Department of Defense

INSTRUCTION

NUMBER 4630.8
June 30, 2004

ASD(NII)/DoD CIO

SUBJECT: Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

References: (a) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002 (hereby canceled)
(b) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) Subtitle III of title 40, United States Code (formerly Division E of the Clinger-Cohen Act of 1996), as amended
(e) through (ae), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues reference (a) to implement updated policy and responsibilities for interoperability and supportability of Information Technology (IT), including National Security Systems (NSS), as defined in reference (b).

1.2. Implements a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability throughout the Department of Defense (DoD). This approach incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership and education, personnel, and facilities) aspects to ensure life-cycle interoperability and supportability of IT and NSS throughout the Department of Defense.

1.3. Implements the Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the

Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability.

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies (see paragraph E2.1.15.), the DoD Field Activities, and all other organizational entities in the Department of Defense (referred to collectively as the "DoD Components").

2.2. All IT, including NSS (referred to hereafter as "IT and NSS"), acquired, procured (systems or services), or operated by any DoD Component, to include:

2.2.1. All IT and NSS defense acquisition programs, defense technology IT and NSS projects, and IT and NSS pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations (ACTDs), Advanced Technology Demonstrations, and Joint Warrior Interoperability Demonstrations (JWIDs) when selected for acquisition or procurement), Joint Experimentation, and Joint Tests and Evaluations; non-5000 Series IT and NSS acquisitions or procurements (e.g., the Combatant Command and Control Initiatives Program, Combatant Commander Initiatives Fund, Combatant Commander Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, and Tactical Exploitation of National Capabilities Programs); and post-acquisition (fielded) IT and NSS systems.

2.2.2. All inter- and intra-DoD Component IT and NSS that exchange and use information to enable units or forces to operate in joint, combined, coalition, and interagency operations.

2.2.3. All DoD Component IT and NSS supporting business areas and domains within the Department of Defense.

2.2.4. All IT and NSS acquired, procured, or operated by DoD intelligence agencies, DoD Component intelligence elements, and other DoD intelligence activities engaged in direct support of DoD missions. This Instruction recognizes that special measures may be required for protection and handling of foreign intelligence or counterintelligence information, or other need to know information. Accordingly, implementation of this Instruction must be tailored to comply with coordinated Director of Central Intelligence Directives and Intelligence Community (IC) policies.

2.2.5. All DoD IT and NSS that share information with other external U.S. Government Departments and Agencies, combined and coalition partners, and multinational alliances (e.g., North Atlantic Treaty Organization (NATO)).

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate. The Department of Defense shall achieve and maintain decision superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining, and leveraging interoperable and supportable IT and NSS.

4.2. Further guidance is provided in enclosure 3.

5. RESPONSIBILITIES

To implement the policies and responsibilities of reference (b):

5.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) shall:

5.1.1. Maintain this Instruction, in coordination with the other DoD Components, to codify responsibilities and procedures necessary to ensure interoperability and supportability of IT and NSS throughout the Department of Defense.

5.1.2. Provide policy, guidance, and oversight, in coordination with the DoD Components, to ensure that IT and NSS are interoperable and supportable with other relevant IT and NSS, internal and external to the Department of Defense.

5.1.3. Ensure the development, implementation, and maintenance of the Global Information Grid (GIG) Architecture per DoD Directive 8100.1 (reference (c)), as the sound and integrated Information Technology Architecture required by Subtitle III of title 40, U.S.C. (formerly Division E of the Clinger-Cohen Act of 1996), as amended (reference (d)).

5.1.4. Ensure, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Chairman of the Joint Chiefs of Staff, the Commander, U.S. Joint Forces Command (USJFCOM), and the other DoD Components, that integrated architectures are defined, developed, integrated, coordinated, validated, synchronized, and implemented. Establish format and content requirements for integrated architectures in the DoD Architecture Framework (reference (e)). Development of integrated architectures shall be consistent with the products required by reference (e).

5.1.5. Establish processes, in coordination with the USD(AT&L), the Director Operational Test and Evaluation (DOT&E), the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM , and the other DoD Components, to review and verify that the NR-KPP is adequately defined, and that IT and NSS interoperability and supportability test objectives are consistent with assessing the NR-KPP.

5.1.6. Establish responsibilities and procedures, in coordination with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, to ensure early interoperability assessment, verification, and evaluation of the NR-KPP, and reassessment and re-evaluation, as required, throughout a system's life. The ASD(NII)/DoD CIO, in coordination with the DoD Components, shall also ensure that user-defined, capability-focused, effects-based performance measures are established for interoperability verification of the NR-KPP.

5.1.7. Establish, in coordination with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, process, procedures, format, and content guidance for developing and submitting Acquisition Category (ACAT) and non-ACAT Information Support Plans (ISPs).

5.1.8. Lead DoD-wide review of ISPs for all ACAT I and Information Assurance (IA) acquisition and OSD-designated ISP special interest programs (see paragraph E4.5.2.). Ensure all ISPs are forwarded to the Defense Information Systems Agency (DISA) for review.

5.1.9. Establish a process to notify the Milestone Decision Authority (MDA), prior to each program review whether an IT or NSS program is meeting its NR-KPP and supportability requirements. If satisfactory progress is not being made, recommend, in coordination with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, a course of action that the program manager must follow.

5.1.10. Maintain liaison with the office of the IC CIO to ensure continuous coordination of DoD and IC interoperability and supportability issues.

5.1.11. Define, organize, and approve, in coordination with the USD(AT&L), the Chairman of the Joint Chiefs of Staff, and the other DoD Components, Universal

Reference Resources (URRs) for developing integrated architectures throughout the Department of Defense.

5.1.12. Establish and maintain, in coordination with the DoD Components, policy and processes for developing, prescribing, and implementing IT and NSS standards, consistent with reference (b), 10 U.S.C. 2223 and 2224, DoD Instruction 4120.24, and DoD 4120.24-M (references (f), (g), and (h)), that apply throughout the Department of Defense. Coordinate with the IC CIO to develop a consistent set of approved standards for both communities. Provide oversight, with other DoD Components, for the development and maintenance of the DoD Information Technology Standards Registry (DISR).

5.1.13. Participate in Integrated Product Team (IPT) reviews, including Defense Acquisition Board (DAB) proceedings, for acquisition programs of systems that contain or acquire IT and NSS. From these reviews:

5.1.13.1. Assess and evaluate IT and NSS acquisitions and procurements, and, in coordination with the DoD Components, propose recommendations to the Secretary of Defense for addressing IT and NSS deficiencies and for the elimination of unnecessary duplication of IT and NSS within and among the DoD Components.

5.1.13.2. Ensure applicable IT and NSS interoperability and supportability policy is considered and document potential interoperability and supportability issues for MDA consideration.

5.1.14. Establish a process, in coordination with the USD(AT&L), the Under Secretary of Defense (Comptroller/Chief Financial Officer (USD(C)/CFO), the Under Secretary of Defense for Intelligence (USD(I)), the Director Program Analysis and Evaluation (DPA&E), the DOT&E, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, to identify IT and NSS interoperability issues and propose operationally prioritized recommendations to the DAB, DoD Overarching IPTs, ASD(NII)/DoD CIO Reviews, Joint Capabilities Integration and Development System (JCIDS) Functional Capabilities Boards (FCBs), and the Joint Requirements Oversight Council (JROC), as appropriate, for resolving critical issues. This process shall identify IT and NSS interoperability and supportability needs and consolidate, prioritize, and phase materiel and non-materiel solutions for addressing deficiencies.

5.1.15. Provide oversight and direction, in coordination with the USD(C)/CFO, the USD(I), the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, of the transition fund (currently within Navy Program Element "Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Battle Center") to address high priority fielded IT and NSS interoperability issues requiring resolution pending inclusion in Program Objective Memorandum (POM) or other funding mechanisms. Among the

issues considered shall be those identified by the Commander, USJFCOM in Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF) remedy sets for JROC process consideration and validation. Once coordinated through the JROC process, materiel and non-materiel remedies requiring immediate funding may be addressed through the transition fund.

5.1.16. Maintain consolidated DoD Mission Critical Information System and Mission Essential Information System lists for use by the DoD Components.

5.1.17. Establish and maintain, in coordination with the DoD Components and the Chairman of the Joint Chiefs of Staff, a DoD Architecture Repository (DAR). The DAR shall comply with the data naming conventions documented in the DoD Core Architecture Data Model.

5.1.18. Establish and provide a senior representative to the Interoperability Senior Review Panel (ISRP). The ISRP shall be chaired on a rotating basis, by senior representatives from the USD(AT&L), the USD(C)/CFO, the USD(I), the ASD(NII)/DOD CIO, the DPA&E, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM. The ISRP shall:

5.1.18.1. Coordinate DoD IT and NSS interoperability and supportability policy and processes.

5.1.18.2. Coordinate interoperability reviews and assessments that identify IT and NSS interoperability deficiencies and corrective actions.

5.1.18.3. Review and comment on interoperability deficiencies and proposed DOTMLPF solution sets identified by the Commander, USJFCOM.

5.1.18.4. Review critical systems and programs with significant interoperability deficiencies and approve appropriate candidates for the Interoperability Watch List (IWL).

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics shall:

5.2.1. As the DoD Acquisition Executive (reference (i)), ensure the policies outlined in section 4., above, are incorporated into the DoD 5000 series acquisition documents (DoD Directive 5000.1 and DoD Instruction 5000.2 (references (j) and (k))) and adequately addressed, during system acquisitions, as appropriate.

5.2.2. For all ACAT acquisition and procurement matters, in coordination with the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, approve tradeoffs among operational effectiveness, operational suitability, and IT and NSS interoperability and supportability.

5.2.3. Manage acquisition of Major Defense Acquisition Program-related IT and NSS and assist the ASD(NII)/DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the other DoD Components, in the evaluation of interoperability and supportability requirements in a capability context.

5.2.4. Ensure, in coordination with the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, that IT and NSS interoperability requirements, as outlined in the ISP, are verifiable as part of the acquisition and procurement processes.

5.2.5. Ensure, in coordination with the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, that operationally prioritized materiel and non-materiel interoperability requirements are phased for acquisition and implementation.

5.2.6. Ensure that ISP requirements are reflected in policies and directives governing the Defense Acquisition System (references (j) and (k)).

5.2.7. Ensure that the DISA is included in the review of IT and NSS developmental and operational test plans.

5.2.8. Establish responsibilities and procedures necessary to ensure comprehensive Developmental Test and Evaluation (DT&E) of the NR-KPP during system development.

5.2.9. Provide a senior representative to the ISRP.

5.3. The Under Secretary of Defense for Policy shall ensure the Assistant Secretary for Homeland Defense:

5.3.1. Represents the Department of Defense on all homeland defense-related matters with designated Lead Federal Agencies, the Executive Office of the President, the Department of Homeland Security, other Executive Departments and Federal Agencies, and State and local entities to ensure that IT and NSS interoperability and supportability issues are identified to the ASD(NII)/DoD CIO.

5.3.2. Establishes procedures in coordination with the ASD(NII)/DoD CIO to assess and verify IT and NSS interoperability and supportability requests that are homeland defense-related by Federal, State, and local entities external to the Department of Defense.

5.4. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall:

5.4.1. Ensure, in coordination with the other DoD Components, IT and NSS interoperability and supportability funding issues resulting from the requirements of this Instruction are addressed in the budgetary process.

5.4.2. Provide the Deputy Secretary of Defense, in coordination with the USD(AT&L), the USD(I), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components, budget recommendations for addressing critical IT and NSS interoperability and supportability issues.

5.4.3. Provide a senior representative to the ISRP.

5.5. The Under Secretary of Defense for Intelligence shall:

5.5.1. Require the Director, Defense Intelligence Agency (DIA) to:

5.5.1.1. Collaborate with the DoD Components, as appropriate, to facilitate IT and NSS interoperability and supportability, and to identify required interfaces between DIA IT and NSS and other DoD Components' systems.

5.5.1.2. Coordinate with the DISA to define and implement standards within the DISR and DoD Intelligence Information Systems (DoDIIS) that are consistent with the IC integrated architectures.

5.5.1.3. Coordinate with the DoD Components to ensure IT and NSS interoperability and supportability needs are satisfied for processing foreign intelligence and foreign counterintelligence information.

5.5.1.4. Evaluate the IT and NSS interoperability and supportability in JCIDS documentation and ISPs, and coordinate with the DISA on matters involving IT and NSS interoperability certification processes.

5.5.1.5. Coordinate with the DISA and the National Security Agency/Central Security Service (NSA/CSS) on the requirements for defining and implementing IT and NSS standards.

5.5.1.6. Ensure that industry and non-governmental standards used for DIA intelligence systems and applications are open-systems based and conform to Net-Centric Enterprise Services (NCES)/Common Operating Environment (COE) and DISR tenets for interoperability.

5.5.1.7. Coordinate with the DoD Components to resolve IT and NSS interoperability issues. If resolution cannot be achieved, provide an impact statement and

recommendations for resolution to the Military Communications-Electronics Board (MCEB) or Military Intelligence Board (MIB), as appropriate.

5.5.1.8. Validate DoD Component's System Threat Assessment Reports (STARs) that highlight threats to IT and NSS interoperability and supportability.

5.5.2. Require the Director, NSA/CSS to:

5.5.2.1. Serve as the Community Functional Lead for Cryptology and coordinate with the appropriate DoD Components on matters involving IT and NSS interoperability and supportability of cryptologic systems.

5.5.2.2. Serve as the DoD Lead for approving and enforcing tactical Signal Intelligence (SIGINT) architectures and standards, coordinate with the DoD Components and the U.S. Special Operations Command to develop tactical SIGINT architectures and provide standards compliance and interoperability assessment reports to assist MDAs in production decisions.

5.5.2.3. Ensure that industry and non-governmental standards used for SIGINT and SIGINT systems and applications are open-systems based, and conform to NCES/COE and DISR tenets for interoperability.

5.5.2.4. Serve as technical oversight authority for tactical SIGINT systems and programs according to NSTISSP No. 11 (reference (l)), and provide cryptologic expertise and assistance in assessing IT and NSS JCIDS documentation for interoperability. Generate STARs that highlight threats to IT and NSS interoperability and supportability between tactical SIGINT systems and NSA/CSS IT and NSS.

5.5.2.5. Develop policy and procedures for IT and NSS IA and information releasability for joint, combined, and coalition forces and U.S. Government Departments and Agencies. Ensure IA products are available for security of NSS.

5.5.2.6. Develop, provide, and implement IA and defense-in-depth solutions and applications to ensure integrity and security of data, capabilities, and systems.

5.5.2.7. Ensure interoperability, supportability, and security of NSA/CSS IT and NSS with those systems that provide direct support to the Combatant Commander.

5.5.2.8. Ensure, with other DoD Components, that NSA/CSS-required capabilities are satisfied through the design and development of interoperable and supportable IT and NSS interfaces between joint, combined, coalition or other U.S. Government or Agency IT and NSS.

5.5.2.9. Ensure NSA/CSS IT and NSS programs are certified for standards conformance and IT and NSS interoperability and supportability.

5.5.2.10. Ensure, with other appropriate DoD Components, IC, or other U.S. Government Agencies, that NSA/CSS IT and NSS interoperability needs for processing foreign intelligence and foreign counterintelligence information are satisfied by designing and developing interoperable and supportable technical, procedural, and operational interfaces.

5.5.2.11. Coordinate with the DoD Components to resolve IT and NSS interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the MCEB or MIB, as appropriate.

5.5.3. Require the Director, National Geospatial Intelligence Agency (NGA) to:

5.5.3.1. Coordinate with the other DoD Components to identify National System for Geospatial Intelligence (NSGI) standards and specifications for imagery, imagery intelligence, and geospatial information (formerly mapping, charting, and geodesy) to support the interoperability and supportability of IT and NSS.

5.5.3.2. Ensure NSGI standards and specifications incorporate imagery and geospatial information release or disclosure decisions.

5.5.3.3. Ensure that industry and non-governmental standards used for imagery and geospatial systems and applications are open-systems based and conform to NCES/COE and DISR tenets for interoperability.

5.5.3.4. Coordinate with the DoD Components to resolve IT and NSS interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the MCEB or MIB, as appropriate.

5.5.4. Provide a senior representative to the ISRP.

5.6. The Director of Program Analysis and Evaluation shall:

5.6.1. Provide guidance to the DoD Components for conducting Analysis of Alternatives (AoAs) for IT and NSS capability gaps identified through the JCIDS process. Ensure interoperability and supportability needs are considered and addressed as part of the AoA.

5.6.2. Provide recommendations to Deputy Secretary for addressing, through the Planning, Programming Budgeting, and Execution (PPBE) process, critical IT and NSS interoperability and supportability issues with affected DoD Components.

5.6.3. Provide a senior representative to the ISRP.

5.7. The Director of Operational Test and Evaluation, shall:

5.7.1. Ensure that the NR-KPP specified in JCIDS documents is verifiable through testing and analysis, and contributes to the evaluation of the system's operational effectiveness with the Chairman of the Joint Chiefs of Staff and the Commander, USJFCOM.

5.7.2. Test and evaluate IT and NSS throughout the acquisition and procurement process, with sufficient frequency during a system's life to accurately assess IT and NSS interoperability and supportability.

5.7.2.1. Ensure that capability-focused, effects-based measures of performance and associated metrics are developed to support evaluations of IT and NSS interoperability and supportability throughout a system's life cycle with the USD(AT&L), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components.

5.7.2.2. Ensure that proper tools and testing infrastructure exists to support IT and NSS evaluation, in coordination with the USD(AT&L), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the other DoD Components.

5.7.2.3. Assist the DoD Components with operational test planning and assessment and/or evaluation of IT and NSS interoperability and supportability.

5.7.3. Ensure that Test and Evaluation Master Plans (TEMP) and operational test plans for those programs under DOT&E oversight identify IT and NSS interoperability test requirements with the USD(AT&L), and the other DoD Components. Emphasize, as early as possible during a system's development, evaluation of IT and NSS interoperability and supportability.

5.7.4. Identify from testing and evaluation, IT and NSS interoperability and supportability deficiencies and provide these to the USD(AT&L), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, the DISA, and the responsible DoD Component, for resolution, as appropriate. Report IT and NSS interoperability and supportability status for each program at milestone reviews, and as part of the DOT&E Annual Report to the Congress and the Secretary of Defense.

5.7.5. Establish an IWL to provide DoD oversight for those IT and NSS activities for which interoperability is deemed critical to mission effectiveness, but interoperability issues are not being adequately addressed with the USD(AT&L), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM. IT and NSS considered for the IWL may be pre-acquisition systems,

acquisition programs (any ACAT), already fielded systems, or Combatant Commander-unique procurements.

5.7.6. Sponsor Joint Test and Evaluations (JT&Es) and, in coordination with the Commander, USJFCOM, and the other DoD Components, identify resulting IT and NSS interoperability and supportability shortfalls and issues.

5.7.7. Provide a senior representative to the ISRP.

5.8. The Heads of the DoD Components shall:

5.8.1. Establish mandatory procedures for implementing the policy, responsibilities, and processes contained in this Instruction and in reference (b).

5.8.1.1. Issue directives, instructions, policy memorandums, or regulations, as necessary, to implement the policy, responsibilities, and procedures of this Instruction. Provide copies of all such documents to the USD(AT&L) and the ASD(NII)/DoD CIO prior to publication.

5.8.1.2. Submit waivers or requests for exceptions to this Instruction to the USD(AT&L), the ASD(NII)/DoD CIO, and the DOT&E, as appropriate. Statutory requirements may only be waived if the statute specifically provides for doing so.

5.8.2. Require the DoD Component Chief Information Officer to:

5.8.2.1. Ensure compliance with this Instruction and the requirements of reference (d).

5.8.2.2. Ensure that the development, implementation, and maintenance of the DoD Component architectures are consistent with the GIG architecture, and support development of ISP architecture product requirements.

5.8.2.3. Advise the DoD Component Head regarding alternatives and solutions to interoperability and supportability issues.

5.8.2.4. Provide policy and guidance to ensure DoD Component IT and NSS are interoperable and supportable with other relevant IT and NSS internal and external to the DoD Component.

5.8.2.5. Advise the ASD(NII)/DoD CIO on implementation of responsibilities and processes contained in this Instruction.

5.8.3. Comply with reference (l), DoD Directive 8500.1, DoD Instruction 8500.2, and DoD Instruction 5200.40 (references (m), (n), and (o)) requirements for IA certification and accreditation. Per DCI Directive 6/3 (reference (p)), certain systems

processing intelligence information or components of such systems must be accredited by the appropriate Designated Approval Authority depending upon the level of information protection required. For Top Secret/Sensitive Compartmented Information and Special Access Program systems, comply with reference (p) and IC CIO TSABI Policy (reference (q)) requirements for IA certification and accreditation.

5.8.4. Ensure IT and NSS interoperability, supportability, and information assurance is designed, developed, tested, evaluated, and incorporated into all DoD Component IT and NSS. When necessary, recommend tradeoffs among operational effectiveness, operational suitability, information assurance, and IT and NSS interoperability and supportability to the USD(AT&L), the ASD(NII)/DoD CIO, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM.

5.8.5. Ensure, for all IT and NSS ACAT acquisitions or procurements, that JCIDS documents (i.e., Initial Capabilities Document (ICD), Capability Development Document (CDD), Capability Production Document (CPD)) are submitted to the Chairman of the Joint Chiefs of Staff and the Commander, USJFCOM, for validation.

5.8.6. Ensure all IT and NSS CDD and CPD documents include a NR-KPP. The NR-KPP shall be used when developing ISPs and test documents.

5.8.7. Identify, and document in an ISP, a NR-KPP for all ACAT, non-ACAT, and fielded IT and NSS acquisitions and procurements, and submit the ISP with NR-KPP to the cognizant authority for review and validation.

5.8.8. Coordinate interoperability needs with the Chairman of the Joint Chiefs of Staff, the Commander, USJFCOM, and the Combatant Commanders, to ensure that the system design identifies all critical external IT and NSS interfaces with required joint, combined, coalition, and other non-DoD systems.

5.8.9. Ensure that:

5.8.9.1. ISPs for all ACAT and non-ACAT acquisitions and procurements are prepared and processed according to procedures contained in enclosure 4. The MDA or cognizant fielding authority shall review, assess, and approve ISPs for ACAT II, III, and non-ACAT programs.

5.8.9.2. All ACAT and non-ACAT ISPs are submitted to the Joint C4 Program Assessment Tool-Empowered (JCPAT-E) repository for further dissemination, as appropriate.

5.8.10. Participate in IT and NSS interoperability and supportability assessment, test, and evaluation by planning, programming, budgeting, and providing resources consistent with accepted schedules and test plans or TEMPs. Resources

include the systems, equipment, and personnel necessary to accomplish IT and NSS interoperability testing.

5.8.11. Assess IT and NSS compliance with the NR-KPP and supportability needs as an element of technical, program, and funding reviews of IT and NSS programs, and document potential IT and NSS interoperability and supportability issues for MDA consideration.

5.8.12. Provide:

5.8.12.1. Direction to acquisition managers to ensure that all ACAT programs using or relying on IT and NSS are submitted to the DISA Joint Interoperability Test Command (JITC) for interoperability test and certification.

5.8.12.2. Results of select developmental and operational interoperability assessments, tests, and evaluations (where significant interoperability issues have been observed) to the USD(AT&L), the ASD(NII)/DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM.

5.8.13. Ensure all test plans are sufficient to verify the NR-KPP, and are submitted to the USD(AT&L) and the DOT&E for approval, as appropriate.

5.8.14. Submit to the DISA (JITC), for IT and NSS interoperability certification, those systems acquired or modified through non-ACAT designated acquisitions or procurements (e.g., ACTDs, JWIDs that lead to acquisitions, the Combatant Command and Control Initiative Program, Combatant Commander Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, and Tactical Exploitation of National Capabilities Programs), DoDIIS, and fielded systems when modified with changes affecting interoperability or supportability. This includes instances where changes to requirements, interfacing systems, or other communications infrastructure impact on interoperability and require re-certification. IT and NSS interoperability testing may be performed in conjunction with other tests to conserve resources.

5.8.15. Develop, in coordination with the USD(AT&L), the DOT&E, and the DISA (JITC), IT and NSS interoperability test and evaluation criteria for inclusion in acquisition and procurement documents, and other test plan submissions.

5.8.16. Ensure, prior to production and fielding decision, all new or modified IT and NSS are tested, evaluated, and interoperability certified, and that all elements of the NR-KPP have been met.

5.8.17. Comply with Chairman of the Joint Chiefs of Staff procedures for interoperability certification. Upon request, an Interim Certificate to Operate (ICTO) may be granted by the Chairman of the Joint Chiefs of Staff or the ASD(NII)/DoD CIO,

as appropriate, when certification has not been achieved and there are urgent operational requirements for fielding. An ICTO shall not be permanent, and normally not exceed 1 year.

5.8.18. Participate in developing programmatic and technical guidance (including NCES/COE), integrated architectures, strategies, IT and NSS standards (including the DISR), and quantifiable performance measures.

5.8.19. Submit Change Requests for adding, deleting, or revising standards contained in the DISR to the IT Standards Committee.

5.8.20. Enforce DISR implementation and establish administrative procedures for submitting Component IT and NSS system-specific DISR waiver requests. A DoD Component Acquisition Executive (CAE), Component CIO, or cognizant official, as appropriate, may grant a waiver from use of DISR-mandated standards where potential negative impacts to cost, schedule, or performance are identified.

5.8.20.1. For mission-critical or mission-essential ACAT designated programs, all granted waivers shall be submitted through the ASD(NII)/DoD CIO to the USD(AT&L) for review and concurrence.

5.8.20.2. Waivers for non-ACAT acquisitions and procurement shall be submitted to the ASD(NII)/DoD CIO for review and concurrence.

5.8.20.3. Concurrence may be assumed if no response is received within 2 weeks of the date of submittal.

5.8.21. Include DISA (JITC)-approved standards conformance testing events and procedures in interoperability test plans.

5.8.22. Participate in DoD efforts to influence development of non-Government standards for interoperability and supportability of IT and NSS.

5.8.23. Participate in Configuration Management (CM) of IT standards, standards profiles, and Key Interface Profiles (KIPs).

5.8.24. Generate STARs that highlight threats to IT and NSS interoperability and supportability.

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

5.9.1. Establish policy and procedures for developing, coordinating, reviewing, and approving IT and NSS interoperability and supportability needs, in coordination with the Commander, USJFCOM, and the other DoD Components.

5.9.2. Direct the use of integrated architectures when defining the NR-KPP. Review, certify and validate the NR-KPP contained in JCIDS documents and OSD-designated Special Interest ISPs.

5.9.3. Develop, approve, and issue Joint Operational Concepts (JOCs), Joint Functional Concepts (JFCs), and associated doctrine and operational procedures, in coordination with the USD(AT&L), the ASD(NII)/DoD CIO, the Commander, USJFCOM, and the other DoD Components, to achieve interoperability and supportability of IT and NSS employed by U.S. Military Forces and, where required, with joint, combined, and coalition forces, and other U.S. Government Departments and Agencies.

5.9.4. Provide advice to the DoD Components so that integrated architectures, strategies, concepts, and visions of the DoD Components support IT and NSS interoperability. Identify opportunities for, and impediments to, interoperability.

5.9.5. Allocate resources, in coordination with the ASD(NII)/DoD CIO, to manage and develop KIPs.

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

5.9.7. Coordinate among and furnish advice, guidance, direction, and assistance to the DoD Components for IT and NSS interoperability and supportability matters.

5.9.8. Establish, in coordination with the Commander, USJFCOM, processes and procedures to ensure insights gained from joint operations, exercises, and experiments on IT and NSS interoperability and supportability are presented to the USD(AT&L), the ASD(NII)/DoD CIO, and the DOT&E.

5.9.9. Validate, with the assistance of the DISA, that IT and NSS interoperability and supportability is assessed and certified for IT and NSS acquisitions prior to production and fielding.

5.9.10. Through the MCEB and the MIB, consider interoperability and supportability matters referred to it by the Secretary of Defense, the ASD(NII)/DoD CIO, and the Commander, USJFCOM. These Boards shall:

5.9.10.1. Convene a senior resolution body for IT and NSS interoperability and supportability requirements and testing issues in accordance with DoD Directive 5100.35 and DoD Directive 5105.21 (references (r) and (s)).

5.9.10.2. Coordinate issues presented to the boards among the DoD Components, between the Department of Defense and other Government Departments and Agencies, and between the Department of Defense and representatives of foreign nations.

5.9.10.3. Coordinate with the other DoD Components to resolve IT and NSS interoperability and supportability conflicts and conformance issues. If resolution of IT and NSS interoperability and supportability issues cannot be achieved within the MCEB or MIB process, the cognizant board shall refer it to the ASD(NII)/DoD CIO for review.

5.9.11. Provide a senior representative to the ISRP.

5.10. The Commander, U.S. Joint Forces Command, shall:

5.10.1. Establish a Joint Interoperability and Integration (JI&I) organization involving the operational community to identify, consolidate, prioritize, and synchronize materiel and non-materiel solutions for resolution of IT and NSS interoperability and supportability issues. The JI&I shall:

5.10.1.1. Define and advocate DOTMLPF-synchronized solutions with the DoD Components for near-term interoperability shortfalls.

5.10.1.2. Propose solutions (including programmatic means for inclusion in the POM) to the appropriate DoD Components. A transition fund shall address high-priority fielded IT and NSS interoperability issues requiring resolution.

5.10.2. Participate in the JCIDS process for IT and NSS. Review and comment on the sufficiency of the NR-KPP, for a given capability, to assess and evaluate IT and NSS interoperability. This assessment shall be based on the warfighter's perspective using integrated architectures.

5.10.3. Determine, in coordination with the Chairman of the Joint Chiefs of Staff, the operational impacts of select DISA (JITC) IT and NSS interoperability test and certification results and provide results of these operational impact assessments to the USD(AT&L), the ASD(NII)/DoD CIO, the DOT&E, and the other DoD Components, as appropriate.

5.10.4. Collect, consolidate, and prioritize the IT and NSS interoperability and supportability needs for emerging and fielded Joint Task Force systems using the DoD Components' inputs. Assess the current operational force against required capabilities to determine the impact on warfighting readiness. Leverage existing repositories of the Chairman of the Joint Chiefs of Staff, Agencies, and the ASD(NII)/DoD CIO for these issues, to produce a consolidated priority list of interoperability and supportability shortfalls.

5.10.5. Participate, as appropriate, in assessing, testing, and evaluating IT and NSS interoperability and supportability. The Commander, U.S. Joint Forces Command, as the Chairman's Advocate for interoperability, may require selected programs and systems for interoperability demonstrations using the Joint C4ISR Battle Center's (JBC) Interoperability Technology Demonstration Center (ITDC).

5.10.6. Propose to the USD(AT&L), the ASD(NII)/DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the other DoD Components and Agencies new or modified procedures for joint operational assessments, tests, and evaluations to identify, prioritize, and document IT and NSS interoperability and supportability deficiencies.

5.10.7. Coordinate and integrate the efforts of the DoD Components to ensure IT and NSS, materiel and non-materiel solutions are conceived and developed in an integrated joint warfighting context that addresses interoperability and supportability, as specified in Management Initiative Decision 912 (reference (t)) and the JCIDS process.

5.10.8. Review and endorse, on an annual basis, a prioritized list of materiel and non-materiel warfighting IT and NSS capability gaps, as specified in reference (t) and the JCIDS process. As part of that review, ensure the gaps address interoperability needs.

5.10.9. Provide recommendations regarding the Joint Potential Designation of materiel and non-materiel interoperability solutions.

5.10.10. Provide a senior representative to the ISRP.

5.11. The Director, Defense Information Systems Agency, shall:

5.11.1. Manage and conduct the Joint IT and NSS Interoperability Assessment, Test, and Evaluation Program, in collaboration with the other DoD Components. The DISA (JITC) shall certify joint and combined IT and NSS interoperability for the Department of Defense.

5.11.2. Certify IT and NSS conformance with DISR standards during joint interoperability certification testing by the DISA (JITC).

5.11.3. Coordinate with the DoD Components to resolve IT and NSS interoperability issues. If resolution cannot be achieved, provide an impact statement and recommendations for resolution to the MCEB or MIB, as appropriate.

5.11.4. Submit an annual report containing an executive summary of systems tested for IT and NSS interoperability, and relevant information regarding test certification to the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DPA&E, the DOT&E, the Chairman of the Joint Chiefs of Staff, the Commander,

USJFCOM , the other DoD Components, and to the developmental and operational testing organizations of the DoD Components.

5.11.5. Provide systems engineering, planning, and program guidance. The DISA shall also assist the DoD Components with developmental IT and NSS interoperability testing to implement solutions, minimize duplication of effort, facilitate maximum IT and NSS interoperability and supportability, and ensure spectrum management responsibilities of DoD Directive 4650.1 (reference (u)) consider spectrum supportability, and control of Electromagnetic Environmental Effects. The DISA shall make DISR-compliant and NSA/CSS-verified platform solutions available to the DoD Components for proof-of-concept, prototyping, and IT and NSS development. The DISA shall also ensure that the DoD Components have access to DISR-compliant/NSA/CSS-verified router, local area network, and network security solutions.

5.11.6. Review DoD Component JCIDS documentation, TEMPs, and ISPs to assess if the NR-KPP and test objectives are adequately defined. Conduct standards profile reviews and provide recommendations on planned IT and NSS interoperability assessments, tests, and evaluations. Incorporate results of reviews into systems engineering, planning, and program guidance provided to the DoD Components.

5.11.7. Review TEMPs, or equivalent documents, and recommend IT and NSS interoperability test and evaluation criteria for test plans.

5.11.8. Establish an assessment process and repository for select JCIDS documentation and all ISPs (all ACAT and non-ACAT). Coordinate with the ASD(NII)/DoD CIO and the Chairman of the Joint Chiefs of Staff to ensure proposed inputs to the repository are consistent with appropriate techniques, procedures, architectures, and DISR standards.

5.11.9. Serve as the DoD Executive Agent for developing and prescribing IT and NSS standards that apply to interoperability throughout the Department of Defense. Coordinate, integrate, and configuration manage DoD IT standards activities and processes to ensure compliance with IT and NSS standards.

5.11.10. Chair and provide staff and administrative support to the IT Standards Committee for identification, cross-functional integration and technical collaboration of IT standards.

5.11.11. Maintain the DISR consisting of approved IT standards and standards profiles to aid program and project managers, acquisition authorities, and systems and technical architects in the development and fielding of interoperable and net-centric enabled systems and products. Establish process and procedures for life-cycle CM of IT standards contained in the DISR. Provide on-line Non-Classified IP Router Network (NIPRNET) and Secret IP Router Network (SIPRNET) access to the DISR. The DISA

shall ensure there is a linkage between the IT standards contained in the DISR and the Acquisition Streamlining and Standardization Information System database.

5.11.12. Establish, in coordination with the Chairman of the Joint Chiefs of Staff and the DoD Components, processes and procedures for enforcing IT standards compliance, through requirements and/or capabilities document reviews, the DoD acquisition and procurement process, and standards compliance verification.

5.11.13. Establish, in coordination with the DoD Components, specific testing methodologies for DoD Components and test facilities to conduct standards validation, standards conformance, and systems interoperability testing.

5.11.14. Provide an assessment of the suitability of standards identified for use by the Department of Defense. The DISA shall forward standards issues that cannot be resolved to the MCEB, MIB, or Defense Standardization Council, as appropriate.

5.11.15. Coordinate with national and international standards bodies and provide guidance in establishing the appropriate abstract test suites and methodology for standards validation, standards conformance, and interoperability testing.

5.11.16. Provide guidance, assistance, and information on appropriate use of standards, the development of standards profiles, the applicability of standards to functional areas (e.g., networking), system domains (e.g., intelligence), and program phases (e.g., use of existing standards for imminent acquisitions and use of emerging standards for long-range program planning).

5.11.17. Allocate resources, manage and develop GIG KIPs in support of the ASD(NII)/DoD CIO and the Chairman of the Joint Chiefs of Staff.

5.11.18. Ensure that test documentation and ISPs identify DISR-mandated standards and NCES/COE technical measures and technologies required for IT and NSS standards conformance. Conduct associated standards profile reviews and provide recommendations to the USD(AT&L), the ASD(NII)/DoD CIO, the DOT&E, and the Chairman of the Joint Chiefs of Staff on planned IT and NSS interoperability assessments, tests, and evaluations.

5.11.19. Certify, through the DISA (JITC), to the Operational Test Agency (OTA) during (or prior to) the Operational Test Readiness Review (OTRR) the following:

5.11.19.1. Status of all IT and NSS interoperability and standards conformance issues.

5.11.19.2. That all required Developmental Testing (DT) relating to IT and NSS interoperability has been successfully completed.

5.11.19.3. That no outstanding issues preventing the commencement of Operational Test and Evaluation (OT&E) remain.

5.11.20. Assess compliance with bilateral and multilateral standardization agreements (STANAGs) (e.g., U.S.-ratified NATO STANAGs).

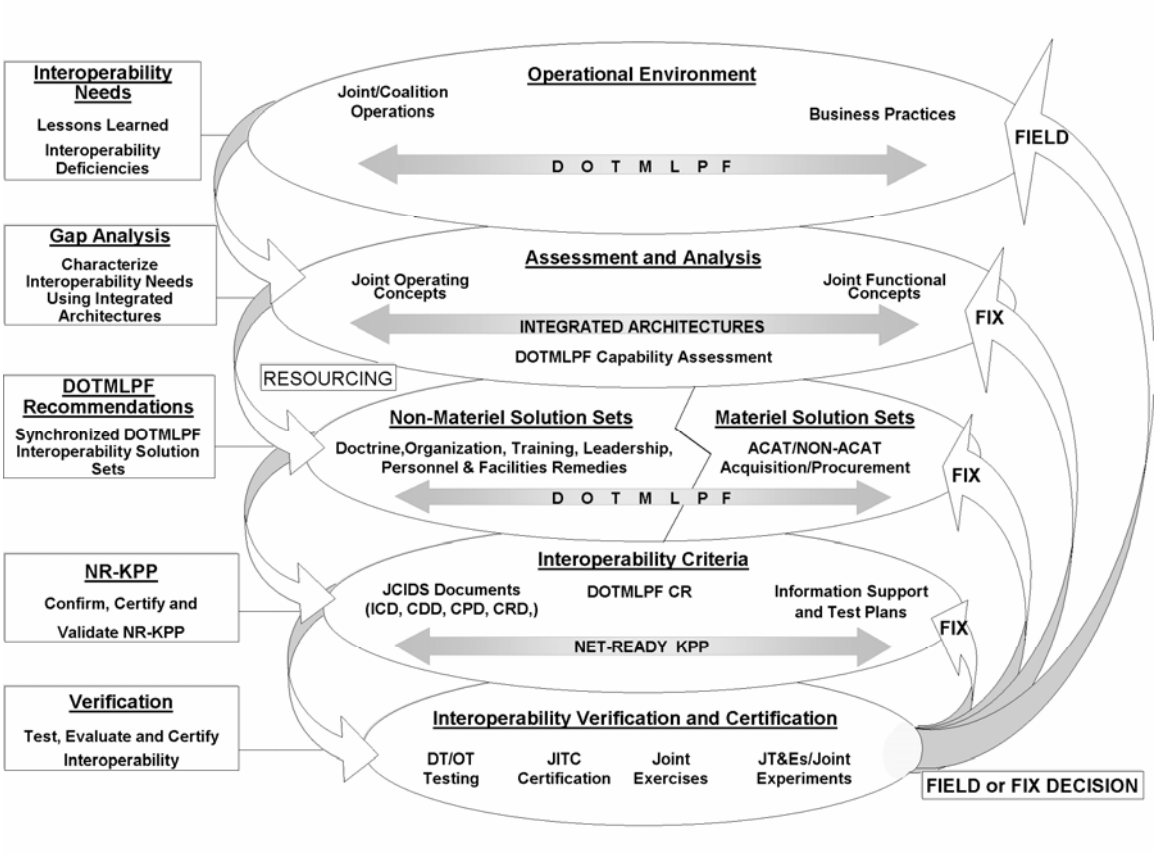
6. PROCEDURES

6.1. Capability-Focused, Effects-Based IT and NSS Interoperability Process Overview

6.1.1. Decision superiority is the state at which better decisions are arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. To achieve decision superiority, IT and NSS systems must be interoperable and supportable, and must exchange and use relevant information in a timely manner to operate together effectively. The required interoperability between systems shall be determined based on an evaluation of the functional role of the system(s) comprising a given capability.

6.1.2. A capability-focused, effects-based IT and NSS interoperability process shall serve as the foundation for all DoD IT and NSS interoperability and supportability initiatives. This approach addresses JCIDS, acquisition and procurement, and resource allocation processes. Figure F1. illustrates the capability-focused, effects-based process for achieving IT and NSS interoperability and is further discussed in the following paragraphs.

Figure F1. Capability-Focused, Effects-Based Interoperability Process



6.1.3. This approach for achieving IT and NSS interoperability is an iterative process that begins with an assessment of the operational environment to identify interoperability, supportability, and IA needs using JOCs, JFCs, associated integrated architectures, experience gained from joint/coalition operations, business practices, and evaluation of DOTMLPF solutions. Integrated architectures shall be used as the basis for assessment and analysis to characterize interoperability needs for a given capability. Solutions to the identified needs may be materiel or non-materiel solution sets, or both. Interoperability needs shall be documented in applicable capabilities documents and the NR-KPP. System information and interoperability dependencies and supportability requirements shall be documented in an ISP. Regardless of the solution (materiel or non-materiel), interoperability and supportability shall be tested and verified prior to operational use or fielding. Specifically, this process:

6.1.3.1. Includes experts from the operational community to identify, consolidate, and prioritize interoperability needs; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities.

6.1.3.2. Characterizes IT and NSS interoperability needs in a capability-focused, effects-based context using integrated architectures derived from the JOCs and JFCs.

6.1.3.3. Assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

6.1.3.4. Incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership and education, personnel, and facilities) solutions.

6.1.3.5. Verifies interoperability solutions in formal tests or operational exercises.

6.1.3.6. Continuously evaluates the NR-KPP and verifies overall IT and NSS interoperability, for a given capability, throughout a system's life.

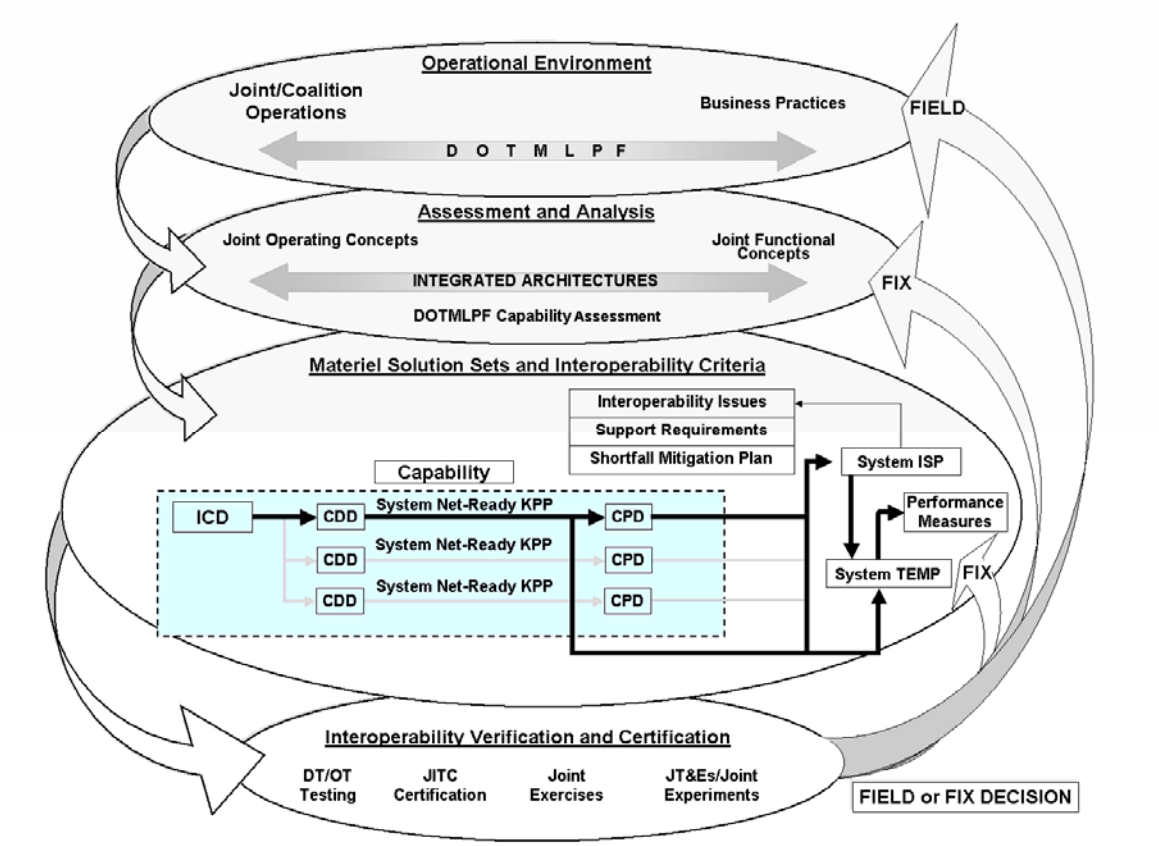
6.1.4. Integrated Architectures. Integrated architectures are the common foundation for capability-focused, effects-based IT and NSS interoperability and supportability processes for ACAT-designated acquisitions, non-ACAT acquisitions or procurements, and fielded capabilities.

6.1.4.1. The DoD Components shall define and relate IT and NSS interoperability needs using integrated architectures derived from JOCs and JFCs.

6.1.4.2. Integrated architectures include a representation (often graphical) of the processes, systems, and system interfaces. As described in reference (g), an integrated architecture is comprised of three views. These views are the Operational View (OV) describing the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions; the Systems View (SV) describing (including graphics) systems and interconnections providing for, or supporting, DoD functions; and the Technical Standards View (TV) describing the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements.

6.2. Interoperability Process for ACAT-Designated IT and NSS Acquisitions. Figure F2. depicts the capability-focused, effects-based, interoperability and supportability process template for ACAT-designated IT and NSS. Essential elements for acquisition, JCIDS, and test documentation are described below.

Figure F2. ACAT IT and NSS Acquisition Process



6.2.1. ACAT IT and NSS Acquisition Process Overview

6.2.1.1. The operational or business environment establishes the need for new capabilities. Integrated architectures define IT and NSS interoperability needs for the operational and technical communities. Joint capability needs for ACAT-designated acquisition programs are documented through the JCIDS process using ICDs, CDDs, and CPDs. The ICD reflects the results of the JCIDS assessment and analysis conducted in response to a capability gap. The CDDs and CPDs document key performance parameters including the required NR-KPP for ACAT-designated programs. References (j) and (k) guide ACAT-designated IT and NSS acquisitions.

6.2.1.2. AoA. The AoA, as described in reference (k), consists of a broad examination of program alternatives to include technical risk, maturity, and cost. The AoA shall be quantitative and comprehensive, examining the full range of alternatives over the full life cycle to meet the mission requirements, as documented in the associated ICD. The AoA alternatives shall contain all of the materiel solution sets that satisfy the NR-KPP. Alternatives should be compared to the existing systems or capabilities. The DPA&E shall assess, review, and provide a recommendation to the MDA for approval of the AoA.

6.2.1.3. NR-KPP. The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP, documented in CDDs and CPDs, shall be used in analyzing, identifying, and describing IT and NSS interoperability needs in the ISP; and test strategies in the TEMP. The NR-KPP is comprised of the following elements:

6.2.1.3.1. Compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM). The NCOW RM (reference (v)) describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest (COI) services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the GIG are realized.

6.2.1.3.2. Compliance with Applicable GIG KIPs. GIG KIPs provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. A KIP is the set of documentation produced as a result of interface analysis, which designates an interface as key; analyzes it to understand its architectural, interoperability, test and CM characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Engineering Management Plan, CM Plan, TV-1 with SV-TV Bridge, and procedures for standards conformance and interoperability testing. Relevant GIG KIPs, for a given capability, shall be documented in the CDD and CPD. Compliance with identified GIG KIPs shall be analyzed during the development of the ISP and TEMP, and assessed during DISA (JITC) joint interoperability certification testing. Since all of the GIG KIPs have not been developed, the following applies:

6.2.1.3.2.1. The Chairman of the Joint Chiefs of Staff shall continue the development of the GIG KIPs.

6.2.1.3.2.2. The Chairman of the Joint Chiefs of Staff shall continue the well-defined, phased implementation of the GIG KIPs, to be completed by Fiscal Year 2006.

6.2.1.3.2.3. The DISA shall maintain completed GIG KIPs in the DISR.

6.2.1.3.3. Compliance with DoD Information Assurance Requirements. Verification of compliance with DoD IA requirements specified in references (l) through (q).

6.2.1.3.4. Supporting Integrated Architecture Products. The following integrated architecture products described in reference (e) shall, as a minimum, be incorporated in the NR-KPP and used to assess information exchange and use for a given capability:

Table T1. Architecture Products Required to Assess Information Exchange and Use

Framework Product	Framework Product Name	General Description
V-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
OV-2	Operational Node Connectivity Description	Operational Nodes, operational activities performed at each node, connectivity and information exchange between nodes
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
OV-5	Operational Activity Model	Operational Activities, relationships among activities, inputs and outputs. Overlays can show cost, performing nodes, or other pertinent information.
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity sequence and timing - traces actions in a scenario or sequence of events and specifies timing of events
SV-4	Systems Functionality Description	Functions performed by systems and the information flow among system functions
SV-5	Operational Activity to System Function Traceability Matrix	Mapping of systems back to operational capabilities or of system functions back to operational activities
SV-6	Systems Data Exchange Matrix	Provides details of systems data being exchanged between systems
TV-1	Technical Standards Profile	Extraction of standards that apply to the given architecture

6.2.1.4. ISPs and TEMPs. IT and NSS interoperability needs shall drive testing constructs within the program's TEMP and the development of the program's ISP.

6.2.1.4.1. The ISP shall document the program's interoperability, information, and support requirements for the program. The ISP shall also document interoperability and supportability shortfalls for the program of record and propose shortfall mitigation plans (as applicable). Major interoperability and supportability program issues identified in the ISP shall be captured and maintained in an ASD(NII)/DoD CIO database.

6.2.1.4.2. The program's TEMP shall reflect interoperability and supportability requirements, as described in the CDD, CPD, and ISP, and shall serve as the basis for IT and NSS interoperability assessment through measurable, performance-based criteria to verify overall IT and NSS interoperability and supportability.

6.2.1.5. The DISA (JITC) shall evaluate and certify all IT and NSS, for all ACAT programs for interoperability. IT and NSS interoperability test and evaluation shall be conducted throughout a system's life, and should be initially achieved as early as is practical to support scheduled acquisition or procurement decisions. The cognizant MDA shall address critical interoperability or supportability issues remaining at the time of the milestone decision.

6.2.2. JCIDS, Acquisition, and Test Documentation

6.2.2.1. ICD. The ICD describes capability gaps in joint warfighting functions as described in the applicable JFC and integrated architectures. It establishes the need for a materiel approach to resolve a specific capability gap derived from the JCIDS assessment and analysis process. The ICD defines the capability gap in terms of the functional area(s), the relevant range of military operations, time, obstacles to overcome, and key attributes with appropriate measures of effectiveness, e.g., distance, effect (including scale), etc. The ICD describes the recommended approach to best satisfy the desired joint capability. It also supports the AoA by providing operational context for assessing the performance characteristics of alternatives. The ICD serves as the baseline document for linking related CDDs and CPDs, including overarching DOTMLPF aspects necessary to develop an effective capability. Identification of the NR-KPP is not required in the ICD.

6.2.2.2. CDD. The CDD captures information necessary to develop a proposed program(s), usually using an evolutionary acquisition strategy. The CDD outlines an affordable increment of capability. An increment is a militarily useful and supportable operational capability that can be effectively developed, produced or acquired, deployed, and sustained. Each increment of capability possesses its own set of attributes and associated performance values with thresholds and objectives established by the sponsor with input from the user. The CDD provides the operational performance attributes, including interoperability and supportability, necessary for the acquisition community to design the proposed system. The CDD references the originating ICD, identifies other CDDs and/or CPDs that are required for full realization of the capability(ies), and describes the synchronization required between programs. The CDD also references any additional overarching DOTMLPF aspects necessary to develop an effective capability. The NR-KPP shall be defined by the acquiring authority, certified by the Chairman of the Joint Chiefs of Staff, and documented in the CDD.

6.2.2.3. CPD. The CPD captures the information necessary to support production, testing, and deployment of an affordable and supportable increment within an acquisition strategy. The CPD provides the operational performance attributes necessary

for the acquisition community to produce a single increment of a specific system. It presents performance attributes, including KPPs, to guide the production and deployment of the current increment. CPD development is guided by the integrated architectures, relevant JCIDS documentation, the AoA or supporting analytical results, developmental and operational test results, and the design readiness review. A NR-KPP, certified by the Chairman of the Joint Chiefs of Staff, shall be documented in the CPD.

6.2.2.4. TEMPs. Reference (k) identifies requirements for submission of TEMPs. The TEMP shall document the overall structure and objectives of the tests that shall be performed to evaluate and verify IT and NSS interoperability. TEMPs address how key IT and NSS interfaces shall be tested. Test issues and measurable test parameters shall be derived from the NR-KPP, found in the CDD, CPD, and ISP, and operational performance requirements specified in doctrine and Tactics, Techniques, and Procedures (TTPs).

6.2.2.5. Information Support Plans

6.2.2.5.1. ISPs for ACAT I and IA, and other acquisition programs the ASD(NII)/DoD CIO has designated as Special Interest, are submitted to the ASD(NII)/DoD CIO for review and assessment.

6.2.2.5.2. Should interoperability issues arise between ACAT I or IA and ACAT II and III programs, the DoD Components shall, if requested, provide the ISP for the ACAT II and III program(s) to the ASD(NII)/DoD CIO to support issue resolution.

6.2.2.5.3. The DoD Components shall develop an ISP for all ACAT-designated programs. Format, content, and process for the ISP provide a mechanism to identify and resolve implementation issues related to IT and NSS infrastructure and support elements. ISPs shall identify IT and NSS information needs, dependencies, and interface requirements, focusing on interoperability, supportability, and sufficiency. The ISP shall include an operational employment concept; system interface descriptions; required information exchanges; IT and NSS information support requirements derived from analysis of applicable JOCs, JFCs, and JCIDS documentation, and the associated integrated architecture(s); potential issues; and proposed solutions. IT and NSS systems dependencies and interface requirements shall be described in sufficient detail to enable test planning for verification of the NR-KPP. The ISP enables the DoD Components to conduct IT and NSS supportability reviews for all ACAT-designated programs. Enclosure 4 contains specific ISP preparation and review procedures, formats, and timelines.

6.2.2.5.4. The DoD Components shall identify IT and NSS interoperability requirements, infrastructure, and other support requirements early in the acquisition life cycle. The DoD Components shall prepare the initial ISP concurrently and collaboratively with the associated CDD or CPD, but initially with sufficient time to

accommodate associated document reviews prior to the associated Milestone. The ISP process shall depend upon capability performance parameters and the operational context developed in the JCIDS process; and the refinement of the NR-KPP first identified in the CDD must consider the outputs of the ISP process as identified in enclosure 4. ISPs shall be maintained throughout the acquisition life cycle. At each milestone review, ISPs shall contain progressively more detailed and specific time-phased descriptions of the types of information needed, operational, systems, and technical architecture views; security, connectivity, and interoperability issues; and infrastructure and support issues.

6.2.3. IT and NSS Interoperability Verification and Certification

6.2.3.1. Test Documentation. The TEMPs shall state the NR-KPP for the evaluation of IT and NSS interoperability and shall specify IT and NSS interoperability test concepts. The TEMPs shall reference and extract requirements and critical operational and technical parameters to be tested and evaluated from the appropriate JOCs, JFCs, JCIDS documents, ISPs, and integrated architectures, and TTPs. The Chairman of the Joint Chiefs of Staff shall ensure that all appropriate JCIDS documents contain verifiable performance measures and associated metrics required to evaluate the NR-KPP. The USD(AT&L) and the ASD(NII)/DOD CIO shall ensure that the ISP and integrated architectures reflect the appropriate capability context to support the system's IT and NSS interoperability needs. The OTAs, the Chairman of the Joint Chiefs of Staff, and the system's user or program proponent, with DISA (JITC) and DoD Component interoperability testing organizations, respectively, shall develop the IT and NSS interoperability test procedures and measures of performance based on the IT and NSS needs and expected concepts of operations for the system. The OTAs may develop additional operational issues and measures to add to the TEMP and test plans based on reference (k).

6.2.3.2. DT. The objective of DT is to provide decision-makers with accurate assessments of the technical capabilities and limitations of the system under test and to reduce program risk by identifying technical interoperability problems early on. Both contractor and Government DT should assess whether specific technical parameters (including standards, protocols, and interface controls) have been adequately demonstrated before formal Operational Testing (OT) begins. The DISA shall provide input to this process to ensure that DT provides sufficient information for standards conformance certifications.

6.2.3.3. Operational Assessments (OAs). An objective of OAs is to reduce program risk by identifying potential operational problems early on. An assessment shall be conducted by the OTA and DISA (JITC) concerning the viability of plans and resources to test and evaluate IT and NSS interoperability and shall be presented at Milestone B or at the System Integration Milestone, whichever comes first, and at subsequent milestones. Such OAs should leverage the Preliminary and Critical Design Reviews, DT, and other appropriate sources (e.g., information assurance testing) to produce IT and NSS interoperability assessments.

6.2.3.4. OTRRs. All available interoperability assessments (e.g., OAs, DISA (JITC) IT and NSS interoperability assessments, certifications, and standards conformance reports) should be reviewed during the OTRR before OT&E. OTRRs shall assess IT and NSS interoperability results from DT and the DISA (JITC) also shall provide recommendations regarding IT and NSS readiness for interoperability certification testing. Potentially critical IT and NSS interoperability and supportability issues must be highlighted for assessment during OT&E.

6.2.3.5. OT. The DOT&E and the OTAs shall develop guidelines to assist in evaluating overall IT and NSS interoperability. Operational test plans, coordinated with the DISA (JITC), shall include the IT and NSS interoperability evaluation and supporting measures critical to operational effectiveness. OT of IT and NSS interoperability shall focus on both the ability of the subject system to exchange information and services accurately and in a timely manner, and the effect of IT and NSS interoperability on mission accomplishment. The OTAs and the DISA (JITC) shall use the results of the OT&E to evaluate IT and NSS interoperability. These evaluations shall assess the adequacy of interoperability in the accomplishment of the mission for the proposed system within the context of the system's intra-DoD Component and inter-Component (including joint, combined, coalition, and other U.S. Government Departments and Agencies) operational environment. These evaluations shall support DISA (JITC) IT and NSS interoperability certification.

6.2.3.6. IT and NSS Interoperability Certification Testing

6.2.3.6.1. All IT and NSS, regardless of ACAT, must be tested for interoperability before fielding and the test results evaluated and systems certified by the DISA (JITC). IT and NSS interoperability test and evaluation shall be conducted throughout a system's life, and should be achieved as early as is practical to support scheduled acquisition or procurement decisions. Interoperability testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early-user test) whenever possible to conserve resources.

6.2.3.6.2. IT and NSS interoperability testing can occur in multiple stages. Evolutionary acquisitions or procurements, and normal life-cycle modifications, result in a progressively more complete capability. Therefore, there may be instances when it is important to characterize a system's interoperability before all critical interface requirements have been tested and certified. However, all critical interfaces, identified in the NR-KPP, which have been tested, must be successfully certified for interoperability prior to fielding. When appropriate (e.g., between successful completion of OT and the fielding decision), the DISA (JITC) shall issue interim interoperability certification letters specifying which of the system's interoperability needs have been successfully met and which have not. The DISA (JITC) shall issue an overall system certification once the system successfully meets all requirements of the NR-KPP validated by the Chairman of the Joint Chiefs of Staff. The DISA (JITC) shall provide interoperability certification letters to the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DPA&E, the

DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, as well as to the OTA and program manager, as applicable.

6.2.3.6.3. The Chairman of the Joint Chiefs of Staff shall validate that the NR-KPP, in approved JCIDS documents and ISPs, is adequately verified as part of the interoperability and supportability certification process.

6.2.3.6.4. The Commander, U.S. Joint Forces Command, as the Chairman's Advocate for interoperability, may require selected programs and systems for interoperability demonstrations using the JBC's ITDC.

6.2.3.7. Interoperability Reviews. IT and NSS shall be subject to interoperability reviews over the life of a system to determine if interoperability objectives are being met. The USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DOT&E, the DPA&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, shall review and assess interoperability to identify IT and NSS interoperability deficiencies. Multiple sources may be used to identify IT and NSS interoperability deficiencies including JCIDS documents; ISPs; TEMPs and operational test plans; and observation of tests and exercises by the DOT&E and the OTAs, the USJFCOM interoperability priority list, the Joint Warfighting Capability Assessments, program management offices, the MCEB, the MIB, the DISA, DoD Component interoperability testing organizations, and the Joint C4ISR Battle Center. Identified IT and NSS interoperability deficiencies may pertain to both the technical exchange of information and the end-to-end operational effectiveness of that exchange required for mission accomplishment.

6.2.3.8. IWL

6.2.3.8.1. IT and NSS with significant interoperability deficiencies (as determined by the offices of the USD(AT&L), the USD(C)/CFO, the USD(I), the ASD(NII)/DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM), shall be placed on the IWL to ensure that sufficient attention is given to achieving and maintaining interoperability objectives. The IWL shall be updated and coordinated quarterly with the ISRP. Criteria for nominating programs to the IWL include, but are not limited to:

6.2.3.8.1.1. No plans for DISA (JITC) joint interoperability certification testing.

6.2.3.8.1.2. Failed DISA (JITC) joint interoperability certification test and no plans for addressing the identified deficiencies.

6.2.3.8.1.3. Operational problems noted with TTPs, and training that impact joint interoperability for fielded (legacy) systems.

6.2.3.8.1.4. Lack of JCIDS or test documentation for defense technology projects and pre-acquisition demonstrations (e.g., ACTDs, JT&Es, and JWIDs that lead to acquisitions), the Combatant Command and Control Initiative Program, Combatant Commander Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, Tactical Exploitation of National Capabilities Programs, DoDIIS, post-acquisition (fielded) IT and NSS systems, and modifications to fielded IT and NSS capabilities.

6.2.3.8.1.5. Known significant joint interoperability deficiencies observed during operational exercises or real world operations.

6.2.3.8.1.6. Capability or net-centric warfare joint interoperability certification issues.

6.2.3.8.1.7. Unresolved issues from other activities concerned with interoperability (MCEB, MIB, Overarching Integrated Product Teams (OIPTs)).

6.2.3.8.1.8. Non-compliance with approved integrated architectures.

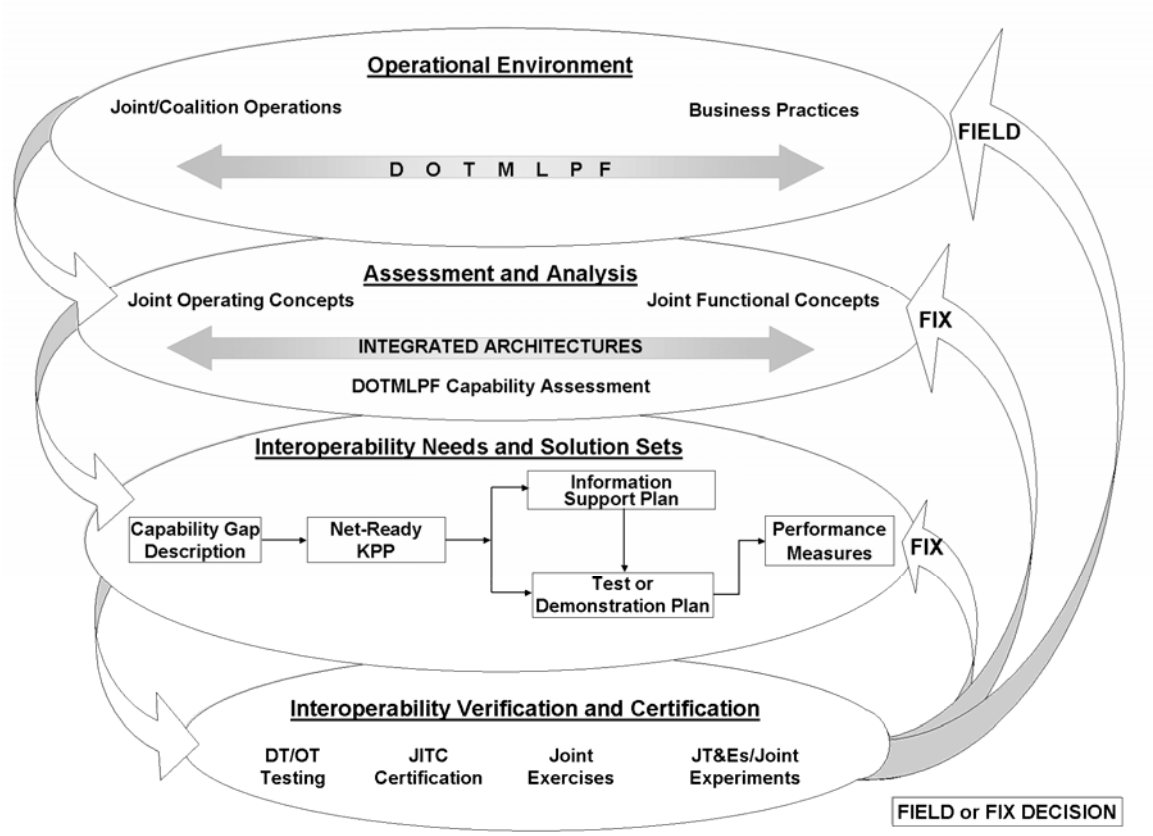
6.2.3.8.1.9. Non-compliance with the Commander, USJFCOM Standing Joint Forces Headquarters (SJFHQs) DOTMLPF recommendations for common architectures, Joint TTPs, and Standard Operating Procedures for the SJFHQs.

6.2.3.8.2. Program managers (or the operating/sponsoring command), and the responsible test organization (either developmental or operational), with DISA (JITC), shall provide periodic updates of current status of correcting identified IT and NSS interoperability deficiencies for those systems on the IWL to the USD(AT&L), the USD(C)/CFO, the USD(I), the ASD(NII)/DoD CIO, the DOT&E, the DPA&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM. These updates shall support an assessment by the USD(AT&L), the USD(C)/CFO, the USD(I), the ASD(NII)/DoD CIO, the DOT&E, the DPA&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, that shall determine if IT and NSS interoperability issues are being adequately addressed, and whether a change in status is warranted (e.g., whether the IT or NSS should be removed from the IWL or transferred to the Office of the Secretary of Defense T&E Oversight List).

6.3. Non-ACAT IT and NSS Acquisitions and Procurements Process. Figure F3. illustrates the capability-focused, effects-based, interoperability and supportability process for non-ACAT IT and NSS acquisitions and procurements. This process applies to IT and NSS under consideration for operational use, but being acquired or procured outside of the ACAT program processes described in references (j) and (k). Included in this category are all defense technology projects and pre-acquisition demonstrations (e.g., ACTDs, JT&Es, and JWIDs that lead to acquisitions), the Combatant Command and Control Initiative Program, Combatant Commander Field Assessments, Military

Exploitation of Reconnaissance and Technology Programs, Tactical Exploitation of National Capabilities Programs, DoDIIS, post-acquisition (fielded) IT and NSS systems, and modifications to fielded IT and NSS capabilities.

Figure F3. Non-ACAT IT and NSS Acquisition and Procurement Process



6.3.1. Non-ACAT IT and NSS Acquisition and Procurement Process Overview

6.3.1.1. The procurement of non-ACAT IT and NSS has attained an unprecedented level of importance, impact, and visibility in the Department of Defense. This is due, in part, to the Department of Defense's policy of using Government-Off-The-Shelf, Non-Developmental Items and Commercial-Off-The-Shelf (COTS)-based solutions wherever possible; industry dominance in the development of new IT systems; and the critical impact of new IT and NSS (regardless of their source) on interoperability. To better manage interoperability and supportability of IT and NSS, the capability-focused, effects-based process (defines the NR-KPP, and tests interoperability prior to fielding), used for ACAT programs, shall also be used to the maximum extent practicable for non-ACAT acquisition and procurements. If the acquisition or procurement of non-ACAT IT or NSS or services transitions to an acquisition program, then it shall be managed and fielded per the DoD 5000 series guidance (references (j) and (k)).

6.3.1.2. IT or NSS procured or acquired outside of the ACAT program process shall document interoperability needs, dependencies and supportability requirements in an ISP, and verify interoperability and supportability prior to operational use or fielding. Unresolved critical interoperability or supportability issues, identified during interoperability test and evaluation, shall be reviewed and assessed by the ISRP. Where necessary, the ISRP shall approve appropriate candidates for the IWL. The sponsoring or cognizant organization shall develop and tailor, and the USD(AT&L), the ASD(NII)/DoD CIO, and the DOT&E shall review, specific DoD Component procedures for non-ACAT acquisitions and procurements.

6.3.2. Non-ACAT Interoperability Needs and Test Documentation. The subparagraphs below describe essential elements required for non-ACAT acquisitions and procurements. Interoperability needs for non-ACAT acquisitions and procurements shall be derived from relevant integrated architectures, for a given capability. IT and NSS interoperability needs shall be documented in an ISP to a level of detail suitable for deriving the NR-KPP. An AoA for non-ACAT IT and NSS shall quantitatively analyze all alternatives that satisfy the interoperability requirements at a level that allows reliable replication of the calculation method. The cost, schedule, and technical characteristics of the alternatives shall be compared to the existing systems or capabilities. The sponsoring or cognizant authority shall review, assess, and approve the AoA and associated requirements document.

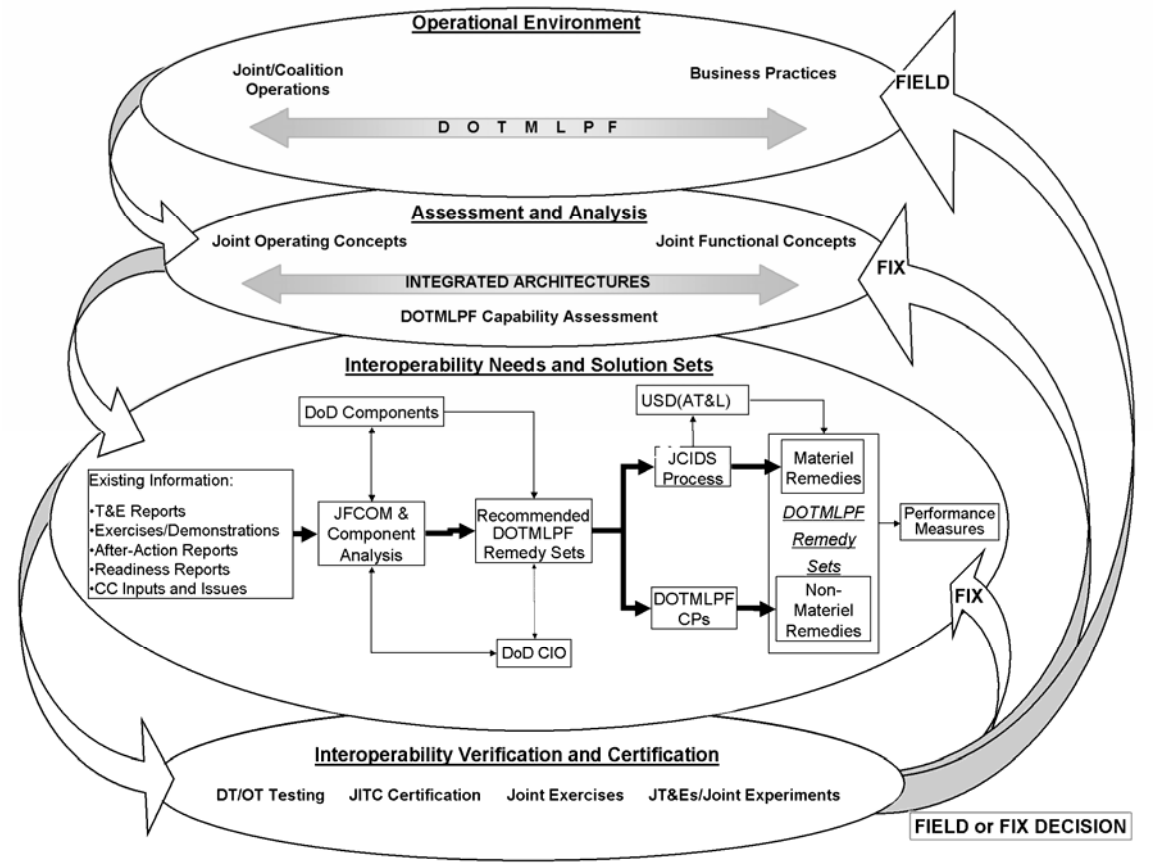
6.3.2.1. ISP. An ISP shall be developed for all non-ACAT acquisitions and procurements to document IT and NSS needs, dependencies, interface requirements, and the NR-KPP. The plan shall describe system dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability requirements. The ISP shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of performance, and interoperability shortfalls. The scope of the ISP shall be scaled to the relative size and funding profile for the program. The sponsoring or cognizant authority shall review, assess, and approve (unless designated Special Interest by the ASD(NII)/DoD CIO) the ISP for non-ACAT acquisitions and procurements, and forward any critical interoperability or supportability issues to the ASD(NII)/DoD CIO for review. The ASD(NII)/DoD CIO shall lead the review for all Special Interest ISPs.

6.3.2.2. Test or Demonstration Plans. A test or demonstration plan shall be developed for all non-ACAT acquisitions and procurements. The test or demonstration plan shall describe how the assessment of IT and NSS interoperability shall be accomplished and identify measurable, performance-based criteria that shall be used to verify overall IT and NSS interoperability and supportability. The scope of test or demonstration plan shall be scaled, as necessary, based on the relative size and funding profile for the program. The sponsoring or cognizant authority shall review, assess, and approve test or demonstration plans.

6.3.3. Interoperability Verification/Certification. All non-ACAT acquisitions and procurements shall be tested and evaluated for required interoperability and supportability according to the approved test plan. IT and NSS interoperability testing shall be scaled, as necessary, based on the relative size and funding profile, criticality, and other risk factors for the program and may be performed in conjunction with other tests, exercises or demonstrations (e.g., Component interoperability testing) to conserve resources. The DISA (JITC) shall conduct an interoperability evaluation, based on DISA (JITC) interoperability testing or other test results, and certify systems and/or interfaces as ready for operational use. The sponsoring or cognizant authority shall review and consider IT and NSS interoperability test results prior to operational use or fielding decision. IT and NSS with significant interoperability deficiencies (as determined by the ISRP) may be placed on the IWL to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

6.4. Fielded IT and NSS Interoperability Process. Figure F4. depicts the capability-focused, effects-based interoperability process for addressing operational warfighting interoperability and supportability issues for fielded IT and NSS.

Figure F4. Fielded (Legacy Systems) IT and NSS Interoperability Process



6.4.1. Fielded IT and NSS Interoperability Process Overview

6.4.1.1. The Unified Command Plan (UCP) (reference (w)) assigns the USJFCOM as the Joint Force Integrator responsible for combining DoD Component capabilities to enhance interoperability and joint, combined, and coalition capabilities by recommending changes in DOTMLPF. The UCP also requires the USJFCOM to support the development and integration of fully interoperable systems and capabilities, including command, control, communications, computers, and intelligence, surveillance, and reconnaissance for joint warfighting.

6.4.1.2. The USJFCOM (JI&I) shall identify interoperability and supportability issues for fielded Joint Task Force IT and NSS by assessing the current operational force against the required capabilities and determining the impact on warfighting readiness. This assessment shall provide the "state of joint force IT and NSS interoperability."

6.4.1.3. The USJFCOM (JI&I), in coordination with the DoD Components, shall define and assume advocacy for the DOTMLPF-synchronized solutions for near-term IT and NSS interoperability and supportability shortfalls. An interoperability transition fund shall address necessary materiel and non-materiel remedy sets. The USJFCOM (JI&I) shall document and track these remedy sets.

6.4.1.4. The USJFCOM (JI&I), in coordination with the USD(AT&L), the USD(C)/CFO, the ASD(NII)/DoD CIO, the DPA&E, the DOT&E, and the other DoD Components, shall forward recommendations to the appropriate forum for programs where potential IT and NSS interoperability and supportability, and infrastructure impacts may occur.

6.4.1.5. The USD(AT&L), the USD(C)/CFO, the USD(I), the ASD(NII)/DoD CIO, the DPA&E, and the DOT&E shall provide policy and oversight for the capability-focused, effects-based interoperability and supportability process; and with the Chairman of the Joint Chiefs of Staff and the Commander, USJFCOM, provide a synchronized capability for addressing fielded IT and NSS interoperability and supportability issues of: joint, combined, and coalition forces; and, where required, other U.S. Government Departments and Agencies.

6.4.2. Fielded IT and NSS Interoperability Shortfalls and DOTMLPF Remedies

6.4.2.1. The USJFCOM (JI&I) shall leverage existing ASD(NII)/DoD CIO, Chairman of the Joint Chiefs of Staff, and DoD Component repositories to produce a consolidated priority list of interoperability and supportability shortfalls. The USJFCOM, in conjunction with the DoD Components, shall provide this list to the JROC for endorsement. The JROC process shall be the central decision forum for interoperability shortfall validation and DOTMLPF remedy set implementation,

providing strategic guidance and direction regarding the materiel or non-materiel solution(s) within the proposal. The JROC shall recommend a DoD Component lead for remedy-set implementation, as appropriate. The JROC may request an AoA from the responsible DoD Component and an assessment of the AoA interoperability issues from either the DPA&E or the responsible CAE to examine the range of materiel and non-materiel solutions.

6.4.2.2. The lead DoD Component assigned to implement the non-materiel and/or materiel solution shall obligate funds to support the recommended solution. Once coordinated through the JROC process, the lead DoD Component may draw upon the USJFCOM JI&I transition fund to bridge unfunded program requirements until addressed in the next POM cycle. The DoD Component shall be responsible to POM for the out-years to sustain the recommended solution in the long-term. Transition funds shall not be applied to National Foreign Intelligence Program-funded components unless a formal reprogramming action has been approved by the Secretary of Defense in coordination with the Director Central Intelligence and approved by the Congress.

6.4.3. Interoperability Verification/Certification. All proposed materiel and non-materiel remedies for fielded IT and NSS capabilities shall be verified as meeting interoperability and supportability requirements. IT and NSS interoperability verification may be performed in conjunction with other activities such as Joint Tests and Evaluations, operational tests and exercises, demonstrations or Component interoperability testing to conserve resources. The DISA (JITC) shall conduct an interoperability evaluation, based on DISA (JITC) interoperability testing or other test results, and certify interoperability requirements have been achieved. The cognizant authority for the materiel or non-materiel remedy shall review and consider IT and NSS interoperability test results prior to operational use or a fielding decision. IT and NSS with significant interoperability deficiencies (as determined by the ISRP) may be placed on the IWL to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

6.5. IT and NSS Standards Development and Prescription

6.5.1. As the DoD Executive Agent, the DISA shall coordinate and integrate all DoD IT and NSS standards activities. The DISA shall propose, coordinate among the DoD Components, and post on the DISR, IT and NSS standards that apply throughout the Department of Defense.

6.5.2. The DISR improves interoperability and supportability by identifying IT and NSS standards that facilitate exchange of IT services among systems, units or forces, to operate effectively together. The DISA shall develop a process to continuously evaluate the standards contained in the DISR, and adopt the IT and NSS standards best suited for achieving interoperability across the DoD enterprise.

6.5.2.1. DISR standards are mandated for all emerging or new IT and NSS and for changes to fielded capabilities that produce, use, or exchange information in any form electronically.

6.5.2.2. The DoD Components' use of DISR-mandated standards must consider impacts to cost, schedule, performance, and information security. If the use of a DISR-mandated standard will negatively impact cost, schedule, performance, or information security, a DoD CAE, Component CIO, or cognizant official, as appropriate, may grant a waiver from use.

6.5.2.2.1. For mission-critical or mission-essential ACAT-designated programs, all granted waivers shall be submitted through the ASD(NII)/DoD CIO to the USD(AT&L) for review and concurrence.

6.5.2.2.2. Waivers for non-ACAT acquisitions and procurement shall be submitted to the ASD(NII)/DoD CIO for review and concurrence.

6.5.2.2.3. To ensure proper and timely consideration, all requests for a waiver shall state the cost, schedule, and performance impacts that shall occur if the waiver is not granted, and any resulting operational limitations.

6.5.2.2.4. Concurrence may be assumed if no response to the waiver request is received within 2 weeks of submission to the ASD(NII)/DoD CIO.

6.5.2.3. The DISA shall assess whether systems conform to DISR standards.

6.5.2.4. Each DoD Component CIO is responsible for DISR implementation, including compliance, planning, programming, and budgeting.

6.5.3. The DISA shall review and assess all JCIDS and DoD Component documentation, test plans, and ISPs involving IT and NSS, for standards conformance, incorporating inputs from the other DoD Components. These assessments shall be forwarded to the cognizant DoD CAE who shall address all highlighted issues. The DISA shall also forward outstanding issues to the Chairman of the Joint Chiefs of Staff for resolution and/or make recommendations to the appropriate body (e.g., DAB, ASD(NII)/DoD CIO Executive Board, MCEB, or MIB) during the program decision process. The following shall be considered during this assessment:

6.5.3.1. Standards implementation for IT and NSS interoperability with current or planned systems of the other DoD Components, or between one or more of the: DoD Components and joint, combined, and coalition forces; and where required, other U.S. Government Departments and Agencies.

6.5.3.2. Standards implementation for Communications Security, especially in cases of combined interoperability, shall be carefully considered.

6.5.3.3. Adherence to U.S. Federal and DoD standards, U.S.-ratified NATO STANAGs, and other international standards accepted for U.S. use.

7. INFORMATION REQUIREMENTS

IT and NSS interoperability assessments; conformance assessment certifications and reports; submissions for revisions to existing standards or development of new interoperability and supportability standards; the Executive Summary required by subparagraph 5.11.4., DoD Component ISPs required by subparagraph 6.2.2.5., and the periodic updates to the DoD IWL are exempt from licensing according to paragraph C4.4.2. of DoD 8910.1-M (reference (x)).

8. EFFECTIVE DATE

This Instruction is effective immediately.

Linton Wells II
Acting Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures - 4

E1. References, continued
E2. Definitions
E3. Guidance for IT and NSS
E4. Information Support Plan (ISP)

E1. ENCLOSURE 1

REFERENCES, continued

(e) "DoD Architecture Framework, Version 1.0," February 9, 2004[1]
(f) Sections 2223 and 2224 of title 10, United States Code, as amended
(g) DoD Instruction 4120.24, "Defense Standardization Program (DSP)," June 18, 1998
(h) DoD 4120.24-M, "Defense Standardization Program (DSP) Policies and Procedures," March 9, 2000
(i) Section 133 of title 10, United States Code
(j) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
(k) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003
(l) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," June 2003[2]
(m) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(n) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(o) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
(p) DCI Directive 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999
(q) Office of the Intelligence Community (IC) Chief Information Officer (CIO), "Top Secret/Sensitive Compartmented Information and Below Interoperability (TSABI) Policy," v4.20, November 24, 2003[3]
(r) DoD Directive 5100.35, "Military Communications-Electronics Board (MCEB)," March 10, 1998
(s) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," February 18, 1997

[1] Available at: http://www.defenselink.mil/nii/doc/
[2] Available at: http://www.nstissc.gov/Assets/pdf/NSTISSP_11_revised_fst.pdf
[3] Available on JWICS at: http://www.iccio.ic.gov/docs/side_menu/security/tsabi/

(t) Management Initiative Decision 912, "Joint Battle Management Command and Control," January 7, 2003[4]
(u) DoD Directive 4650.1, "Management and Use of the Radio Frequency Spectrum," June 24, 1987
(v) "Net-Centric Operations and Warfare Reference Model," July 2, 2003[5]
(w) "Unified Command Plan 2002," April 30, 2002[6]
(x) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
(y) USD(AT&L)/ASD(C3I) Memorandum, "Clinger-Cohen Act Compliance Policy," March 8, 2002
(z) USD(AT&L)/ASD(C3I) Memorandum, "Clinger-Cohen Act Compliance Policy for Major Automated Information Systems," June 19, 2002
(aa) Deputy Chief Information Officer Memorandum, "Department of Defense Information Technology (IT) Registry Interim Guidance," March 17, 2003
(ab) "Global Information Grid Capstone Requirements Document," August 30, 2001[7]
(ac) DoD CIO Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003
(ad) ASD(C3I) Memorandum, "Approval of Commercial Off-The-Shelf Information Technology/National Security Systems Software Action Plan," April 8, 2003
(ae) DoD "Interim Defense Acquisition Guidebook," October 30, 2002[8]

---

[4] Release limited: Forward request to Under Secretary of Defense (Comptroller)/Chief Financial Officer, 1100 Defense Pentagon, Washington, DC 20301-1100
[5] Available at: https://disain.disa.mil/ncow.html
[6] Available on SIPRNET
at: http://www.js.smil.mil/masterfile/sjsimd/jel/cdata/class/others/mcm_0016_03.pdf
[7] Available at: https://jdl.jwfc.jfcom.mil
[8] Available at: http://dod5000.dau.mil/InterimGuidebook.doc

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Acquisition Category (ACAT). Categories established to facilitate decentralized decision-making and execution, and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. Reference (d) provides the specific definition for each acquisition category (ACAT I through III).

E2.1.2. Advanced Concept Technology Demonstration (ACTD). The primary goal of an ACTD is to assess the military utility of a significant new capability and to conduct the assessment at a scale size adequate to clearly establish operational utility and system integrity.

E2.1.3. Approval. To give formal or official sanction. The formal or official sanction of the identified capability described in the capability documentation.

E2.1.4. Architectures. The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

E2.1.5. Assessment (Assess). The act or result of determining the contribution or disposition of an activity, product, or condition, based on an appraisal of the state of IT and NSS interoperability.

E2.1.6. Capability. The ability to execute a specified course of action defined by an operational user and expressed in broad operational terms. It includes the DOTMLPF required to achieve a specified course of action. It is documented in an ICD or a DOTMLPF change recommendation. In the case of materiel proposals, the definition progressively evolves to DOTMLPF performance attributes specified in the CDD and the CPD.

E2.1.7. Capability Development Document (CDD). A JCIDS document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable, and technically mature capability.

E2.1.8. Capability-Focused, Effects-Based Interoperability. An interoperability process that:

E2.1.8.1. Includes experts from the operational community to identify, consolidate, and prioritize interoperability needs; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities.

E2.1.8.2. Characterizes IT and NSS interoperability needs in a capability-focused context using integrated architectures derived from JOCs and JFCs.

E2.1.8.3. Assesses net-readiness; information assurance requirements; and both the technical exchange of information and the end-to-end operational effectiveness of that exchange using the NR-KPP.

E2.1.8.4. Incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organization, training, leadership and education, personnel, or facilities) solutions.

E2.1.8.5. Verifies interoperability solutions in formal tests or operational exercises.

E2.1.8.6. Continuously verifies the NR-KPP and evaluates overall IT and NSS interoperability, within a given capability, throughout a system's life.

E2.1.9. Capability Gaps. Those synergistic resources (DOTMLPF) unavailable, but potentially attainable to the operational user for effective task execution.

E2.1.10. Capability Production Document (CPD). A JCIDS document that addresses the production elements specific to a single increment of an acquisition program.

E2.1.11. Certification (Certify). A formal statement of adequacy provided by a responsible Agency attesting that a system has met its interoperability and supportability needs.

E2.1.12. Common Operating Environment (COE). Integrated software infrastructure that facilitates the migration and implementation of functional mission applications and integrated databases across information systems. The COE provides architecture principles, guidelines, and methodologies that assist in the development of mission application software by capitalizing on a thorough, cohesive set of infrastructure support services.

E2.1.13. Conformance Testing. Testing the extent to which a system or subsystem adheres to or implements a standard.

E2.1.14. Decision Superiority. The state at which better decisions are arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.

E2.1.15. Defense Agencies. All agencies and offices of the Department of Defense, including the Missile Defense Agency, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and

Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Geospatial Intelligence Agency, National Reconnaissance Office, and National Security Agency/Central Security Service.

E2.1.16. DoD Information Technology Standards Registry (DISR). The DISR provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It defines the service areas, interfaces, standards (DISR elements), and standards profiles applicable to all DoD systems. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense. The DISR replaced the Joint Technical Architecture.

E2.1.17. DoD Component. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, DoD Field Activities, and all other organizational entities in the Department of Defense.

E2.1.18. DoD 5000 Series. Refers collectively to references (j) and (k).

E2.1.19. Electromagnetic Environmental Effects. The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility/electromagnetic interference; electromagnetic vulnerability, electromagnetic pulse; electromagnetic protection; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and p-static.

E2.1.20. Evaluation (Evaluate). Measuring or quantifying the value, characteristics, or capabilities of something against established standards, (as in "Test and Evaluation"). The determination of, or act of determining the relative degree to which IT and NSS interoperability is achieved.

E2.1.21. Global Information Grid (GIG)

E2.1.21.1. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes NSS as defined in section 11103 of title 40 of the United States Code (reference (d)). The GIG supports all Department of Defense, National Security, and

related IC missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

E2.1.21.2. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.21.2.1. Transmits information to, receiving information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.21.2.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.21.2.3. Processes data or information for use by other equipment, software, or services.

E2.1.21.3. Non-GIG IT. Stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

E2.1.22. Global Information Grid (GIG) Key Interface Profiles (KIPs). GIG KIPs provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. The KIP is the set of documentation produced as a result of interface analysis which designates an interface as key; analyzes it to understand its architectural, interoperability, test and CM characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. GIG KIPs provide a description of required operational functionality, systems functionality and technical specifications for the interface. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Engineering Management Plan, CM Plan, TV-1 with SV-TV Bridge, and procedures for standards conformance and interoperability testing. An interface is designated as a key interface when one or more the following criteria are met:

E2.1.22.1. The interface spans organizational boundaries.

E2.1.22.2. The interface is mission critical.

E2.1.22.3. The interface is difficult or complex to manage.

E2.1.22.4. There are capability, interoperability, or efficiency issues associated with the interface.

E2.1.22.5. The interface impacts multiple acquisition programs.

E2.1.22.6. The interface is vulnerable or important from a security perspective.

E2.1.23. Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.24. Information Needs. A condition or situation requiring knowledge or intelligence derived from received, stored, or processed facts and data.

E2.1.25. Information Support Plan (ISP). The identification and documentation of information needs, infrastructure support, IT and NSS interface requirements and dependencies focusing on net-centric, interoperability, supportability and sufficiency concerns.

E2.1.26. 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), related resources and NSS. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E2.1.27. Information Technology Architecture. An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the Agency's strategic goals and information resources management goals.

E2.1.28. Information Timeliness. Occurring at a suitable or appropriate time for a particular condition or situation.

E2.1.29. Initial Capabilities Document (ICD). Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects, and time. The ICD summarizes the results of the DOTMLPF analysis and describes why non-materiel changes alone have been judged inadequate in fully providing the capability.

E2.1.30. Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, systems view, and technical standards view) facilitating

integration and promoting interoperability across capabilities and among related integrated architectures.

E2.1.30.1. The operational view is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions.

E2.1.30.2. The systems view is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions.

E2.1.30.3. The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

E2.1.31. Interim Certificate To Operate (ICTO). An ICTO provides interim authority to deploy or operate IT and NSS when interoperability certification has not been completed and there is an urgent operational requirement to field a given system or capability.

E2.1.32. 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. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with information assurance.

E2.1.33. Interoperability and Supportability Needs. A condition, situation, or capability in which interoperability and supportability deficiencies have been identified, based on an approved or established rule set, test, or measure of value for judging interoperability and supportability sufficiency of IT and NSS.

E2.1.34. Joint Capabilities Integration and Development System (JCIDS). A Chairman of the Joint Chiefs of Staff process identifying, assessing and prioritizing joint military capability needs. The JCIDS process is a collaborative effort that uses joint concepts and integrated architectures to identify prioritized capability gaps and integrated DOTMLPF solutions (materiel and non-materiel) to resolve those gaps.

E2.1.35. Joint Functional Concept (JFC). An articulation of how a future Joint Force Commander shall integrate a set of related military tasks to attain capabilities required across the range of military operations. Although broadly described within the Joint Operations Concepts, JFCs derive specific context from the joint operating concepts and promote common attributes in sufficient detail to conduct experimentation and measure effectiveness.

E2.1.36. Joint Operating Concept (JOC). An articulation of how a future Joint Force Commander shall plan, prepare, deploy, employ, and sustain a joint force against potential adversaries' capabilities or crisis situations specified within the range of military operations. JOCs guide the development and integration of JFCs to provide joint capabilities. JOCs articulate the measurable detail needed to conduct experimentation and allow decision makers to compare alternatives.

E2.1.37. Joint Operations Concepts. A concept that describes how the Joint Force intends to operate 15 to 20 years from now. It provides the operational context for the transformation of the Armed Forces of the United States by linking strategic guidance with the integrated application of Joint Force capabilities.

E2.1.38. Key Performance Parameters (KPPs). Those minimum attributes or characteristics considered most essential for an effective military capability. KPPs are validated by the Chairman of the Joint Chiefs of Staff.

E2.1.39. Materiel Solution. Correction of a deficiency, satisfaction of a capability gap, or incorporation of new technology that results in the development, acquisition, procurement or fielding of a new item (including ships, tanks, self-propelled weapons, aircraft, etc., and related software, spares, repair parts and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without disruption as to its application for administrative or combat purposes.

E2.1.40. Milestones. Major decision points that separate the phases of an acquisition program.

E2.1.41. Milestone Decision Authority (MDA). The individual designated according to criteria established by the USD(AT&L) or by the ASD(NII)/DoD CIO for IT and NSS acquisition programs to approve entry of an acquisition program into the next phase.

E2.1.42. Military Department. Departments of the Army, the Navy, and the Air Force.

E2.1.43. Mission Critical Information System (MCIS). A system meeting the definitions of "information system" and "national security system" in reference (d) that the loss of which would cause the warfighter operations or direct mission support of warfighter operations to cease. The designation of mission critical should be made by the Head of a DoD Component, a Combatant Commander or one of their designees. MCIS is defined the same as a Mission Critical IT System.

E2.1.44. Mission Essential Information System. A system that meets the definition of "information system" in reference (d), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission.

The designation of mission essential should be made by a Head of a DoD Component or a Combatant Commander or their designee.

E2.1.45. Mission Need. A deficiency in current capabilities or an opportunity to provide new capabilities (or enhance fielded capabilities) through the use of new technologies. Mission needs are expressed in broad operational terms by the DoD Components.

E2.1.46. National Security System (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which:

E2.1.46.1. Involves intelligence activities.

E2.1.46.2. Involves cryptologic activities related to national security.

E2.1.46.3. Involves command and control of military forces.

E2.1.46.4. Involves equipment that is an integral part of a weapon or weapons system.

E2.1.46.5. 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).

E2.1.47. Net-Centric. Information-based operations that use service-oriented information processing, networks, and data from the following perspectives: user functionality (capability to adaptively perform assigned operational roles with increasing use of system-provided intelligence/cognitive processes), interoperability (shared information and loosely coupled services), and enterprise management (net operations).

E2.1.48. Net-Centric Enterprise Services (NCES). An acquisition program that identifies, develops, and implements GIG CES. GIG CES include application, discovery, user assistant, collaboration, storage, mediation, messaging, enterprise service management, and information assurance/security.

E2.1.49. Net-Centric Operations and Warfare (NCOW) Reference Model (RM). The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, COI services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the GIG are realized.

E2.1.50. Net-Ready. The continuous ability to interface and interoperate achieving operationally secure exchanges of information in conformance with enterprise constraints. The NR-KPP assesses the net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

E2.1.51. Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements:

E2.1.51.1. Compliance with the NCOW RM.

E2.1.51.2. Compliance with applicable GIG KIPs.

E2.1.51.3. Verification of compliance with DoD information assurance requirements.

E2.1.51.4. Supporting integrated architecture products required to assess information exchange and use for a given capability.

E2.1.52. Non-Materiel Solution. Changes in doctrine, organization, training, leadership and education, personnel or facilities that satisfy identified capability gaps.

E2.1.53. Oversight. Senior executive-level review of programs to ensure compliance with policy and attainment of broad program goals.

E2.1.54. Signals Intelligence (SIGINT). A category of intelligence comprising, either individually or in combination, all Communications Intelligence, Electronics Intelligence, and Foreign Instrumentation Signals Intelligence.

E2.1.55. Spectrum Supportability. The authority to use the electromagnetic spectrum necessary for supporting the operation of a spectrum-dependent equipment or system during its expected life cycle. The equipment or system must be authorized to use spectrum that is, or shall be, available from system development, through developmental and operational testing, to actual operation in the electromagnetic environment. The assessment of an equipment or system having "spectrum supportability" requires, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of the electromagnetic compatibility.

E2.1.56. Standards Compliance. Confirmation that IT and NSS has undergone standards testing and exhibits a specified degree of standards conformity.

E2.1.57. Standards Conformance Certification. Confirmation by the DISA that an IT and NSS has undergone IT standards testing and exhibits IT standards-based implementation. IT standards include standards for information processing, information content (such as standard data definitions), information formats, and information transfer.

E2.1.58. Supportability. The ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capability(ies).

E2.1.59. System Standards Profile. A system-specific list of all technical standards and guidelines for their use. To meet IT and NSS interoperability needs, the system standards profile should be built from applicable standards drawn from the DISR.

E2.1.60. Tactical SIGINT System. All SIGINT systems developed for use by U.S. Forces.

E2.1.61. Test and Evaluation. The act of generating data during the research and development of emerging systems and the creation of information through analysis that is useful to technical personnel and decision-makers for reducing design and acquisition risks. The process that gauges progress by measuring systems against requirements and specifications and analyzing the results.

E2.1.62. Universal Reference Resources (URRs). Reference models and information standards, which serve as sources for guidelines and attributes that must be consulted in building integrated architecture products. The following are the currently listed URRs: DoD Architecture Framework; DoD Core Architecture Data Model; Universal Joint Task List; Technical Reference Model; GIG Architecture; DoD Net-Centric Data Strategy; DoD Metadata Registry; NCOW RM; and the DISR.

E2.1.63. Validation. An authoritative act or process of supporting or corroborating whether IT and NSS interoperability and supportability needs are appropriate.

E2.1.64. Verification. The act of establishing whether IT and NSS interoperability needs are accurate, measurable, supportable, and adequately reflected for a given capability, acquisition strategy, test and evaluation plan, or in non-materiel or non-traditional acquisition IT and NSS ISPs.

E3. ENCLOSURE 3

GUIDANCE FOR IT AND NSS

E3.1.1. IT and NSS, of the DoD GIG, shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare.

E3.1.2. IT and NSS interoperability and supportability needs shall be derived using JOCs, JFCs, and associated integrated architectures and shall be updated as necessary throughout the system's life. For IT and NSS supporting DoD business areas and domains, the GIG Architecture shall be used to determine interoperability and capability needs. IT and NSS interoperability and supportability needs, for a given capability, shall be identified through:

E3.1.2.1. The Defense Acquisition System (as defined in the DoD 5000 series issuances (references (j) and (k))).

E3.1.2.2. The JCIDS process.

E3.1.2.3. The DOTMLPF change recommendation process.

E3.1.3. A capability-focused, effects-based interoperability process (see paragraph E2.1.8.) for improving IT and NSS interoperability and supportability shall incorporate both materiel (acquisition or procurement) and non-materiel (doctrine, organization, training, leadership and education, personnel, and facilities) solution sets. The operational community shall identify, prioritize, and synchronize non-materiel solutions with materiel solutions to resolve interoperability and supportability issues. Once IT and NSS interoperability solution sets are validated, appropriate resources shall be recommended to implement identified remedies.

E3.1.4. IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS.

E3.1.5. A NR-KPP, consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, IA, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. A NR-KPP shall be defined for all IT and NSS defense acquisition and procurement programs and shall be specified to a level of

detail that allows verification of interoperability throughout a system's life. The defined NR-KPP shall be developed so that it can be reliably measured, tested and evaluated.

E3.1.6. IT and NSS interoperability and supportability needs shall be managed, evaluated, and reported over the life of the system using an ISP (see enclosure 4). For all DoD ACAT programs and non-ACAT acquisitions and procurements, a ISP shall be produced and used to analyze interoperability and supportability requirements specified in the NR-KPP. The ISP shall contain detailed and time-phased information for identifying dependencies and interface requirements consistent with relevant integrated architectures, focusing attention on interoperability, supportability, sufficiency, and security concerns. For IT and NSS defense acquisition programs and procurements, system dependencies and interface requirements shall be described in sufficient detail to assist in acquisition and procurement decisions, and to provide test planners the information necessary to ensure that the system test program is sufficient to permit an accurate evaluation of the system's NR-KPP.

E3.1.7. Interoperability and supportability needs shall be balanced with requirements for IA.

E4. ENCLOSURE 4

INFORMATION SUPPORT PLAN (ISP) RESPONSIBILITIES, PROCESS, AND FORMAT

E4.1. INTRODUCTION

E4.1.1. This enclosure provides the responsibilities, process, and format for the ISP, required by references (b), (k), and this Instruction.

E4.1.2. The ISP provides a means to identify and resolve implementation issues related to an acquisition program's IT and NSS information infrastructure support and information interface requirements. It identifies IT and information (including intelligence) needs, dependencies, and interfaces for programs in all acquisition and non-acquisition categories, focusing on net-readiness, interoperability, information supportability, and information sufficiency concerns.

E4.1.3. The ISP process is one of discovery requiring an analysis of the program's integrated architecture. The analysis identifies interoperability and supportability issues and assesses compliance with DoD information policy and goals. The ISP addresses fundamental questions for each piece of information needed to support the operational and/or functional capability(ies):

E4.1.3.1. What information is needed by the program to successfully execute the capability(ies)?

E4.1.3.2. How accurate must the information be?

E4.1.3.3. What quantity of information is needed (or in the case of information sources, what should be provided)?

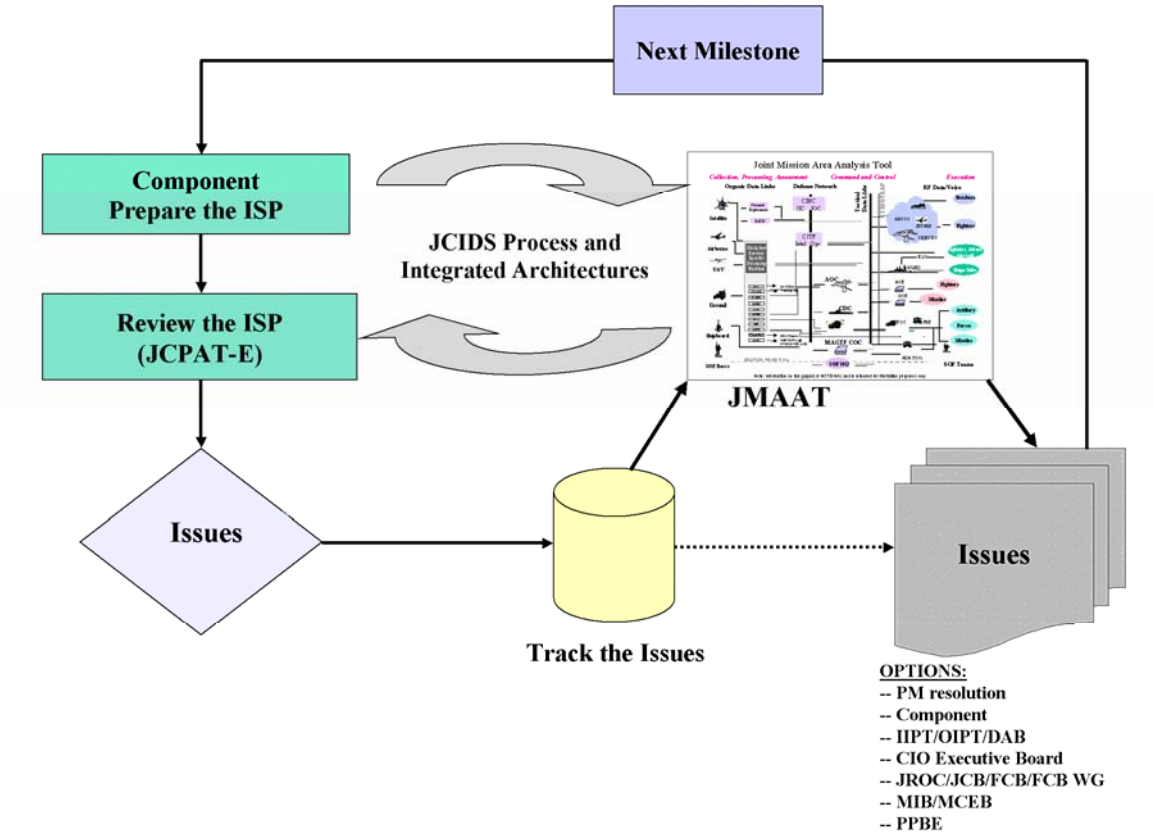
E4.1.3.4. How shall the information be obtained (or access provided)?

E4.1.3.5. How quickly must the information be received to be useful?

E4.1.3.6. Does the program implementation comply with net-centric concepts?

E4.1.3.7. Does the program or capability comply with DoD IT and NSS policies?

Figure E4.F1. Basic ISP Process



E4.1.4. The ISP replaces the Command, Control, Communications, Computer, and Intelligence Support Plan (C4ISP) originally in the DoD 5000 series documents (references (j) and (k)). Programs with existing C4ISPs shall update the plan to the new ISP format and content not later than the next acquisition milestone. Additionally, if a JCIDS document has been generated for the program, the new ISP format and content must be used.

E4.1.5. The following are required (either completed or underway) to generate an ISP: an integrated architecture; relevant JCIDS documentation (ICD, CDD, or CPD); a JOC, a JFC, and an AoA.

E4.1.6. The Basic ISP Process

E4.1.6.1. Prepare the plan. The DoD Component prepares the plan using the JCIDS documentation, integrated architectures, and other sources.

E4.1.6.2. Review the plan. The plan is submitted for formal review coordinated by the ASD(NII)/DoD CIO using the JCPAT-E.

E4.1.6.3. Track the issues from the plan. Issues from the plan and from formal DoD-level reviews are posted in the ASD(NII)/DoD CIO issue database and the Joint Mission Area Analysis Tool (JMAAT).

E4.1.6.4. Resolve the issues from the plan. Issues are disseminated to various forums for possible resolution.

E4.1.6.5. Repeat the process. The final plan is placed in the JCPAT-E document repository and the process is repeated at each major milestone.

E4.2. DEFINITIONS

E4.2.1. Capability. The ability to execute a specified course of action. A capability is defined by an operational user and expressed in broad operational terms. A capability includes the DOTMLPF required to achieve a specified course of action. It is documented in an ICD or a DOTMLPF change recommendation.

E4.2.2. Derived Information Support Requirements. Information, or information tasks (produced, consumed, or transferred), derived from analysis of applicable JOCs, JFCs, and JCIDS documentation, and the associated integrated architecture(s).

E4.2.3. Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

E4.2.4. Information Needs. A condition or situation requiring knowledge or intelligence derived from received, stored, or processed facts and data.

E4.2.5. Information Timeliness. Occurring at a suitable or appropriate time for a particular condition or situation.

E4.2.6. 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. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle and it must be balanced with information assurance.

E4.2.7. ISP Issue Categories:

E4.2.7.1. Critical Issue. An information-related issue that would prevent the program's ability to provide a required operational/functional capability. A critical issue shall frequently relate to another supporting program (e.g., information required from another program), program synchronization, lack of resources, technology gaps, or other factors. A deviation from ISP preparation guidance may not by itself constitute a critical issue. Missing integrated architectural product content may constitute a critical issue.

E4.2.7.2. Substantive Issue. An issue that would significantly impact the program's ability to provide a required operational and/or functional capability. A deviation from ISP preparation guidance may not by itself constitute a substantive issue. Missing integrated architectural product content may constitute a substantive issue.

E4.2.7.3. Administrative Issue. An issue that would misrepresent the facts or detract from the ISP as a document. Format issues are at most administrative.

E4.2.8. Net-Centric. Information-based operations that use service-oriented information processing, networks, and data from the following perspectives: user functionality (capability to adaptively perform assigned operational roles with increasing use of system-provided intelligence/cognitive processes), interoperability (shared information and loosely coupled services), and enterprise management (net operations).

E4.2.9. Net-Ready. The continuous ability to interface and interoperate to achieve operationally secure exchanges of information in conformance with enterprise constraints. The NR-KPP assesses the net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

E4.2.10. Sufficiency. The extent to which information support requirements are satisfied and the necessary supporting infrastructure is available.

E4.2.11. Supportability. The ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capability(ies).

E4.2.12. Synchronization. The extent to which programs (capabilities) are aligned in time.

E4.2.13. Threads. The sequence of operational activities and their performance parameters that together achieve a desired capability. A critical thread's execution is essential to successful achievement of a required capability.

E4.3. RESPONSIBILITIES ASSIGNED IN ACCORDANCE WITH THIS ENCLOSURE

E4.3.1. The ASD(NII)/DoD CIO shall:

E4.3.1.1. Serve as the primary staff activity for the ISP.

E4.3.1.2. Establish policy, process, and provide oversight for conduct of DoD-level ISP reviews.

E4.3.1.3. Review all ISPs for ACAT I, ACAT IAM, and programs designated "Special Interest" by the ASD(NII)/DoD CIO. Verify IT and NSS information support needs, and identified issues from these reviews. For unresolved issues, notify the cognizant acquisition activity (DAB), Defense Space Acquisition Board (DSAB), IPTs, or Information Technology Acquisition Board (ITAB); the JROC, the JCIDS Joint Capabilities Board, the appropriate FCB, the MCEB or the MIB; or to the PPBE process, as appropriate.

E4.3.1.4. Maintain an ISP "Special Interest" List.

E4.3.1.5. Review and coordinate on all ISP waiver requests prior to MDA waiver approval for a specified program in all ACATs.

E4.3.1.6. Participate in Integrating Integrated Product Teams and OIPTs for ACAT I, IAM, and Special Interest programs completing ISPs.

E4.3.1.7. Maintain a database of all critical IT and NSS interoperability and information (including intelligence) issues generated by the ISP process.

E4.3.1.8. Serve as the Point of Contact (PoC) for DoD-level reviews of ISPs.

E4.3.2. Other Principal Staff Assistants (PSAs) shall:

E4.3.2.1. Participate in DoD-level ISP reviews, as appropriate.

E4.3.2.2. Coordinate resolution of issues, as necessary, with other DoD Components.

E4.3.3. The Heads of the DoD Components shall:

E4.3.3.1. Designate a principal PoC to represent the DoD Component on ISP policy and process matters and provide to the ASD(NII)/DoD CIO.

E4.3.3.2. Establish an internal ISP management process that supports preparation and review of ISPs, and provide to the ASD(NII)/DoD CIO. This process shall lead to ISP approval by a designated DoD Component official. This process shall include coordination with all affected DoD Components. Critical and substantive issues raised during ISP reviews shall be addressed to include issue mitigation strategies prior to DoD Component approval.

E4.3.3.3. Ensure ISPs for ACAT I, IAM, and ISP Special Interest programs, are provided to the ASD(NII)/DoD CIO for DoD-level review with the associated ICD, CDD and/or CPD. The DoD Component shall develop an ISP that identifies the IT and NSS required capabilities or information to meet the proposed capability within the context of the relevant integrated architecture. An approved ISP is required not later than Milestone B (program initiation for ships) and should be initially developed concurrently and collaboratively with the associated CDD or CPD, unless exceptions are noted in an Acquisition Decision Memorandum. As the program matures, or proceeds through multiple evolutionary blocks or phases, the DoD Component shall update the ISP. Updates shall contain progressively more detailed and specific time-phased descriptions of the types of information needed; integrated architectures; spectrum supportability, security, connectivity, and interoperability issues; and infrastructure, intelligence, information assurance, net-readiness, and other information support needs. Changes in information support, infrastructure, interface requirements that result from proposed changes in approved JCIDS documents shall be highlighted to facilitate the ISP review.

E4.3.3.4. Ensure copies of ISPs for all ACAT and non-ACAT programs are submitted (posted) to the ASD(NII)/DoD CIO ISP repository located on the JCPAT-E website, managed by the DISA. A user's guide is available with instructions on the JCPAT-E website. The JCPAT-E website can be found at the following web addresses: SIPRNET URL: http://jcpat.ncr.disa.smil.mil or on the NIPRNET at URL: https://jcpat.ncr.disa.mil.

E4.3.3.5. Ensure that Satellite Communications (SATCOM) related information issues are posted in the Emerging Requirements Database.

E4.3.4. The Chairman of the Joint Chiefs of Staff shall:

E4.3.4.1. Participate in the ASD(NII)/DoD CIO-led DoD-level ISP reviews and provide comments representing Combatant Commander interests. Post review comments on the NIPRNET JCPAT-E website unless the comments are classified.

E4.3.4.2. Provide supportability, interoperability, and intelligence certifications to the ASD(NII)/DoD CIO.

E4.3.4.3. Ensure FCBs supporting the JCIDS process consider the impact of information support issues referred by the ASD(NII)/DoD CIO.

E4.3.5. The DISA shall:

E4.3.5.1. Maintain the ISP repository contained in JCPAT-E for the ASD(NII)/DoD CIO.

E4.3.5.2. Distribute ISPs on JCPAT-E for review by the DoD Components, track ISP reviewer comments, and provide the consolidated results of the reviews to the ASD(NII)/DoD CIO.

E4.3.5.3. Review ISPs for all ACAT I, ACAT IAM, and programs designated as Special Interest by the ASD(NII)/DoD CIO.

E4.3.6. DoD-Level OIPT and Integrating Integrated Product Teams shall:

E4.3.6.1. Review critical issues and forward those deemed appropriate to the DAB, DSAB, or ITAB, as appropriate, for consideration in an acquisition decision.

E4.3.6.2. Recommend, as appropriate, to the ASD(NII)/DoD CIO that an issue, identified in an ISP, be forwarded to other activities for resolution.

E4.3.7. The DSAB shall:

E4.3.7.1. Maintain separate process and procedures for review of space related ISPs. The ASD(NII)/DoD CIO shall participate as necessary in this process. The space policy shall delineate the review process for space programs; however, during the Independent Program Assessment a DoD-level review shall be conducted by the ASD(NII)/DoD CIO.

E4.3.7.2. Post the ISPs portions of the Integrated Program Summary on the JCPAT-E repository when a DoD-level review is conducted, and when the ISP is completed.

E4.3.8. The DoD Component and Designated ISP Reviewers shall:

E4.3.8.1. Ensure appropriate Subject Matter Experts (SMEs) review ISPs during the DoD-level review. Ensure comments are submitted in the format provided on the JCPAT-E.

E4.3.8.2. Identify IT and information (including intelligence) support needs that are incorrect, incomplete, or missing from the ISP. Issues shall be categorized using the terms critical, substantive, and administrative to prioritize each review comment.

E4.3.8.3. Post review comments on the NIPRNET JCPAT-E website unless the comments are classified.

E4.4. PROCESS AND PROCEDURES

E4.4.1. Preparation. The DoD Components shall prepare ISPs using the JCIDS documentation, related integrated architectures, SMEs, and other sources, as required. Supporting or supported systems or programs requiring direct interface should also be consulted as sources when developing the ISP.

E4.4.1.1. Ideally, a Working-level Integrated Product Team (WIPT) should develop the ISP. The WIPT should be comprised of SMEs familiar with the system being acquired; the intended use of the system; and, to the extent possible, the integrated architecture within which the system shall operate. As the integrated architecture matures, the WIPT should invite other Program Managers (PMs) of systems for which the system being acquired shall interface and other PMs of systems that must provide support to the system (supporting and supported systems). Assessing the overall interoperability and supportability for interfacing systems, to satisfy the program's operational and derived requirements (analysis section of the ISP), shall require continuing collaboration among SMEs of all systems involved.

E4.4.1.2. The DoD Components shall allow sufficient time to prepare and update the ISP to ensure completion of the DoD-level ISP reviews prior to an upcoming milestone or decision review. Preparation shall include careful consideration of the information, infrastructure, and interface support requirements levied by and on the program, and a thorough (and iterative) document review process. PMs of interfacing programs, identified in the ISP, should review the document during this process for completeness, and validate issues and resolution paths (in the issue section of the ISP). PMs of interfacing programs should also reflect similar information in their respective ISPs.

E4.4.1.3. The DoD Components shall prepare the ISP at the classification level necessary to effectively communicate the required information, without unnecessary reliance on reference documents that may not be generally available to users or reviewers. The DoD Components shall not keep an ISP unclassified to only facilitate document review; however, unclassified ISPs with classified annexes may sometimes be appropriate. The DoD Components shall consider the implications of compiling detailed, sensitive but unclassified information and/or proprietary information in a document that receives wide distribution during review. No competition-sensitive information shall be included in the ISP. ISPs that are competition sensitive shall not be accepted for review.

E4.4.1.4. Before an ISP is distributed for review; the DoD Components shall certify that all SATCOM requirements of the acquisition program have been approved for inclusion in the SATCOM Emerging Requirements Database maintained by the Chairman of the Joint Chiefs of Staff.

E4.4.1.5. The DoD Components shall ensure that spectrum supportability requirements are addressed through:

E4.4.1.5.1. Submission of a DD Form 1494, "Application for Equipment Frequency Allocation," by the acquiring activity.

E4.4.1.5.2. Consideration of supportability comments provided by the Equipment Spectrum Guidance Permanent Working Group under the Frequency Panel of the MCEB.

E4.4.1.5.3. On-going reviews and assessments of relevant JCIDS documents and ISPs within the spectrum management community.

E4.4.1.6. The DoD Component shall ensure compliance with all relevant DoD policy when developing an ISP. Compliance with Service or Agency-specific policy shall be considered separately from the ASD(NII)/DoD CIO review process for ISPs. Relevant DoD policy includes, but is not limited to, the following:

E4.4.1.6.1. Reference (d), USD(AT&L)/Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) Memorandum, dated March 8 and June 19, 2002, (references (y) and (z)) for Subtitle III of title 40, U.S.C. (formerly the Clinger-Cohen Act) compliance policy.

E4.4.1.6.2. Deputy Chief CIO Memorandum, dated March 17, 2003 (reference (aa)) for IT Registry requirements.

E4.4.1.6.3. References (l) through (q) for IA requirements.

E4.4.1.6.4. Reference (e) and GIG Capstone Requirements Document (reference (ab)) for GIG compliance requirements.

E4.4.1.6.5. Reference (g) for integrated architecture compliance requirements.

E4.4.1.6.6. Reference (v) for the NCOW RM.

E4.4.1.6.7. DoD CIO Memorandum, dated May 9, 2003 (reference (ac)), for DoD net-centric data strategy compliance requirements.

E4.4.1.6.8. DoD IT Standards Registry (formerly DoD JTA) for IT standards compliance requirements.[9]

E4.4.1.6.9. ASD(C3I) Memorandum, dated April 8, 2003 (reference (ad)) for approval of COTS IT/NSS software action plan requirements.

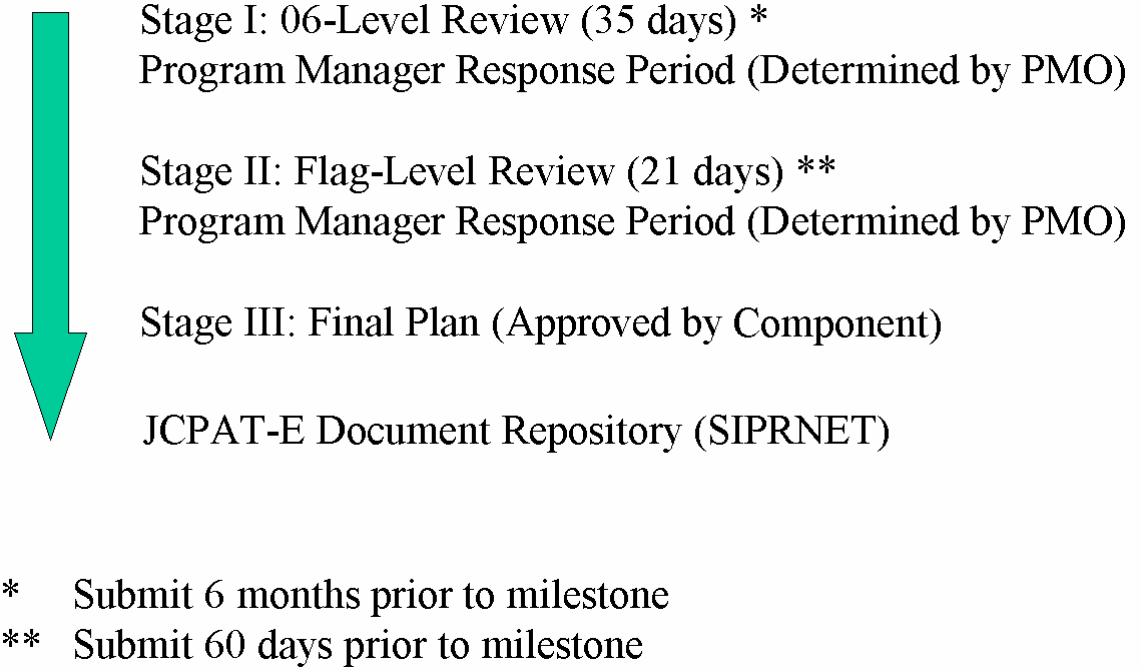
---

[9] Available at: http://disronline.disa.mil/

E4.4.2. Review. The DoD Components shall manage the review of all ISPs within the Component organization, and shall obtain interoperability, supportability and intelligence certifications by the Joint Staff. The ASD(NII)/DoD CIO shall lead a DoD-wide review of: ISPs for all ACAT I (1D and 1C) and IA (IAM, and IAC) acquisition programs; and ISPs for other acquisition programs in which ASD(NII)/DoD CIO has indicated a special interest. Should interoperability issues arise between ACAT I or IA and ACATs II and III programs, the DoD Components shall, if requested, provide an ISP for the affected programs to the ASD(NII)/DoD CIO to support issue resolution. The DSAB has a separate policy for conducting ISP reviews. Space programs under the DSAB shall follow the DSAB ISP policy. Space program ISPs shall be submitted using JCPAT-E for formal review.

E4.4.2.1. Formal ISP reviews are conducted by the ASD(NII)/DoD CIO prior to Milestone B (program initiation for ships) and C, and any subsequent major program change or change in JCIDS documentation. The review is conducted in three stages as shown in Figure E4. F2., below. The ASD(NII)/DoD CIO may grant exceptions to the timeframes for each stage of the review.

Figure E4.F2. Review Stages



E4.4.2.2. All reviews shall be conducted using the JCPAT-E. The JCPAT-E is a suite of online tools and applications used to assist the OSD and the Joint Staff in accepting, staffing, reviewing, and evaluating ISPs. Developed, maintained, and operated by the DISA, the JCPAT-E provides the necessary electronic document distribution,

comment collection and rollup, document storage, and management support necessary to evaluate draft documents.

E4.4.2.3. Reviewers of ISPs shall use the format prescribed in JCPAT-E for submitting comments. Reviewers shall concentrate on ISP content rather than format. It is essential that the reviews identify issues that may prevent a program from meeting its threshold and objective required for a given capability.

E4.4.2.4. DoD Components shall obtain the coordination of other affected DoD Component(s) prior to submitting the ISP for DoD-level review. This coordination shall be reflected in the ISP.

E4.4.2.5. Since JCIDS documentation outlines the operational context and required capabilities to be supported, a DoD-level ISP review shall normally not begin until the corresponding stage of the JCIDS document review has been initiated. In certain situations where time constraints demand, the ASD(NII)/DoD CIO and the Joint Staff may shorten the time of the Stage 1 and the Stage 2 review; however, ISP concurrence or supportability certification shall not be granted until the associated JCIDS documentation has been validated by the Joint Staff. Exceptions to the above are at the discretion of the ASD(NII)/DoD CIO and the Joint Staff, but shall not normally be considered.

E4.4.2.6. The DoD Components shall submit the ISP electronically on the JCPAT-E to the ASD(NII)/DoD CIO for review. The DoD Components shall submit unclassified ISPs on the NIPRNET JCPAT-E website and classified (through SECRET) ISPs on the SIPRNET JCPAT-E website. The ASD(NII)/DoD CIO program lead or the JCPAT-E manager at the DISA shall provide specific instructions, including tailoring recommended document formats, to facilitate the DoD review process. The ASD(NII)/DoD CIO program lead shall provide procedures for submitting ISPs at classification levels higher than SECRET and for Special Access Programs. Information copies of draft and approved ICDs, CDDs, and CPDs shall be submitted with the ISP to facilitate the review process. The information in JCIDS documents (e.g., integrated architecture products), required to complete the ISP, should not be duplicated in the ISP unless necessary. ISPs should not be competition sensitive. Competition-sensitive ISPs shall not be accepted.

E4.4.2.7. Broad ranges of activities are needed for effective review of ISPs and its use as a vehicle to conduct a variety of interoperability, net-readiness, and supportability assessments. At a minimum, the following offices shall review the ISP: the USD(AT&L); the ASD(NII)/DoD CIO; the DOT&E; the Joint Staff; the Combatant Commands; the Services; the DIA, the NSA/CSS, the NGA; and the DISA.

E4.4.2.8. After administrative evaluation of the ISP to determine its readiness for external review, the ASD(NII)/DoD CIO shall release the document for the DoD-level review, assessment, and comment. Information derived from the ISP shall be the

basis of supportability and intelligence certifications by the Joint Staff at the appropriate milestones.

E4.4.2.9. The ISP review shall include an assessment of the program's compliance with DoD IT and NSS goals and objectives. These include the following:

E4.4.2.9.1. Compliance with the NCOW RM as instantiated in associated integrated architecture products and implemented through systems engineering.

E4.4.2.9.2. Ability to fully support and use NCES.

E4.4.2.9.3. Ability to support the DoD transformation objective for Task, Post, Process, and Use concept.

E4.4.2.9.4. Compliance with policy-based, defense in depth IA architecture.

E4.4.2.9.5. Compliance with DoD and net-centric data strategy.

E4.4.2.9.6. Capacity to access and use key external data sources.

E4.4.2.9.7. Implementation and synchronization of the above goals and objectives for both supporting and supported systems.

E4.4.2.10. Comments for ACAT I, ACAT IAM, and programs designated "Special Interest" by the ASD(NII)/DoD CIO, submitted during the Stage 1 review, shall be approved at the GS-15/O-6/Division Chief level. Comments submitted during the Stage 2 review shall be approved at the Senior Executive Service/Flag Officer level. For ACAT II and III programs, Stage 2 reviews shall be approved at the GS-15/O-6/Division Chief level. Stage 2 reviews shall include final intelligence supportability certification by the Joint Staff for Milestone C. Comments shall reflect the position of the responding OSD PSAs, the Military Services, the Joint Staff, the Combatant Commanders, or Defense Agencies. The ASD(NII)/DoD CIO shall review comments for adequacy and to determine consistency with DoD information policy, goals, and objectives.

E4.4.2.11. The ASD(NII)/DoD CIO shall return formal comments to the PM, as an attachment under a standard cover letter, providing an overall assessment of the ISP (concurrence, concurrence with comments, or non-concurrence with comments) and a statement as to whether there are any "critical" issues. Instructions shall also be provided for completing the process. This memorandum shall be signed by the appropriate Director in the Office of the ASD(NII)/DoD CIO.

E4.4.2.12. The objective of the review process is to complete the Stage 2 review prior to the milestone or decision review to allow the PM sufficient time to address and/or resolve outstanding critical issues raised during ISP coordination.

However, ISP review status shall not by itself delay a program milestone review. Any decision to delay program milestone review shall be made by the ASD(NII)/DoD CIO. The PM shall address critical, open ISP issues even after milestone approval. Language may be added to the Acquisition Decision Memorandum or provided in a separate memorandum from the ASD(NII)/DoD CIO providing instructions and schedule for ISP completion or issue resolution. The DoD Component is the approval authority for the ISP after ASD(NII)/DoD CIO review and concurrence. Component-approved Stage III ISPs, for all ACAT and non-ACAT programs, shall be submitted into the JCPAT-E ISP document repository as the ISP record copy.

E4.4.2.13. In addition to review of individual ISPs, the ASD(NII)/DoD CIO shall extract information from other relevant ISPs and sources to facilitate identification and resolution of cross-program IT and NSS infrastructure and information support issues. This shall include issues identified in other relevant ISPs during the DoD-level review process. The ASD(NII)/DoD CIO shall raise, as desired, significant program-specific issues identified during this process with the DoD Component preparing the ISP.

E4.4.3. Issue Tracking. Issues identified in Chapter 3 of the ISP and DoD-level reviews shall be posted in the ASD(NII)/DoD CIO issue database and the JMAAT.

E4.4.3.1. Issues are derived from the ISP analysis and DoD level reviews. Derived information support requirements for interoperability, supportability, and net-readiness are identified during ISP development. Derived information support requirements, which cannot be satisfied, shall be identified as ISP issues. The ISP shall document all issues, schedules for their resolution, and strategies for mitigating the issues until each is resolved. The program's acquisition strategy shall summarize critical issues from the ISP and its review. The acquisition strategy, for programs that have not yet completed an ISP, shall include a placeholder in the strategy for an ISP issue summary.

E4.4.3.2. The JMAAT shall be the official database for ISP issues. Issues identified in ISPs and Stage II reviews shall be posted to the JMAAT. The ASD(NII)/DoD CIO shall also maintain a database of critical and substantive issues. The ASD(NII)/DoD CIO may conduct cross-program analysis using ISPs. The results of cross-program analysis may identify capability or program issues that shall be provided to various forums to include FCBs and PPBE activities for consideration and resolution.

E4.4.4. Issue Resolution. Issues identified in the ISP and subsequent DoD-level reviews shall be forwarded to appropriate forums for resolution.

E4.4.4.1. The goal of the ISP process is to resolve all critical issues at the lowest possible level.

E4.4.4.2. Issues, especially those related to information or information support, may manifest themselves in the need for a new capability. In some cases, such as requirements unique to a particular program, the sponsor of the supported program shall

be responsible for identifying the required capability using the JCIDS process. In other cases, when resolution of an issue lies outside the sponsor's responsibility, it may be forwarded by the ASD(NII)/DoD CIO to appropriate forums (e.g., MCEB, MIB, FCBs, FCB Working Groups, etc.) to facilitate resolution.

E4.4.5. Milestone Requirements. The process is repeated at each major milestone, at major changes to the JCIDS documentation, and at major program upgrades. The ASD(NII)/DoD CIO may also request an ISP or updated ISP at any time for specific purposes.

E4.5. OTHER PROCEDURES

E4.5.1. Waivers

E4.5.1.1. The requirement for an ISP may be waived when the requirement for JCIDS documentation has been waived.

E4.5.1.2. A PM may request a waiver, by memorandum, through the ASD(NII)/DoD CIO (for concurrence), to the MDA for the program. The MDA may grant a waiver if ASD(NII)/DoD CIO has provided concurrence. Waiver requirements apply to all ACAT and non-ACAT ISPs. Waiver authority for non-ACAT ISPs resides with the MDA or cognizant fielding authority.

E4.5.2. ISP Special Interest Designation

E4.5.2.1. The ASD(NII)/DoD CIO may designate ACAT II or III programs as ISP Special Interest. Programs designated as ISP Special Interest require a DoD-level review of the ISP coordinated by the ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO shall designate a program as an ISP Special Interest program through a memorandum from the DoD DCIO to the program office. The ASD(NII)/DoD CIO shall maintain a listing of those programs so designated.

E4.5.2.2. The USD(AT&L), the Joint Staff, the Commander, USJFCOM, and the other DoD Components may recommend programs for the ISP Special Interest list (e.g., identification of non-standard information requirements, mismatch of time-critical information support requirements, and gaps or missing technical capabilities that impact supporting or supported systems).

E4.5.2.3. Special Interest designated program ISPs shall be reviewed using the same process as ACAT I and IA programs.

E4.5.3. ACAT II, III, and Non-ACAT Program ISPs

E4.5.3.1. The DoD Components are responsible for ensuring all ACAT II, III, and non-ACAT programs complete an ISP as outlined in this enclosure. Each DoD Component shall develop an ISP review and approval process and provide a copy of the ACAT II, III, and non-ACAT ISP to the ASD(NII)/DoD CIO. DoD Component-approved Stage III ISPs shall be submitted to the JCPAT-E document repository as documents of record. The DoD Components shall ensure a rigorous ISP approval process for ACAT II, III, and non-ACAT programs.

E4.5.3.2. The ASD(NII)/DoD CIO may review ACAT II, III, and non-ACAT ISPs for cross-program issues. The ASD(NII)/DoD CIO may also require the DoD Component to resubmit the ISP if it does not meet the requirements of this enclosure.

E4.5.4. ISP Relationships

E4.5.4.1. The ISP documents the information support needed to respond to an ICD, CDD, and CPD by describing and evaluating the information needs (including intelligence), infrastructure, and other IT and NSS interfaces that the acquisition program needs during development, testing, training, and operation. When the JCIDS documents are updated, the DoD Component shall also update the ISP, as appropriate.

E4.5.4.2. Capabilities may be either providers or consumers of information, and in some cases may fall into both categories. For the purposes of the ISP, the focus should be on information required for consumption to support or enable the receiving or consuming capability. Depending on the risk level associated with the absence of specific information, unsupported information needs could result in the ultimate success or failure of the consuming capability. These information needs can be used to define testing criteria and are useful in determining critical threads. To assess the supportability of IT and NSS, understanding these relationships is critical to the success of supported higher-level warfighting capabilities.

E4.5.4.3. The ISP should evolve, over time, as system functionality evolves (e.g., through incremental and spiral development). The ISP should include projections of evolutionary functionality and support implications required for incorporating future concepts. ISPs should also identify information needs to support system development, testing, and training.

E4.5.4.4. The acquisition strategy addresses major IT and NSS information need considerations for the acquisition program. This includes major information and information infrastructure enhancements and critical issues resolutions necessary for program success. The acquisition strategy shall include a summary of the critical issues and resolutions to be identified in the ISP. If the ISP is not completed, the acquisition strategy shall include a plan to complete the ISP. The summary of ISP issues and resolutions in the acquisition strategy shall point to the ISP, when complete, for details.

E4.5.4.5. The TEMP addresses key system interfaces and measurable test parameters. The TEMP documents the overall structure and objectives of the tests that will be performed to evaluate system net-readiness, interoperability, and information supportability and sufficiency. This includes the NR-KPP from the associated JCIDS documents; and the IT and NSS interfaces specified in the ISP. The TEMP developer should use the ISP as a source of information for test plan development. Testing should address all testable issues identified in the ISP.

E4.5.4.6. Intelligence, interoperability, and supportability certifications are required from the Joint Staff. The ISP documents a program's information needs, the nature of its external interfaces, the NR-KPP, and integrated architecture products necessary to support these certifications.

Attachments - 2

E4.A1. Information Support Plan (ISP) Format Guidance

E4.A2. ISP Architecture Guidance

E4.A1. ATTACHMENT 1 TO ENCLOSURE 4

INFORMATION SUPPORT PLAN (ISP) FORMAT GUIDANCE

E4.A1.1. FORMAT

ISPs shall contain an Introduction (consisting of an overview and program data); an Analysis Chapter that consists of an incremental analysis process that shall be appropriately tailored to each program; an Issues Chapter that details the information, interoperability and synchronization issues identified in the analysis section and the strategy to address or mitigate these issues. ISPs shall also include the following mandatory appendices: References, Systems Data Exchange Matrix (SV-6), Interface Control Agreements, and Acronym List (AV-2). Other Appendices may be included, as necessary. The format within each chapter of an ISP may be tailored to include only those elements that apply to the subject program. The DoD Interim Defense Acquisition Guidebook (reference (ae)) provides additional information for completing each chapter and appendix in the ISP.

E4.A1.1.1. Chapter 1 - Introduction. The introductory chapter shall be organized into two sections, overview and program data. Further details for overview and program data content are provided in reference (ae).

E4.A1.1.1.1. Overview. Provides a brief introduction describing the scope of the program, the program's relationship to other programs, and the program's relationships to relevant JOC(s) and/or JFC(s), JCIDS documents, and associated integrated architectures impacting the program. Do not duplicate JCIDS documentation content, but reference it as appropriate.

E4.A1.1.1.2. Program Data. Provides background information to the ISP reviewer so that the reviewer can understand the context of the ISP. It also documents the status of the acquisition at the point in time that the ISP was developed.

E4.A1.1.2. Chapter 2 - Analysis. Supporting integrated architecture products shall be used in the ISP analysis (see Figure E4.A2.F1.). It is not intended that the prescribed supporting integrated architecture products be developed for ISP purposes only, but rather that the ISP process will exploit existing products to enable better understanding of required information needs for a given program or capability that shall then support refinement of required architecture products. Analysis of the sufficiency of IT and NSS information support needs shall be accomplished in terms of the operational and functional capabilities that are being supported. This analysis requires an understanding of the operational and functional capabilities, and associated metrics to assess and evaluate: organizations; organizational relationships; operational activities; node connectivity and system data exchanges required to achieve a given capability. Table E4.A1.T1. lists the steps in the ISP information needs discovery and analysis process. Further details on accomplishing these steps are provided in reference (ae).

Table E4.A1.T1. Information Needs Discovery and Analysis Process	
Step 1:	Identify the warfighting missions (or functions within the enterprise business domains).
Step 2:	Identify information needed to support operational/functional capabilities for each warfighting mission identified in step 1.
Step 3:	Determine the operational users and notional suppliers of the information needed.
Step 4:	Establish the quality of the data needed to support the functions identified in the programs integrated architecture.
Step 5:	Determine if timeliness criteria exist for the information.
Step 6:	Determine/Estimate the quantity of information of each type that is needed.
Step 7:	Discuss how the information will be accessed or discovered.
Step 8:	Assess the ability of supporting systems to supply the necessary information.
Step 9:	Discuss RF Spectrum needs.
Step 10:	Perform a Net-Centric Assessment.
Step 11:	Discuss the program's inconsistencies with the GIG Integrated Architecture and its strategy for getting into alignment.
Step 12:	Discuss the program's Information Assurance strategy and reference the Program Protection Plan.
Step 13:	Identify information support needs to support development, testing and training.

E4.A1.1.3. Chapter 3 - Issues. Issues shall be presented in a table (see Table E4.A1.T2.) or an outline containing the same data. Operational issues shall be grouped under the mission impacted, then under the functional capability impacted under that mission. When an issue involves more than one mission, subsequent missions shall be marked with the previous issue number and those fields that are the same as the original, should be marked as such. If the issue's impact differs between missions, then the description for each mission may also differ accordingly. The following minimum column headings: Issue Number; Supporting System; Issue, Issue Description; Issue Impact; and Mitigation Strategy or Resolution Path. Number each issue as "C-#;" for critical shortfalls and "S-#" for substantive issue. Issues shall include resolution paths with projected dates to be corrected. If resolution details are not known, a discussion on the approach (including anticipated responsible parties) shall be provided.

Table E4.A1.T2. Issue Summary					
Operational Issues					
Mission					
Functional Capabilities impacted					
Issue number	Supporting system	Issue	Issue Description	Issue Impact	Mitigation Strategy/Resolution Path (and Timeframe)
Development Issues					
Testing Issues					
Training Issues					

E4.A1.2. APPENDICES

E4.A1.2.1. Appendix A. - References. Identify all related documents (with dates) used to prepare the ISP. All essential and supporting products used in the ISP analysis shall be listed in Appendix A, to include: integrated architecture products; the System Threat Assessment; Analysis of Alternatives; JCIDS documentation; TEMP; System Acquisition Master Plan Acquisition Strategy; Acquisition Program Baseline; and ISPs for other systems. Except the approved or draft JCIDS documents, do not include copies of the reference documents. Indicate sources for any documents that are not available electronically from the program office.

E4.A1.2.2. Appendix B. - Systems Data Exchange Matrix (SV-6). Appendix B shall consist of a detailed SV-6 matrix derived from the associated integrated architectures, with narrative discussion as necessary. Provide additional systems data exchange information (and supporting discussion), identified during the ISP analysis, for each system interface, if not already incorporated in JCIDS documentation. These shall be discussed in the main body of the ISP in the Analysis Section.

E4.A1.2.3. Appendix C. - Interface Control Agreements. Identify documentation that indicates agreements made (and those required) between the subject ISP program and those programs necessary for information support. For example, if System A is relying on information from System B, then this interface dependency must be documented. At a minimum, this dependency should be identified in the ISPs for both System A (the information recipient) and System B (the information provider).

E4.A1.2.4. Appendix D. - Acronym List. Provide an Integrated Dictionary formatted as an AV-2.

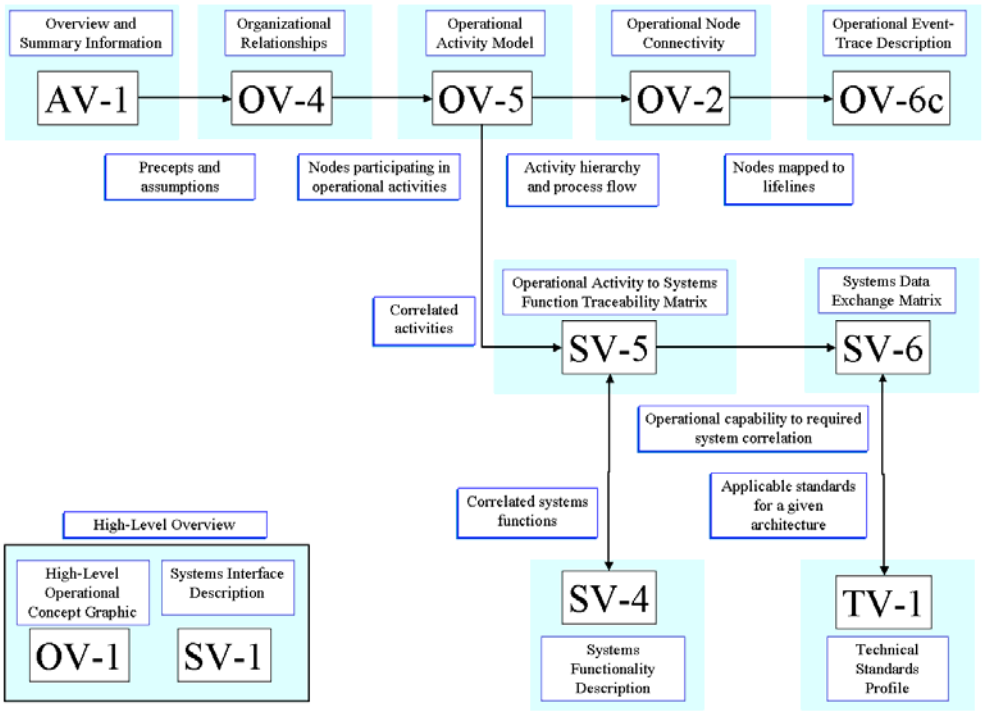
E4.A1.2.5. Other Appendices. Provide supporting information, as required, not included in the body of the ISP or relevant JCIDS documents. Additional, or more detailed information, used to satisfy DoD Component-specific requirements, shall be included as an appendix, and not incorporated in the body of the subject ISP. Additional architecture products used in the ISP analysis will be provided in a separate appendix and referenced in the main body of the ISP. For non-ACAT and fielded acquisitions and procurements, the NR-KPP shall be documented as a separate appendix to the ISP.

E4.A2. ATTACHMENT 2 TO ENCLOSURE 4

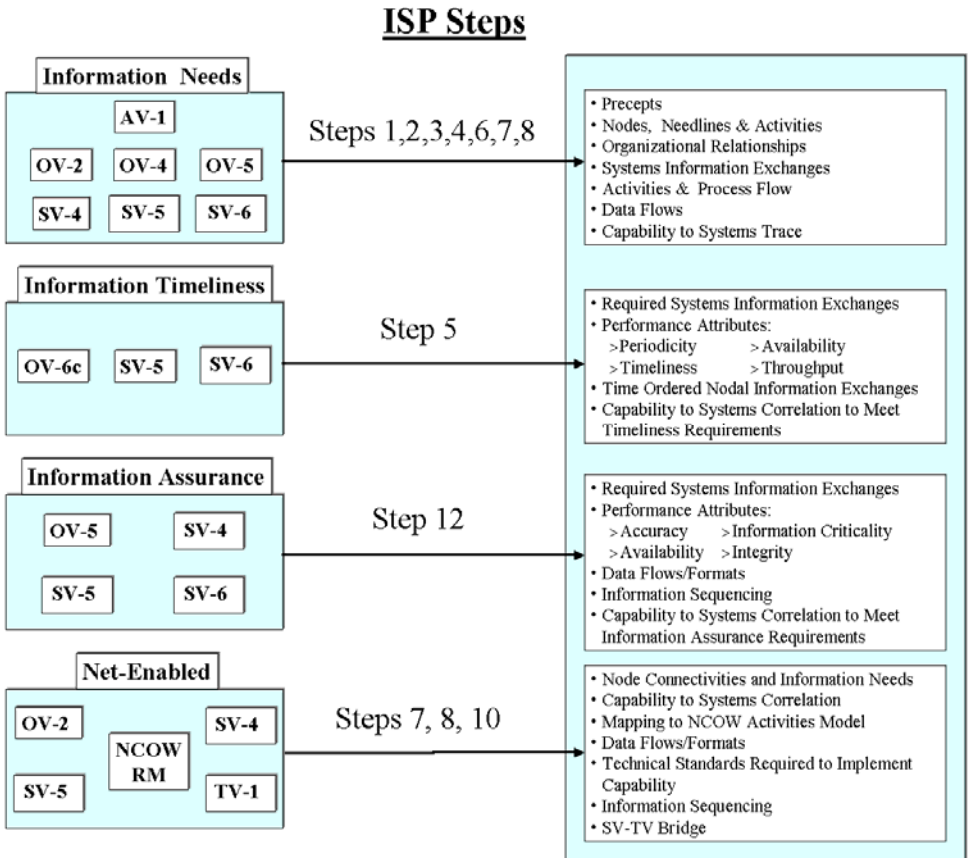
INFORMATION SUPPORT PLAN (ISP) ARCHITECTURE GUIDANCE

E4.A2.1.1. Figure E4.A2.F1. provides a summary of the integrated architecture products, and corresponding relationships, from the DoD Architecture Framework, needed to complete the ISP. These supporting integrated architecture products provide the basis for assessing information needs, information timeliness, information assurance, and net-ready attributes of information exchange and use. Analysis shall include the degree to which requirements of the NR-KPP have been satisfied. Additional integrated architecture products shall be developed as necessary for refining detail in this assessment. Additional integrated architecture products, developed for the ISP analysis, shall be included as an appendix in the ISP.

Figure E4.A2.F1. Architecture View Summary



E4.A2.1.2. Figure E4.A2.F2. provides a summary of supporting integrated architecture products, with corresponding steps of the ISP process, required to assess information needs, information timeliness, information assurance, and net-ready attributes for information exchange and use. Figure E4.A2.F2. Architecture Views for Net-Ready KPP Areas of Analysis



E4.A2.1.3. Figure E4.A2.F3. suggests appropriate integrated architecture products required to evaluate information needs/dependencies, quality, quantity, sources, and timeliness.

Figure E4.A2.F3. Architecture Views vs. Analysis Areas

	Area For Analysis					
Architectural View	**Overview**	**Information Need/Dependency**	**Information Quality**	**Information Quantity**	**Information Sources**	**Information Timeliness**
AV-1	●					
OV-1	●					
OV-2		●			●	
OV-4		●				
OV-5		●				●
OV-6c		●				●
SV-1	●	●			●	
SV-4	●	●				
SV-5		●	●	●	●	●
SV-6		●	●	●	●	●
TV-1		●	●			●