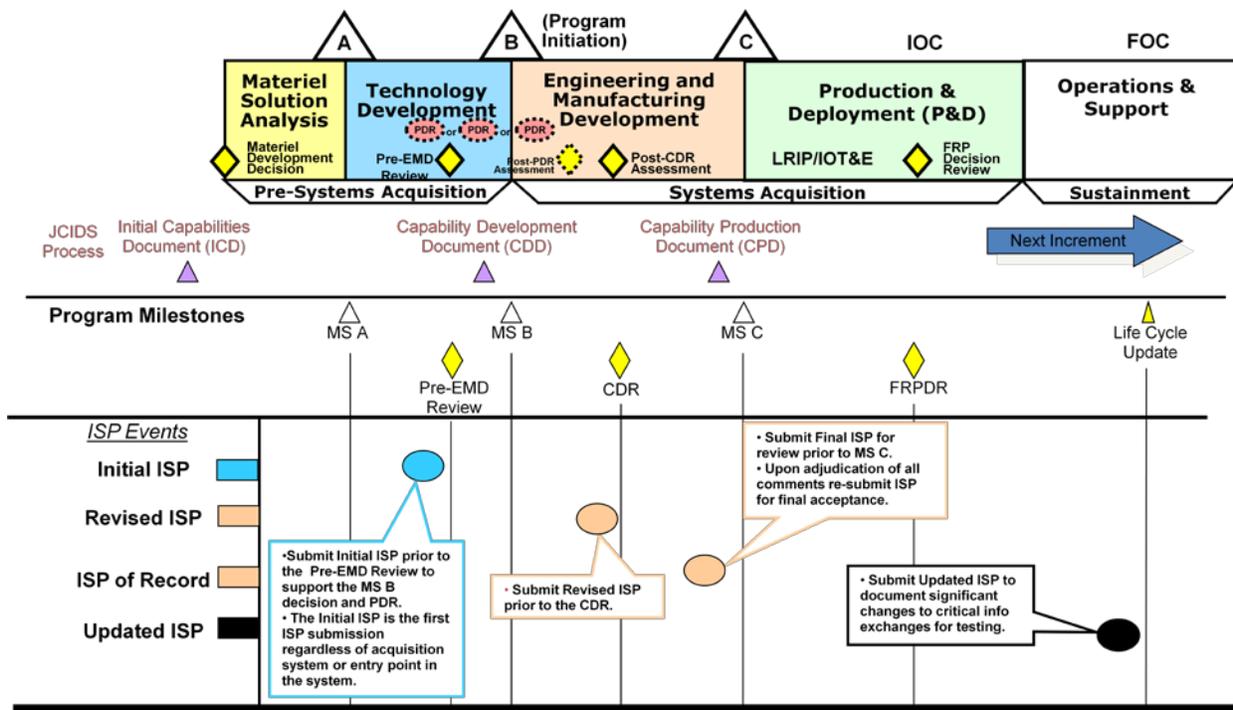


Figure 1, "ISP Submission Timeline"

(a) Initial ISP. Submitted for any given multi-milestone increment. Within the Defense Acquisition System the Initial ISP review is prior to and in support of the pre-Engineering and Manufacturing Development (EMD) phase review prior to MS B. The Initial ISP should facilitate the development of the EMD phase request for proposal (RFP) in accordance with Reference (d).

(b) Revised ISP. Completed prior to Critical Design Review (CDR). Programs with multiple CDRs should coordinate this submission with the Component ISP POC and DoD CIO, as appropriate. The Revised ISP may be waived or become the Final ISP of Record based on DoD Component approval.

(c) Final ISP of Record. Completed prior to MS C unless otherwise determined by the DoD Component and DoD CIO. The Final ISP of Record should describe the production or deployment representative system. DoD Component approval of a Final ISP of Record will consider the recommendations of the DoD CIO and the DoD Components, and both the Joint Staff (J2) Intelligence and Joint Staff (J8) NR-KPP certifications.

(d) Updated ISP. An Updated ISP is provided and reviewed for the next increment or program upgrade during Life Cycle Sustainment, as required.

(6) Failure to complete the ISP process in a timely manner may result in non-concur to proceed by the DoD CIO at MS B, MS C, or future incremental decisions.

b. Interoperability Test and Certification of IT and NSS

(1) Interoperability shall be assessed through formal operational test and evaluation by a DoD Component Operational Test Authority (OTA) or DISA (JITC), joint exercises, or a combination of any of the above.

(2) The JITC shall serve as the Joint Interoperability Certification Authority for the DoD, under the oversight and direction of the DoD CIO. As such, DISA (JITC) shall develop procedures to verify, assess, and certify, through testing, IT and NSS (ACAT and non-ACAT) interoperability throughout a system's life.

(3) DoD Components shall establish processes and procedures for test and certification of DoD Component-unique (i.e., no joint interfaces) IT and NSS.

(4) The JITC will develop and publish an online IPG, in coordination with DoD CIO, to document procedures and data requirements for interoperability testing and certification, waiver processing, and associated processes and procedures. The IPG will be available at <http://jitic.fhu.disa.mil/cgi/icpsite/pubs.aspx>.

c. Governance of IT and NSS Interoperability. The ISG shall propose, review, and coordinate interoperability policies; review critical interoperability issues; and adjudicate requests for Interim Certificates to Operate (ICTOs) and waivers to policy. Representatives from the DoD CIO, the USD(AT&L) and the Joint Staff (J8) shall tri-chair the ISG.

d. Waivers to Policy and ICTO Requests

(1) Only the DoD CIO, in coordination with the USD(AT&L), the DOT&E, and the Chairman of the Joint Chiefs of staff, as appropriate, is authorized to approve waivers to policy contained in this memorandum and Reference (a), and requests for ICTOs, except as specified in paragraph 2.c.(2) for ISPs.

(2) The DoD CIO, in coordination with the USD(AT&L), the DOT&E, and the Chairman of the Joint Chiefs of Staff, shall consider waivers to this policy only:

(a) When the operational chain of command and the Chairman of the Joint Chiefs of Staff have validated an urgent operational need; or

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

(c) When a fielded system is scheduled for retirement, and the cost of complying with this policy outweighs the benefit to the DoD; or

(d) When the system has no joint interoperability requirements.

(3) The DoD CIO, in coordination with the USD(AT&L) and the Chairman of the Joint Chiefs of Staff, shall grant ICTOs only when:

(a) The operational chain of command and the Chairman of the Joint Chiefs of Staff have validated an urgent operational need requiring fielding of the IT or NSS prior to testing, or

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

(4) Waivers and requests for ICTOs shall be submitted in accordance with the IPG.

(5) Waivers may be either permanent or temporary, at the discretion of the DoD CIO.