



Department of Defense INSTRUCTION

NUMBER 4630.8

May 2, 2002

ASD(C3I)

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

- References:
- (a) DoD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," November 18, 1992 (hereby canceled)
 - (b) [DoD Directive 4630.5](#), "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," January 11, 2002
 - (c) Chapter 25 of title 40, United States Code, "Division E of the Clinger-Cohen Act of 1996"
 - (d) "Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework," Version 2.0, December 18, 1997
 - (e) through (o), 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 an approach that considers both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership, and personnel) aspects to ensure life-cycle interoperability and supportability of IT and NSS throughout the Department of Defense (DoD). This approach ensures that information is available to the Department of Defense in an assured, timely, useable, understandable, and cost-effective manner.

1.3. Implements an outcome-based, mission area focused process whereby IT and NSS interoperability and supportability requirements for new, modified, and fielded systems are documented, coordinated, implemented, verified, and approved to achieve an integrated, and secure IT and NSS infrastructure supporting global operations across the peace-conflict spectrum.

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. 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 (see paragraph E2.1.11., below), the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. All IT, including NSS, acquired, procured (systems or services), or operated by any component of the Department of Defense, 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, Advanced Technology Demonstrations, and Joint Warrior Interoperability Demonstration Gold Nuggets 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 Commander in Chief (CINC) Command and Control Initiative Program, CINC Initiatives Fund, CINC 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 effectively in joint, combined, coalition, and interagency operations and simulations.

2.2.3. 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 Directive recognizes that special measures may be required for protection/handling of foreign intelligence or counterintelligence information, or other need to know information. Accordingly, implementation of this Directive must be tailored to comply with separate and coordinated Director of Central Intelligence (DCI) Directives and Intelligence Community policies.

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

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

4. POLICY

It is DoD policy that:

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

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

4.3. For the purposes of interoperability and supportability, IT and NSS used by U.S. Forces shall be developed with the capability to meet essential operational needs, and where required, shall interoperate with existing and planned, functionally related, systems and equipment of joint, combined, and coalition forces; and with other U.S. Government Departments and Agencies, as appropriate.

4.4. IT and NSS interoperability and supportability requirements shall be characterized through operational mission area integrated architectures, operational concepts and Capstone Requirements Documents (CRDs) derived from Joint Mission Areas (JMAs), and business/administrative mission areas. The Joint Operational Architecture (JOA), the Joint Systems Architecture (JSA), and the Joint Technical Architecture (JTA) shall serve as the foundation for development of mission area integrated architectures. Mission area integrated architectures shall relate IT and NSS interoperability and supportability requirements in a Family-of-Systems/System-of-Systems (FoS/SoS) context. IT and NSS FoS/SoS Information Exchange Requirements (IERS) and associated interoperability Key Performance Parameters (KPPs) shall be derived from the operational view of the mission area integrated architecture.

4.5. IT and NSS interoperability and supportability needs shall be identified through the requirements definition and validation process, in conjunction with the acquisition process, and shall be updated as necessary throughout the system's life. IT and NSS interoperability and supportability requirements shall be specified to a level of detail that allows verification of interoperability throughout a system's life. For IT and NSS defense acquisition and procurement programs, an interoperability KPP shall be defined during the requirements definition and validation process. The defined interoperability KPP shall be developed in such a way that it can be reliably measured, tested and evaluated. If an evolutionary acquisition strategy is employed, IT and NSS interoperability and supportability requirements shall evolve consistent with the evolutionary acquisition approach.

4.6. IT and NSS interoperability and supportability shall be managed, evaluated, and reported over the life of the system.

4.6.1. For all DoD Acquisition Category (ACAT) programs, a Command, Control, Communications, Computers, and Intelligence (C4I) Support Plan shall be used to document interoperability and supportability requirements. The C4I Support Plan shall contain detailed and time-phased information for identifying dependencies and interface requirements consistent with mission area integrated architectures, focusing attention on interoperability, supportability, and sufficiency 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 assessment of the systems' KPP capabilities and limitations.

4.6.2. For non-ACAT programs, a determination of IT and NSS interoperability and supportability requirements shall be identified and documented in a management/support plan analogous to the C4I Support Plan. For non-ACAT IT and NSS, the program support or management plan shall contain sufficient detail (commensurate with the size of the program/effort) to permit an evaluation of the associated interoperability and supportability requirements.

4.7. IT and NSS shall be tested early and with sufficient frequency throughout a system's life or upon changes affecting interoperability or supportability to assess, evaluate, and certify its overall level of interoperability and supportability. This certification will be cost effective and shall be successfully completed prior to fielding of new IT and NSS or prior to fielding a new capability or upgrade to existing IT and NSS.

4.8. The process for improving IT and NSS interoperability and supportability shall provide solution sets focused on mission-based outcomes that address both materiel and non-materiel aspects. Once IT and NSS interoperability solution sets are validated, appropriate resources shall be recommended to implement identified remedies. As part of this process, the operational community shall identify, prioritize, and synchronize non-materiel solutions with materiel solutions to resolve interoperability and supportability issues.

4.9. IT and NSS interoperability and supportability oversight and direction shall be jointly provided by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); the Under Secretary of Defense (Comptroller) (USD(C))/DoD Chief Financial Officer (DoD CFO); the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)), ASD(C3I) as the DoD Chief Information Officer (CIO); the Director of Operational Test and Evaluation (DOT&E); the Chairman of the Joint Chiefs of Staff; and the Commander in Chief, U.S. Joint Forces Command (USCINCFJCOM), as appropriate.

5. RESPONSIBILITIES

Under the provisions of DoD Directive 4630.5 (reference (b)):

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, shall:

5.1.1. Define interoperability policy for all Major Automated Information System ACATIA acquisition programs, with the USD(AT&L).

5.1.2. Establish a process, with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, and the Combatant Commands, for early identification of potential FoS/SoS IT and NSS interoperability and supportability issues.

5.1.3. Report, prior to each program review, to the Milestone Decision Authority (MDA) the extent to which an IT or NSS program is meeting its interoperability KPP and supportability requirements. If satisfactory progress is not being made, recommend, with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, and other DoD Components, a course of action that the program office must take.

5.1.4. Establish, with the USD(AT&L) and the DoD CIO, format and content guidance for the C4I Support Plan to identify system interfaces, dependencies and operational context for IT and NSS capabilities.

5.1.5. Lead DoD-wide review of C4I Support Plans for all ACATI and IA acquisition and special interest programs. Ensure all C4I Support Plans, regardless of ACAT, are forwarded to the Defense Information Systems Agency (DISA) for review.

5.2. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, as the DoD Chief Information Officer, shall:

5.2.1. 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.

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

5.2.3. Develop, maintain, and facilitate the implementation of a sound and integrated Information Technology Architecture (ITA) for all DoD IT and NSS, as required by references (b) and (c).

5.2.4. Ensure, with the USD(AT&L), the Chairman of the Joint Chiefs of Staff and the U.S. Joint Forces Command, that FoS/SoS IT and NSS mission area integrated architectures are defined, developed, integrated, coordinated, validated, synchronized, and implemented. Establish format and content requirements for integrated architectures in DoD C4ISR Architecture Framework (reference (d)). Development of mission area integrated architectures shall be consistent with the products required by reference (d).

5.2.5. Establish processes, with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, and the other DoD Components, to review and verify that interoperability KPPs are adequately defined, and that IT and NSS interoperability and supportability test objectives are consistent with assessing the interoperability KPP.

5.2.6. Establish responsibilities and procedures, with the USD(AT&L), the DOT&E, the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, and other DoD Components, to ensure early information interoperability assessment, verification, and evaluation of IT and NSS interoperability KPPs, and reassessment and re-evaluation, as required, throughout a system's life. The DoD CIO, with the DoD Components, shall also ensure that user-defined, mission-related, outcome-based performance measures are established for information interoperability assessment and verification (refer to enclosure 2 for definitions) of IT and NSS interoperability KPP.

5.2.7. Develop a process, with the DoD Components, to annually evaluate DoD IT and NSS interoperability and supportability status. Findings will be reported to the Deputy Secretary of Defense in sufficient time to support the Department's budget decisions.

5.2.8. Maintain liaison with the office of the Intelligence Community (IC) CIO to ensure continuous coordination of DoD and IC interoperability and supportability issues.

5.2.9. Define, organize, and approve, with the USD(AT&L), the Chairman of the Joint Chiefs of Staff, and other DoD Components, Universal Reference Resources for developing mission area integrated architectures throughout the Department of Defense.

5.2.10. Prescribe approved IT and NSS standards with the DoD Components that apply throughout the Department of Defense, and, to the extent possible, work with the IC CIO to develop a consistent set of prescribed standards for both communities.

For non-acquisition (non-ACAT) matters, the prescription of IT and NSS standards shall consider tradeoffs among operational effectiveness, operational suitability, information assurance and IT and NSS interoperability and supportability. Develop and promulgate the DoD JTA with other DoD Components.

5.2.11. 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:

5.2.11.1. Assess and evaluate IT and NSS acquisitions and procurements, and, 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.

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

5.2.12. Establish a process, with the USD(AT&L), the USD(C)/DoD CFO, the DOT&E, the other DoD Components, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command, to propose operationally prioritized recommendations to the DAB, DoD Overarching IPTs, DoD CIO Reviews, and the Joint Requirements Oversight Council (JROC), as appropriate, for resolving critical IT and NSS interoperability and supportability 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 (e.g., early testing using prototypes).

5.2.13. Provide oversight and direction, with the USD(C)/DoD CFO, the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, and other DoD Components, of the small transition fund (currently within Navy Program Element "Joint 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 U.S. Joint Forces Command in Doctrine, Organization, Training, Materiel, Leadership 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.

5.2.14. Maintain consolidated DoD Mission Critical Information System (MCIS) and Mission Essential Information System (MEIS) lists, and associated systems interfaces, for use by the DoD Components in acquisition of IT and NSS and to identify candidate IT and NSS for interoperability assessments, test and evaluations, and interoperability certifications.

5.2.15. Establish and maintain, 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 C4ISR Core Architecture Data Model.

5.2.16. Provide a senior representative to co-chair the Interoperability Senior Review Panel (ISRP) with the USD(AT&L), the USD(C)/DoD CFO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command.

5.2.17. Co-chair the Architecture Implementation Council (AIC) with the USD(AT&L) and the Joint Community CIO to synchronize the Department's integrated architecture activities and guidance.

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

5.3.1. As the DoD Acquisition Executive (reference (e)), ensure the policies outlined in section 4., above, are incorporated into the DoD 5000 series acquisition documents (references (f), (g), and (h)) and adequately addressed, during system acquisitions, as appropriate.

5.3.2. For all ACAT acquisition and procurement matters, with the DoD CIO, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command, approve tradeoffs among operational effectiveness, operational suitability, and IT and NSS interoperability and supportability.

5.3.3. Manage acquisition of Major Defense Acquisition Program-related IT and NSS and assist the DoD CIO, the ASD(C3I), the DOT&E, the other DoD Components, and the Chairman of the Joint Chiefs of Staff, in the evaluation of interoperability and supportability requirements in a FoS/SoS context.

5.3.4. Ensure, with the DoD CIO, the Chairman of the Joint Chiefs of Staff, the JROC and the U.S. Joint Forces Command, that IT and NSS interoperability requirements, as outlined in the C4I Support Plan or analogous management or support plan, are verifiable as part of the acquisition and procurement processes.

5.3.5. Ensure, with the DoD CIO, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command, that the operationally prioritized materiel and non-materiel interoperability requirements are phased for acquisition and implementation.

5.3.6. Establish processes and procedures to identify, coordinate, and integrate DoD systems architecture views into an overall DoD-wide JSA.

5.3.7. Ensure that C4I Support Plan requirements are reflected in policies and directives governing the Defense Acquisition System (reference (g)).

5.3.8. Ensure, through the Director, Strategic and Tactical Systems, that DISA is included in the review of IT and NSS developmental test plans.

5.3.9. Sponsor Joint Test and Evaluations (JT&Es) and, with the DoD Components, identify resulting IT and NSS interoperability and supportability shortfalls and issues.

5.3.10. Establish responsibilities and procedures necessary to ensure comprehensive Developmental Test and Evaluation (DT&E) of interoperability KPP and suitability requirements during system development.

5.3.11. Provide a senior representative to co-chair the ISRP with the USD(C)/DoD CFO, the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command.

5.3.12. Co-chair the AIC with the DoD CIO and the Joint Community CIO, to synchronize the integrated architecture activities and to establish architecture guidance for the Department of Defense.

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

5.4.1. Ensure, 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, with the USD(AT&L), the DoD CIO, the Chairman of the Joint Chiefs of Staff, the other DoD Components, and the U.S. Joint Forces Command, budget recommendations for addressing critical IT and NSS interoperability and supportability issues.

5.4.3. Review and assess the Analysis of Alternatives (AoA).

5.4.4. Review and assess the programming, planning, and budgeting system IT-300 exhibit to ensure that the Architecture and Infrastructure Standards section addresses interoperability.

5.4.5. Provide a senior representative to co-chair the ISRP with the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command.

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

5.5.1. Ensure, with the Chairman of the Joint Chiefs of Staff and the U.S. Joint Forces Command, that interoperability KPPs specified in IT and NSS requirements documents are measurable and contribute to the evaluation of the system's operational effectiveness.

5.5.2. Develop policy and processes, with the USD(AT&L), the DoD CIO, and the other DoD Components, to ensure IT and NSS are tested and evaluated throughout the acquisition and procurement process, and with sufficient frequency during a system's life to accurately assess the level of FoS/SoS IT and NSS interoperability and supportability.

5.5.2.1. Ensure, with the USD(AT&L), the Chairman of the Joint Chiefs of Staff, the DoD CIO, and other DoD Components, that mission-related, outcome-based measures of effectiveness are developed to support evaluations of IT and NSS interoperability and supportability throughout a system's life cycle.

5.5.2.2. Ensure, with the DoD CIO, the USD(AT&L), the Chairman of the Joint Chiefs of Staff, the Joint Forces Command, and other DoD Components, that the proper tools and a testing infrastructure exists to support IT and NSS evaluation in FoS/SoS environments.

5.5.2.3. Assist the DoD Components with operational test planning and assessment of FoS/SoS IT and NSS interoperability and supportability.

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

5.5.4. Identify from testing and evaluation, IT and NSS interoperability and supportability deficiencies and provide these to the USD(AT&L), the DoD CIO, the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, DISA, and the responsible DoD Component, for resolution, as appropriate. Report IT and NSS interoperability and supportability status for each program as it relates to FoS/SoS at milestone reviews, and as part of the DOT&E Annual Report to Congress and the Secretary of Defense.

5.5.5. Establish, with the USD(AT&L), the DoD CIO, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command, an Interoperability Watch List (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. IT and NSS considered for the IWL may be pre-acquisition systems, acquisition programs (any ACAT), already fielded systems, or CINC-unique procurements.

5.5.6. Provide a senior representative to co-chair the ISRP with the USD(AT&L), the USD(C), the DoD CIO, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command.

5.6. The Heads of the DoD Components shall:

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

5.6.1.1. 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 DoD CIO prior to publication.

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

5.6.2. Identify all DoD Component IT and NSS that require internal DoD or external joint, combined, coalition, and U.S. Government Department and Agency information exchanges to the DoD CIO.

5.6.3. Ensure IT and NSS interoperability and supportability capabilities are designed in, developed, tested, evaluated, and incorporated into all DoD Component IT

and NSS. When necessary, recommend tradeoffs among operational effectiveness, operational suitability, and IT and NSS interoperability and supportability to the USD(AT&L), the DoD CIO, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command.

5.6.4. Ensure, for all IT and NSS acquisitions or procurements, that requirements and acquisition documents (i.e., Mission Need Statements (MNSs), CRDs, and Operational Requirements Documents (ORDs); and C4I Support Plans) are submitted to the Chairman of the Joint Chiefs of Staff for certification to ensure compliance with joint policy, doctrine, and interoperability requirements. Requirements documents shall also be submitted to DISA for review of DoD JTA compliance.

5.6.5. Ensure all IT and NSS requirement documents include an interoperability KPP. Interoperability KPPs shall be used when developing C4I Support Plans and test documents.

5.6.6. Identify interoperability performance criteria, analogous to a KPP, to be used when developing non-ACAT management or support plans and submit those criteria to the cognizant authority for review and certification.

5.6.7. Coordinate interoperability requirements with the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, and the Combatant Commanders, to ensure that the system design identifies all critical external IT and NSS interfaces with required joint, combined, and coalition systems.

5.6.8. Ensure that:

5.6.8.1. C4I Support Plans for ACATI and IA, and other acquisition programs in which the OASD(C3I) has indicated a special interest, are submitted to the ASD(C3I) and DISA for review and assessment. Should interoperability issues arise between ACATI or IA and less-than-ACATI or IA programs, the DoD Components shall, if requested, provide the C4I Support Plan for the less-than-ACATI or IA program(s) to the ASD(C3I) to support issue resolution.

5.6.8.2. C4I Support Plans for all ACAT programs are prepared and processed according to references (g) and (h).

5.6.8.3. Analogous management/support plans for non-ACAT programs are prepared and processed as directed by the sponsoring or cognizant authority.

5.6.9. 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 Test and Evaluation Master Plans (TEMPs). Resources include the systems, equipment, and personnel necessary to accomplish IT and NSS interoperability testing.

5.6.10. Assess compliance with FoS/SoS IT and NSS interoperability KPPs and supportability requirements 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.

5.6.11. Provide:

5.6.11.1. Direction to acquisition managers to ensure that all programs using or relying on IT and NSS capabilities are tested and certified at the Service and joint level for IT and NSS interoperability and supportability.

5.6.11.2. Results of all developmental and operational interoperability assessments, tests and evaluations to the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command.

5.6.12. Ensure all appropriate test plans are sufficient to evaluate interoperability requirements and are submitted to the USD(AT&L) and the DOT&E for approval.

5.6.13. Submit to the DISA Joint Interoperability Test Command (JITC), for IT and NSS interoperability certification, those systems acquired or modified through non-ACAT designated acquisitions or procurements (e.g., ACTDs, JWID Gold Nuggets that lead to acquisitions, the CINC Command and Control Initiative Program, CINC Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, and Tactical Exploitation of National Capabilities Programs), DoD Intelligence Information Systems (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.

5.6.14. Develop, 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. Prior to production and fielding approval for all new or modified IT and NSS, the DoD Components shall ensure

systems are tested and evaluated, and certify which of the interoperability criteria have been met.

5.6.15. Comply with procedures the Chairman of the Joint Chiefs of Staff establishes to manage the initiation and processing of IT and NSS interoperability testing waivers. While a waiver from joint interoperability certification (or re-certification) based on justifiable circumstances and impacts may be granted under the authority of the Chairman of the Joint Chiefs of Staff, it shall not be permanent.

5.6.16. Participate in developing programmatic and technical guidance (including the Common Operating Environment (COE)), mission area integrated architectures, strategies, IT and NSS standards (including the DoD JTA), and quantifiable performance measures.

5.6.17. Develop mission area integrated architecture implementation plans; submit them to the DoD CIO for review and approval by the USD(AT&L), and the Chairman of the Joint Chiefs of Staff; and enforce implementation of these plans for all DoD Component IT and NSS.

5.6.18. Submit the following:

5.6.18.1. Proposals for revising or developing standards for IT and NSS interoperability and supportability to the USD(AT&L), the Chairman of the Joint Chiefs of Staff, and DISA.

5.6.18.2. Change requests to the DoD JTA Development Group (JTADG) or Defense Standardization Program Office (DSPO) Standard Preparing Activity when the need for option selection, implementation conventions, or semantic/syntax corrections is identified.

5.6.19. Enforce DoD JTA implementation and establish administrative procedures for submitting Component IT and NSS system-specific JTA waiver requests. A DoD Component Acquisition Executive (CAE) or cognizant official may grant a waiver from JTA use where potential negative impacts to cost, schedule, or performance are identified. Waivers from JTA use shall not be used to waive Defense Information Systems Network or Defense Enterprise Computing Center usage. Waivers for non-ACAT programs require the concurrence of the DoD CIO and the USD(AT&L). For mission-critical or mission-essential ACAT designated programs, all granted waivers shall be submitted through the DoD CIO to the USD(AT&L) for review. In either case, concurrence may be assumed if no response is received within 2 weeks of the date of receipt.

5.6.20. Ensure program managers for IT and NSS acquisitions and procurements include a standards profile and a summary list of all FoS/SoS interfaces in the C4I Support Plan or analogous management/support plan. All IT and NSS acquisition and procurement standards profiles shall be forwarded to DISA for certification.

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

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

5.6.23. Participate in Configuration Management (CM) of interfaces and interface standards.

5.6.24. Generate System Threat Assessment Reports (STARs) that highlight threats to IT and NSS interoperability and supportability.

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

5.7.1. Establish policy and procedures for developing, coordinating, reviewing, and approving IT and NSS interoperability and supportability requirements with the U.S. Joint Forces Command and other DoD Components.

5.7.2. Develop, approve, and direct the use of the JMA-based JOA and direct its use when developing IT and NSS interoperability and supportability requirements. Review and validate that IT and NSS interoperability KPPs in requirement documents are derived from mission area integrated architectures.

5.7.3. Develop, approve, and issue joint doctrinal concepts and associated operational procedures with the USD(AT&L), the DoD CIO, the DOT&E, the U.S. Joint Forces Command, and the other DoD Components, to achieve interoperability and supportability of IT and NSS capabilities employed by U.S. Military Forces and, where required, with joint, combined, and coalition forces, and other U.S. Government Departments and Agencies.

5.7.4. Ensure mission area integrated architectures, strategies, concepts, and visions of the DoD Components are synchronized to support IT and NSS interoperability requirements and identify opportunities for, and impediments to, interoperability.

5.7.5. Establish, with the USD(AT&L), the DoD CIO, the DOT&E, the U.S. Joint Forces Command, and the other DoD Components, procedures to certify and validate the IT and NSS IERs and interoperability KPP throughout a system's life.

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

5.7.7. Establish, with the U.S. Joint Forces Command, a process and procedures to ensure insights gained from joint operations, exercises, and experiments on IT and NSS interoperability and supportability are presented to the DoD CIO, the USD(AT&L), the DOT&E, and the U.S. Joint Forces Command.

5.7.8. Certify interoperability requirements for all IT and NSS requirements documents.

5.7.9. Perform intelligence interoperability assessment of all IT and NSS requirements documents.

5.7.10. Certify, with the assistance of DISA, that IT and NSS interoperability and supportability requirements are established, assessed, and verified for IT and NSS acquisitions prior to production and fielding.

5.7.11. Through the Military Communications Electronics Board (MCEB) and the Military Intelligence Board (MIB), consider interoperability and supportability matters referred to it by the Secretary of Defense, the DoD CIO, and the U.S. Joint Forces Command. These boards shall:

5.7.11.1. Convene a senior resolution body for IT and NSS interoperability and supportability requirements and testing issues.

5.7.11.2. 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.

5.7.11.3. 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 DoD CIO for review.

5.7.12. Provide a senior representative to co-chair the ISRP with the USD(AT&L), the USD(C), the DoD CIO, the DOT&E, and the U.S. Joint Forces Command.

5.7.13. Co-chair the AIC with the USD(AT&L) and the DoD CIO to synchronize integrated architecture activities and to establish architecture guidance for the Department of Defense.

5.8. The Commander-in-Chief, U.S. Joint Forces Command, shall:

5.8.1. 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:

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

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

5.8.2. Participate in the requirements validation process for IT and NSS. Review and confirm that the interoperability IERs and KPPs are sufficient for requirements documents. This assessment shall be based on the warfighter's perspective using mission area integrated architectures.

5.8.3. Determine, 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 DoD CIO, the DOT&E, and the other DoD Components, as appropriate.

5.8.4. Collect, consolidate, and prioritize the IT and NSS interoperability and supportability requirements for emerging and fielded Joint Task Force systems using the DoD Components' inputs. Assess the current operational force capability against the requirement to determine the impact on warfighting readiness and leverage existing repositories of the Chairman of the Joint Chiefs of Staff, Agencies, and the ASD(C3I) for these issues, to produce a consolidated priority list of interoperability and supportability shortfalls.

5.8.5. Participate, as appropriate, in assessing, testing, and evaluating IT and NSS interoperability and supportability.

5.8.6. Propose to the USD(AT&L), the 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.

5.8.7. Provide a senior representative to co-chair the ISRP with the USD(AT&L), the USD(C)/DoD CFO, the DoD CIO, the DOT&E, and the Chairman of the Joint Chiefs of Staff.

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

5.9.1. Establish and conduct an IT and NSS interoperability and supportability assessment, test, and evaluation program, in collaboration with the other DoD Components.

5.9.2. Manage the Joint IT and NSS Interoperability Assessment, Test, and Evaluation Program. The DISA (JITC) shall certify joint and combined IT and NSS systems interoperability for the Department of Defense.

5.9.3. Certify IT and NSS conformance with and implementation of DoD JTA standards to the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, the U.S. Joint Forces Command, and to the developmental, operational, and interoperability testing organizations of the DoD Components.

5.9.4. 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.

5.9.5. 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 DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, the other DoD Components, the U.S. Joint Forces Command, and to the developmental and operational testing organizations of the DoD Components.

5.9.6. Provide systems engineering, planning, and program guidance. 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 reference (i) consider spectrum supportability, and control of Electromagnetic Environmental Effects (E3). DISA shall make DoD JTA-compliant and National Security Agency (NSA)-verified platform solutions available to the DoD Components for proof-of-concept, prototyping, and IT and NSS development. DISA shall also ensure that the DoD Components have access to DoD JTA-compliant/NSA-verified router, local area network, and network security solutions.

5.9.7. Review DoD Component requirements documents, TEMP's, C4I Support Plans, or equivalent documentation to assess if interoperability KPPs 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.

5.9.8. Review TEMP's, or equivalent documents, and recommend IT and NSS interoperability test and evaluation criteria for test plans.

5.9.9. Establish an IT and NSS interoperability assessment process requirements repository for all requirements documents and C4I Support Plans. Verify and coordinate with the DoD CIO and the Chairman of the Joint Chiefs of Staff that proposed inputs to the repository are consistent with appropriate techniques, procedures, architectures, and DoD JTA standards.

5.9.10. Serve as the DoD CIO's Executive Agent for developing, and prescribing IT and NSS standards that apply to interoperability throughout the Department of Defense. As the DoD Executive Agent, coordinate and integrate DoD IT standards activities and processes to promote compliance with IT and NSS standards.

5.9.11. Develop and maintain, with the DoD Components, the DoD JTA to prescribe IT and NSS standards for the Department of Defense. Administer the process to ensure that appropriate standards are available and used, including defining standards requirements and planning, prioritizing, and providing required resources to standards projects.

5.9.12. 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). DISA shall maintain a list of products that conform to DoD JTA-mandated standards.

5.9.13. Provide an assessment of the suitability of standards identified in requirement documents and C4I Support Plans submitted under this Instruction. DISA shall forward standards issues that cannot be resolved to the MCEB or MIB, as appropriate.

5.9.14. Ensure that test documentation and C4I Support Plans identify DoD JTA-mandated standards and 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 (C3I), the DoD CIO, the DOT&E, and the Chairman of the Joint Chiefs of Staff on planned IT and NSS interoperability assessments, tests, and evaluations.

5.9.15. Certify, through the DISA (JITC) for all applicable IT and NSS programs, to the Operational Test Agency (OTA) during (or prior to) the Operational Test Readiness Review (OTRR):

5.9.15.1. The status of all IT and NSS interoperability and standards conformance issues.

5.9.15.2. That all required developmental testing relating to IT and NSS interoperability has been successfully completed.

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

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

5.9.17. Coordinate with the Defense Intelligence Agency (DIA) regarding IT and NSS interoperability certification processes.

5.10. The Director, Defense Intelligence Agency shall:

5.10.1. 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.

5.10.2. Coordinate with DISA to define and implement standards within the DoD JTA and DoDIIS that are consistent with the mission area integrated architectures of the Intelligence Community.

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

5.10.4. Evaluate the IT and NSS interoperability and supportability in requirements documents and C4I Support Plans, and coordinate with DISA on matters involving IT and NSS interoperability certification processes.

5.10.5. Coordinate with DISA and NSA on the requirements for defining and implementing IT and NSS standards.

5.10.6. 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.

5.10.7. Validate DoD Component's STARS that highlight threats to IT and NSS interoperability and supportability.

5.11. The Director, National Security Agency, shall:

5.11.1. As the Community Functional Lead for Cryptology, coordinate with the appropriate DoD Components on matters involving IT and NSS interoperability and supportability of cryptologic systems.

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

5.11.3. As technical oversight authority for tactical SIGINT systems and programs (reference (k)), provide cryptologic expertise and assistance in assessing IT and NSS requirement documents for interoperability. Generate System Threat Assessment Reports (STARS) that highlight threats to IT and NSS interoperability and supportability between tactical SIGINT systems and with NSA IT and NSS.

5.11.4. 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 to secure NSS.

5.11.5. Ensure interoperability and supportability of NSA IT and NSS with those systems that provide direct support to the combatant commander.

5.11.6. Ensure, with other DoD Components, that NSA mission area integrated architecture requirements 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.

5.11.7. Ensure NSA IT and NSS programs are certified for standards conformance and IT and NSS interoperability and supportability.

5.11.8. Ensure, with other DoD Components, that NSA IT and NSS interoperability requirements for processing foreign intelligence and foreign counterintelligence information are satisfied by designing and developing interoperable and supportable technical, procedural, and operational interfaces.

5.11.9. 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.

5.12. The Director, National Imagery and Mapping Agency, shall:

5.12.1. Ensure, by coordinating with the other DoD Components, that U.S. Imagery and Geospatial Information Service (USIGS) standards and specifications for imagery, imagery intelligence, and geospatial information (formerly mapping, charting, and geodesy) support the interoperability and supportability of IT and NSS.

5.12.2. Ensure USIGS standards and specifications incorporate imagery and geospatial information release or disclosure decisions.

5.12.3. Ensure that industry and non-governmental standards used for imagery and geospatial systems and applications are open-systems based and conform to COE and DoD JTA tenets for interoperability.

5.12.4. 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.

5.13. The Department of Defense Architecture Implementation Council, co-chaired by the USD(AT&L), the DoD CIO, and the Joint Community CIO, shall synchronize integrated architecture activities, establish DoD architecture guidance, and

serve as the senior resolution body for interoperability issues related to DoD integrated architectures efforts. The co-chairs shall determine appropriate membership for the AIC.

5.14. The Interoperability Senior Review Panel (ISRP), co-chaired by senior representatives from the USD(AT&L), the USD(C)/DoD CFO, the ASD(C3I), as the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command, shall:

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

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

5.14.3. Review and comment on interoperability deficiencies and proposed DOTMLPF solution sets identified by the U.S. Joint Forces Command.

5.14.4. Review critical systems and programs with significant interoperability deficiencies and approve appropriate candidates for the IWL.

6. PROCEDURES

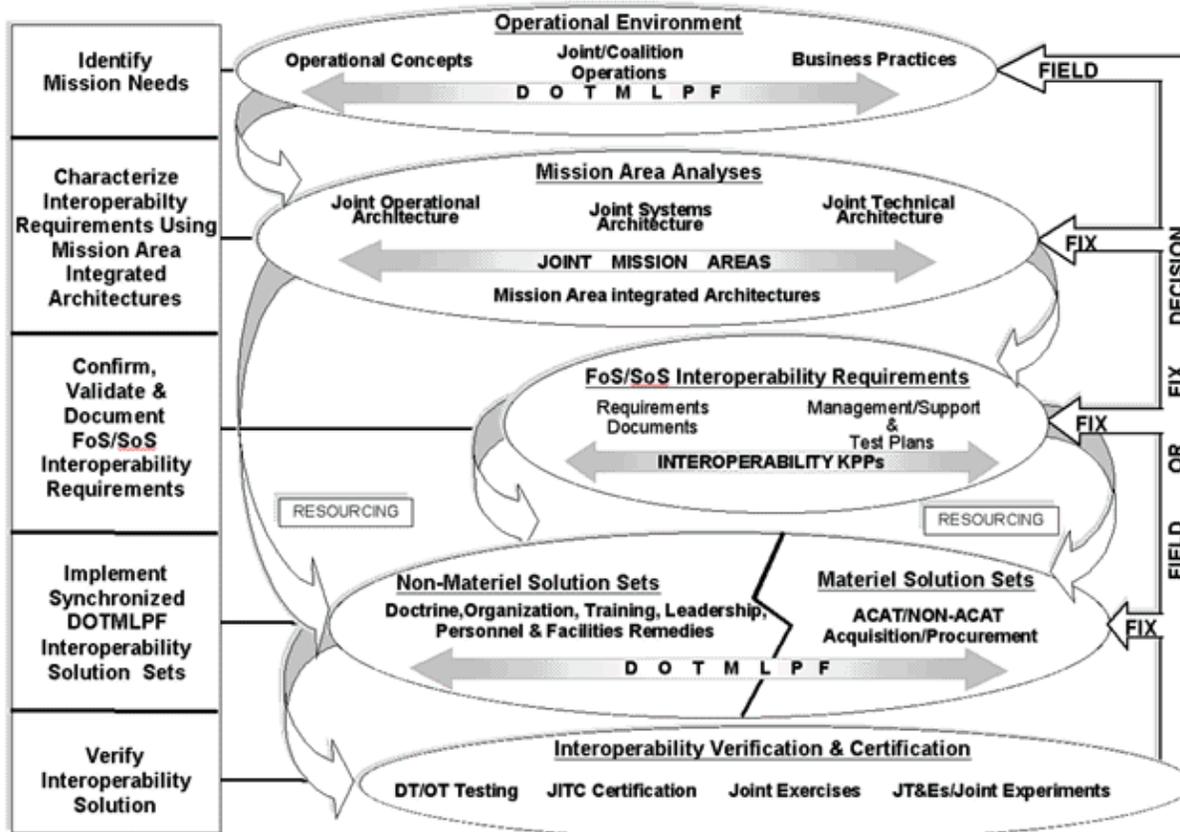
6.1. Mission-Related, Outcome-Based IT and NSS Interoperability Process Overview

6.1.1. Information superiority, a key tenet of Joint Vision 2020, is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. To achieve information 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 level of interoperability between systems shall be determined based on an evaluation of the functional role of the systems within their anticipated FoS/SoS operational environment.

6.1.2. The USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command have developed a strategy that shall serve as the foundation for all DoD IT and NSS interoperability and supportability initiatives. This approach addresses user requirements generation, acquisition and procurement management, and resource allocation processes. Although this process has been developed specifically for FoS/SoS interoperability, the essential elements

may also be used to effectively characterize and evaluate non-IT and NSS (e.g., logistics, munitions, maintenance) interoperability requirements. The following diagram depicts the mission-related, outcome-based process for achieving IT and NSS interoperability and is further discussed in the following paragraphs.

Figure F1. Outcome-Based Interoperability Process



6.1.3. The mission-related, outcome-based approach for achieving IT and NSS interoperability is an iterative process that begins with an assessment of the operational environment to identify mission needs and security services using operational concepts, business practices, experience gained from joint/coalition operations, and evaluation of DOTMLPF aspects. Using mission needs as the foundation, mission area analyses shall evaluate and characterize FoS/SoS interoperability requirements within the context of the JOA, associated JMAs, the JSA, and JTA. The resulting FoS/SoS mission-level architectures are referred to as mission area integrated architectures. These architectures in turn guide determination of individual system interoperability requirements. Solutions to the identified requirements may be materiel or non-materiel solution sets or both. FoS/SoS interoperability requirements shall be documented in applicable requirements documents. System dependencies and

supportability requirements shall be documented in system management or support plans. Regardless of the solution, 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 mission needs, interoperability deficiencies; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities.

6.1.3.2. Characterizes IT and NSS interoperability and supportability requirements in a FoS/SoS mission area context and relates IT and NSS through integrated architectures derived from the JOA and associated JMAs.

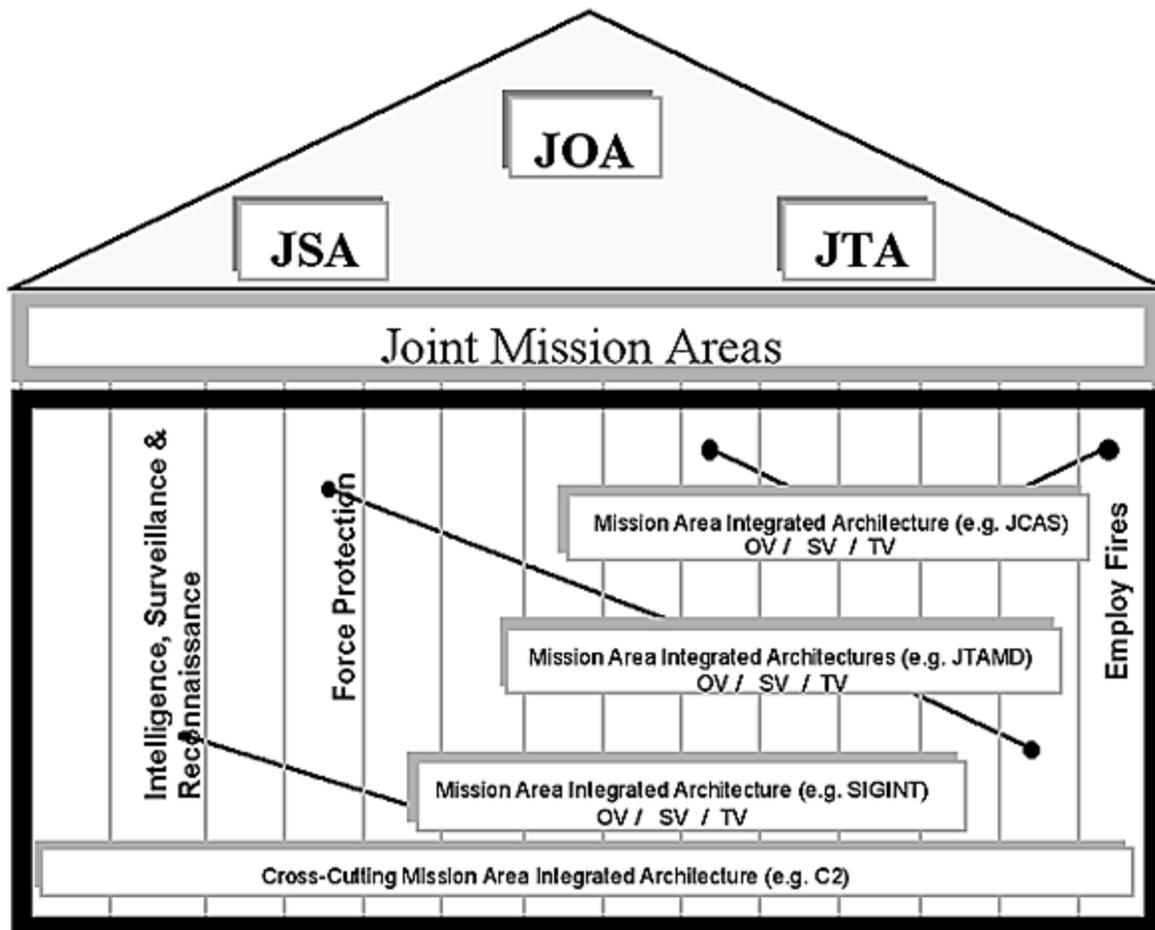
6.1.3.3. Precisely defines operational user requirements to include interoperability as a KPP.

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

6.1.3.5. Verifies solution sets in formal tests or operational exercises.

6.1.3.6. Continuously evaluates interoperability KPPs and verifies overall IT and NSS interoperability throughout a system's life.

6.2. The DoD Joint Integrated Architecture. The operational environment is the aggregate of the threats, forces, physical features, doctrine, concepts of operation, training, materials, leadership, personnel, and facilities with which DoD systems must interact throughout the system's life. Since the nature of the threat and specific missions change with time, the operational environment is dynamic and may be difficult to predict. Nonetheless, based upon evaluation of the operational environment, operational concepts may be developed. The JOA and associated JMAs, the JSA, and JTA are derived from, and will be responsive to, these operational concepts. The diagram below depicts the relationship between the JOA, JSA, JTA, JMAs, and mission area integrated architectures and is further discussed in the following paragraphs.

Figure F2. The DoD Joint Integrated Architecture

6.2.1. Joint Operational Architecture (JOA). The JOA is a description of tasks and activities, operational elements, and information flows required to accomplish or support military operations. It defines types of information exchanged, frequency of exchanged information, which tasks and activities are supported by information exchanges, and the nature of information exchanges in sufficient detail to ascertain specific interoperability requirements. The JOA is intended to represent the entire spectrum of joint operations and has been further subdivided into a set of Joint Mission Areas. The JOA is the encyclopedia of joint operations, with each JMA representing a single volume within that set.

6.2.2. Joint Systems Architecture (JSA). The JSA identifies and describes all DoD systems and their interconnections necessary to accomplish the tasks and activities described in the Joint Operational Architecture.

6.2.3. Joint Technical Architecture (JTA). The JTA defines the interface standards and provides the minimal set of rules governing interdependence of system parts or elements. The JTA defines the service areas, interfaces, and standards (JTA elements) that apply to all DoD IT and NSS.

6.2.4. Joint Mission Areas (JMAs). JMAs serve as JOA cornerstones representing a functional group of joint tasks and activities that share a common purpose and facilitate the operation and interoperability of joint forces. JMAs provide a logical way to organize the JOA and the context for defining those FoS/SoS relationships sharing a common mission area. From the JMAs, the DoD Components shall develop mission area integrated architectures consisting of operational, systems, and technical views of the FoS/SoS architecture. Where appropriate, mission area integrated architectures shall be further codified into CRDs that consider both materiel and non-materiel aspects for fulfilling JMA requirements.

6.2.5. Mission Area Integrated Architectures. Mission area integrated architectures are the common foundation for mission area focused, outcome-based IT and NSS interoperability and supportability processes for ACAT designated acquisitions, non-ACAT acquisitions or procurements, and fielded capabilities.

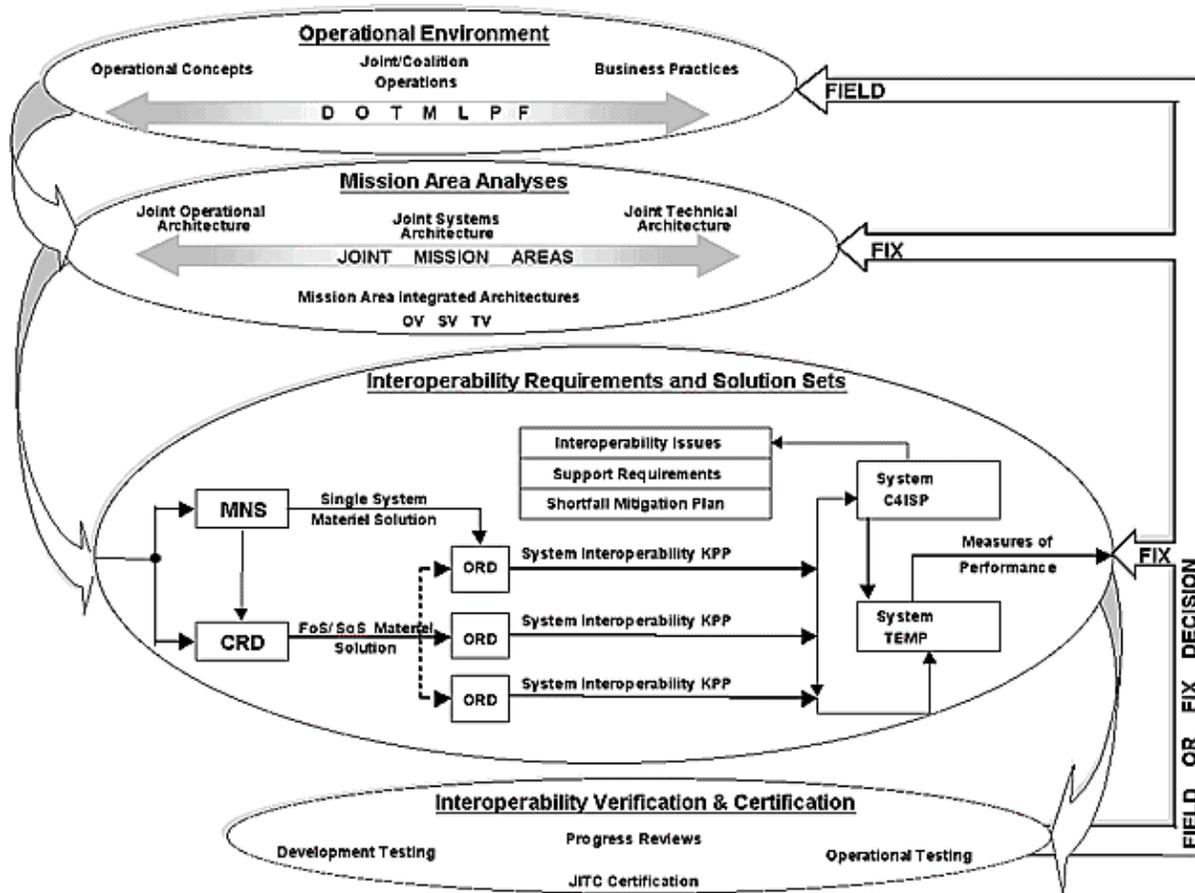
6.2.5.1. DoD Components shall define and relate IT and NSS interoperability requirements using mission area integrated architectures derived from the JOA and associated JMAs, the JSA, and JTA.

6.2.5.2. Integrated architectures include a representation (often graphical) of the IT and NSS processes, systems, and system interfaces. As described in the C4ISR Architecture Framework Document (reference (d)), an integrated architecture is comprised of three views. These views are the Operational View (OV) describing the tasks and activities, operational elements, and information flows required to accomplish or support a military operation; the System View (SV) describing the systems and system interfaces supporting the operational nodes; and the Technical View (TV), which lists the standards and rules governing the interdependence of system parts or elements.

6.2.5.3. When properly depicted for a specified FoS/SoS, the SV should correlate with the associated OV, and the TV should correlate with the associated SV.

6.3. Interoperability Process for ACAT-Designated IT and NSS Acquisitions. The following diagram depicts the mission-related, outcome-based, interoperability and supportability process template for ACAT-designated IT and NSS. Essential elements for requirements and test documentation are described below.

Figure F3. ACAT IT and NSS Acquisition Process



6.3.1. ACAT IT and NSS Acquisition Process Overview

6.3.1.1. The operational environment establishes the mission need for new acquisitions. Mission area integrated architectures define IT and NSS interoperability requirements within a FoS/SoS context for the operational and technical communities. Overall requirements for ACAT-designated acquisition programs are documented in Mission Need Statements (MNSs), Capstone Requirements Documents (CRDs), and Operational Requirements Documents (ORDs). ORDs reflect the results of an Analysis of Alternatives (AoA) conducted in response to a MNS. In those cases where there is no preceding MNS, an ORD shall respond directly to the overarching requirements of all CRDs under which the proposed systems fall. The Chairman of the Joint Chiefs of Staff Requirements Generation Process procedures govern the development of CRD and ORD requirements and interoperability KPPs for ACAT-designated programs. The DoD 5000 series Directives (references (f), (g), and (h)) guide ACAT-designated IT and NSS acquisitions.

6.3.1.2. The AoA, as described in reference (h), 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 MNS. The AoA alternatives shall contain all of the materiel solution sets that satisfy the required interoperability KPPs. Alternatives should be compared to the status quo (existing systems or capabilities). The USD(C) will assess, review and approve the AoA.

6.3.1.3. CRDs and ORDs must contain interoperability KPPs derived from the set of top-level IERs characterizing the information exchanges required by the proposed FoS/SoS. Mission area integrated architectures and associated CRDs shall be used to determine these top-level IERs. The interoperability KPP, along with other KPPs and critical technical and operational issues, shall be referenced when describing and analyzing IT and NSS interoperability in the C4I Support Plan and test strategies in the Test and Evaluation Master Plan (TEMP).

6.3.1.4. IT and NSS interoperability requirements shall drive testing constructs within the program's TEMP and the development of the program's C4I Support Plan.

6.3.1.4.1. The C4I Support Plan shall contain the program's interoperability requirements and corresponding supportability requirements external to the program. The C4I Support Plan 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 C4I Support Plan shall be captured and maintained in an ASD(C3I) database.

6.3.1.4.2. The program's TEMP shall reflect interoperability and supportability requirements, as described in the ORD and C4I Support Plan, 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.

6.3.1.5. DISA shall test, evaluate, and certify all IT and NSS, regardless of ACAT, 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.

6.3.2. Requirements, Acquisition, and Test Documentation

6.3.2.1. Mission Need Statements (MNSs). The Chairman of the Joint Chiefs of Staff Requirements Generation System produces information for decision-makers on the projected mission needs of the warfighter. These mission needs are defined in broad operational terms in a MNS, a non-system specific statement of required operational capability, and are assessed through an AoA against the specified mission need, and subsequently developed into a CRD (for multiple-system materiel solutions) and ORD (ORD alone for single-system materiel solutions). MNSs are prepared for needs that develop into warfighters' operational requirements that may result in new Defense acquisition programs. Validation of a MNS confirms that a non-materiel solution alone cannot satisfy the identified need, and that a potential "new concept/system" materiel system should be considered.

6.3.2.2. Capstone Requirements Documents (CRDs)

6.3.2.2.1. The JROC directs initiation of all CRDs. DoD Components may recommend initiation of a CRD to the JROC during MNS validation. The U.S. Joint Forces Command may recommend initiation of a CRD as an output from joint experimentation. The CRD captures the overarching requirements for a mission area, as derived from mission area integrated architectures, that forms a FoS/SoS (e.g., space control, Theater Missile Defense, etc.). CRDs guide DoD Components in developing mission needs and operational requirements documents for fielded, emerging or new systems. The CRD facilitates development of interoperable and supportable IT and NSS through validated, performance-based, overarching capabilities. Since CRDs define IT and NSS interoperability requirements for mission area integrated architectures, they must reflect the needs of the joint force commander.

6.3.2.2.2. To develop CRDs, the warfighter identifies top-level operational interface requirements for information exchange within a FoS/SoS context. For CRDs, top-level IERs are defined as those information exchanges between systems that make up the FoS/SoS, as well as those that are external to the FoS/SoS (i.e., with other DoD Components, joint, combined or coalition systems). IERs identify the elements of warfighter information supporting a particular activity and between any two activities. IERs are the primary basis and measure for FoS/SoS IT and NSS interoperability KPP threshold and objective requirements for ORDs and CRDs. The focus for the CRD interoperability KPP shall be information exchange and required level of IT and NSS interoperability for the FoS/SoS information needs.

6.3.2.3. Operational Requirements Documents (ORDs)

6.3.2.3.1. The ORD contains operational performance requirements for a proposed concept or system in direct response to a MNS and reflects the preferred alternative resulting from an AoA. Mission area integrated architectures and CRDs provide ORD development guidance through validated, performance-based, overarching capabilities for the mission area that forms a FoS/SoS. ORDs translate the MNS and CRD requirements into detailed, refined performance capabilities and characteristics of the proposed system. ORDs provide the specific requirements base for acquiring and developing programs.

6.3.2.3.2. The ORD interoperability KPP shall focus on information exchanges and the required level of IT and NSS interoperability for system information needs. This allows the warfighter to identify the essential, top-level IERs that reflect both the information needs for the system under consideration and the information this new capability may provide to enhance fielded systems. For ORDs, top-level IERs are those essential interface requirements for information exchange among DoD Component, joint, combined, coalition and other U.S. Government Departments and Agencies needed to support the proposed system. Often these IERs only involve information exchanges with activities external to a proposed system. However, these IERs may also include internal exchanges when the proposed system encompasses multiple-component activities. The ORD interoperability KPP shall define the level of interoperability required for the proposed system. The interoperability KPP shall be derived from IERs identified in the mission area integrated architecture and associated CRD that characterize the information exchanges required by the proposed system. ORDs that come under the umbrella of a CRD should ensure compliance with the CRD KPPs and requirements pertaining to interoperability and supportability.

6.3.2.4. Test and Evaluation Master Plans (TEMPS). DoD Components shall develop TEMPs for all ACAT-designated programs. 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 interoperability KPP, IERs found in the ORD and C4I Support Plan, and operational performance requirements derived from doctrine and Tactics, Techniques, and Procedures (TTPs).

6.3.2.5. C4I Support Plans

6.3.2.5.1. The DoD Components shall develop C4I Support Plans for all ACAT-designated programs. Format, content, and process for the C4I Support Plan provides a mechanism to identify and resolve implementation issues related to IT and NSS infrastructure and support elements. C4I Support Plans shall identify IT and NSS needs, dependencies, and interface requirements, focusing on interoperability, supportability, and sufficiency. The C4I Support Plan shall include: an operational employment concept, system interface descriptions, IERs, IT and NSS support requirements derived from analysis of the system's operational employment concept, potential shortfalls, and proposed solutions. IT and NSS systems' dependencies and interface requirements shall be described in sufficient detail to enable test planning for resolution of the interoperability KPP. The C4I Support Plan enables the DoD Components to conduct IT and NSS supportability reviews for all ACAT designated programs. Reference (h) contains specific C4I Support Plan preparation and review procedures, formats, and timelines.

6.3.2.5.2. The DoD Components shall identify IT and NSS interoperability requirements, infrastructure, and other support requirements early in the acquisition life cycle. DoD Components shall prepare the initial C4I Support Plan prior to acquisition program Milestone B. C4I Support Plans shall be maintained throughout the acquisition life cycle. At each milestone review, C4I Support Plans 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 shortfalls.

6.3.3. IT and NSS Interoperability Verification and Certification

6.3.3.1. Test Documentation. The TEMP's shall state the interoperability KPP for the evaluation of IT and NSS interoperability and shall specify IT and NSS interoperability test concepts. The TEMP's shall reference and extract requirements and critical operational and technical parameters to be tested and evaluated from the appropriate requirements documents, C4I Support Plans, and mission area integrated architectures, as well as doctrine, operational concepts, and TTPs. The Chairman of the Joint Chiefs of Staff shall ensure that all appropriate requirements documents contain specific, testable, and measurable IT and NSS interoperability requirements and KPPs. The USD(AT&L), the ASD(C3I), and the DoD CIO shall ensure that C4I Support Plans and mission area integrated architectures reflect the appropriate FoS/SoS context to support the system's IT and NSS interoperability requirements. The OTAs, the Chairman

of the Joint Chiefs of Staff, and the system's user or program proponent, with DISA and DoD Component interoperability testing organizations, shall develop the IT and NSS interoperability test procedures and effectiveness measures based on the IT and NSS requirements 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 references (g) and (h).

6.3.3.2. Developmental Testing (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 begins. DISA shall provide input to this process to ensure that DT provides sufficient information for standards conformance certifications.

6.3.3.3. 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 concerning the viability of plans and resources to test and evaluate FoS/SoS 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/Critical Design Reviews, DT, and other appropriate sources (e.g., information assurance testing) to produce IT and NSS interoperability assessments.

6.3.3.4. Operational Test Readiness Reviews (OTRRs). All available interoperability assessments (e.g., OAs, DISA 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 DISA also shall provide recommendations regarding IT and NSS readiness for interoperability certification testing. Potentially critical IT and NSS interoperability and supportability problems must be highlighted for assessment during OT&E.

6.3.3.5. Operational Testing (OT). DOT&E and the OTAs shall develop guidelines to assist in evaluating overall IT and NSS interoperability. Operational test plans shall include the IT and NSS interoperability evaluation and supporting measures critical to operational effectiveness. Operational testing 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 DISA 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's IT and NSS interoperability certification.

6.3.3.6. IT and NSS Interoperability Certification Testing

6.3.3.6.1. 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.

6.3.3.6.2. IT and NSS interoperability testing can occur in multiple stages. Therefore, there may be instances when it is important to characterize a system's interoperability before all critical interface requirements have been tested. When appropriate (e.g., between successful completion of operational testing and the fielding decision), DISA shall issue interim interoperability certification letters specifying which of the system's interoperability requirements have been successfully met and which have not. DISA shall issue an overall system certification once the system successfully meets all interoperability KPPs validated by the Chairman of the Joint Chiefs of Staff. DISA shall provide interoperability certification letters to the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command, as well as to the OTA and program manager, as applicable.

6.3.3.6.3. The Chairman of the Joint Chiefs of Staff shall validate that the IT and NSS interoperability KPPs, derived from mission area integrated architectures and the set of top-level IERs approved in the requirement documents and C4I Support Plan are adequately tested and verified. The Chairman of the Joint Chiefs of Staff shall also validate DISA's IT and NSS interoperability test and certification results.

6.3.3.7. Interoperability Reviews. IT and NSS shall be subject to interoperability reviews over the life of a system, FoS, or SoS to determine if interoperability objectives are being met. The DOT&E, the USD(AT&L), the DoD CIO, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command 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 requirements documents; C4I Support Plans; TEMPs and operational test plans; and observation of tests and exercises by the DOT&E and the OTAs, the U.S. Joint Forces Command interoperability priority list, the Joint Warfighting Capability Assessments, program management offices, the MCEB, the Military Intelligence Board (MIB), 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.

6.3.3.8. Interoperability Watch List (IWL)

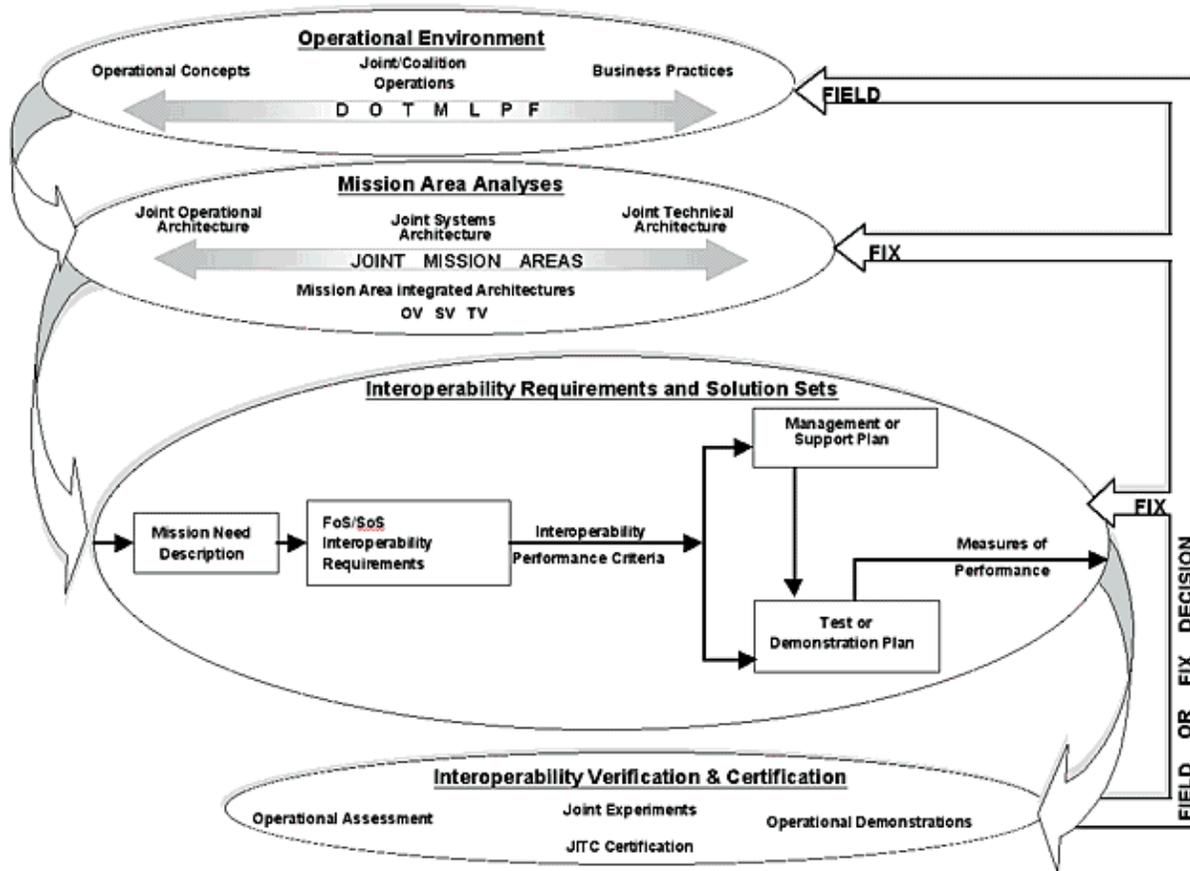
6.3.3.8.1. IT and NSS with significant interoperability deficiencies (as determined by the offices of the USD(AT&L), the DoD CIO, the DOT&E, and the Chairman of the Joint Chiefs of Staff) shall be placed on the IWL to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives. The IWL shall be updated and coordinated quarterly with the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command.

6.3.3.8.2. Program managers (or the operating/sponsoring command), and the responsible test organization (either developmental or operational), with DISA, shall provide periodic updates of current status toward correcting identified IT and NSS interoperability deficiencies for those systems on the IWL to the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command. These updates shall support an assessment by the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command 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).

6.4. Non-ACAT IT and NSS Acquisitions and Procurements Process. The following diagram depicts the mission-related, outcome-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 (f) and (g). Included in this category are all defense technology projects and pre-acquisition demonstrations (e.g., ACTDs, JT&Es, and JWID Gold Nuggets that lead to acquisitions), the CINC Command and Control Initiative Program, CINC 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 F4. Non-ACAT IT and NSS Acquisition and Procurement Process



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

6.4.1.1. 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 (GOTS/NDI) 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 DoD 5000 series policy for acquisitions, which precisely defines requirements, builds to these requirements, and tests against these requirements prior to fielding, 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 becomes an acquisition program, then it shall be managed and fielded per the DoD 5000 series guidance.

6.4.1.2. IT or NSS procured or acquired outside of the ACAT program process shall document requirements according to mission need, identify FoS/SoS interoperability requirements, document dependencies and supportability requirements in a management/support plan, 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 DoD CIO, and the DOT&E shall review, specific DoD Component procedures for non-ACAT acquisitions and procurements.

6.4.2. Non-ACAT Interoperability Requirements and Test Documentation. The paragraphs below describe essential elements required for non-ACAT acquisitions and procurements.

6.4.2.1. Interoperability Requirements Documentation. Interoperability requirements for non-ACAT acquisitions and procurements shall be derived principally from mission area integrated architectures, based on mission need. IT and NSS interoperability shall be documented to a level of detail suitable for deriving FoS/SoS IERs and interoperability KPPs. The scope of the requirements document shall be scaled, as necessary, based on the relative size and funding profile for the program. 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.

6.4.2.2. Management or Support Plans. A management or support plan, analogous to the C4I Support Plan, documenting IT and NSS needs, dependencies, interface requirements, and interoperability KPPs shall be developed for all non-ACAT acquisitions. The plan shall describe FoS/SoS dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability requirements. The management/support plan shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of effectiveness/performance and interoperability shortfalls. The scope of the management/support plan shall be scaled to the relative size and funding profile for the program. The sponsoring or cognizant authority shall review, assess, and

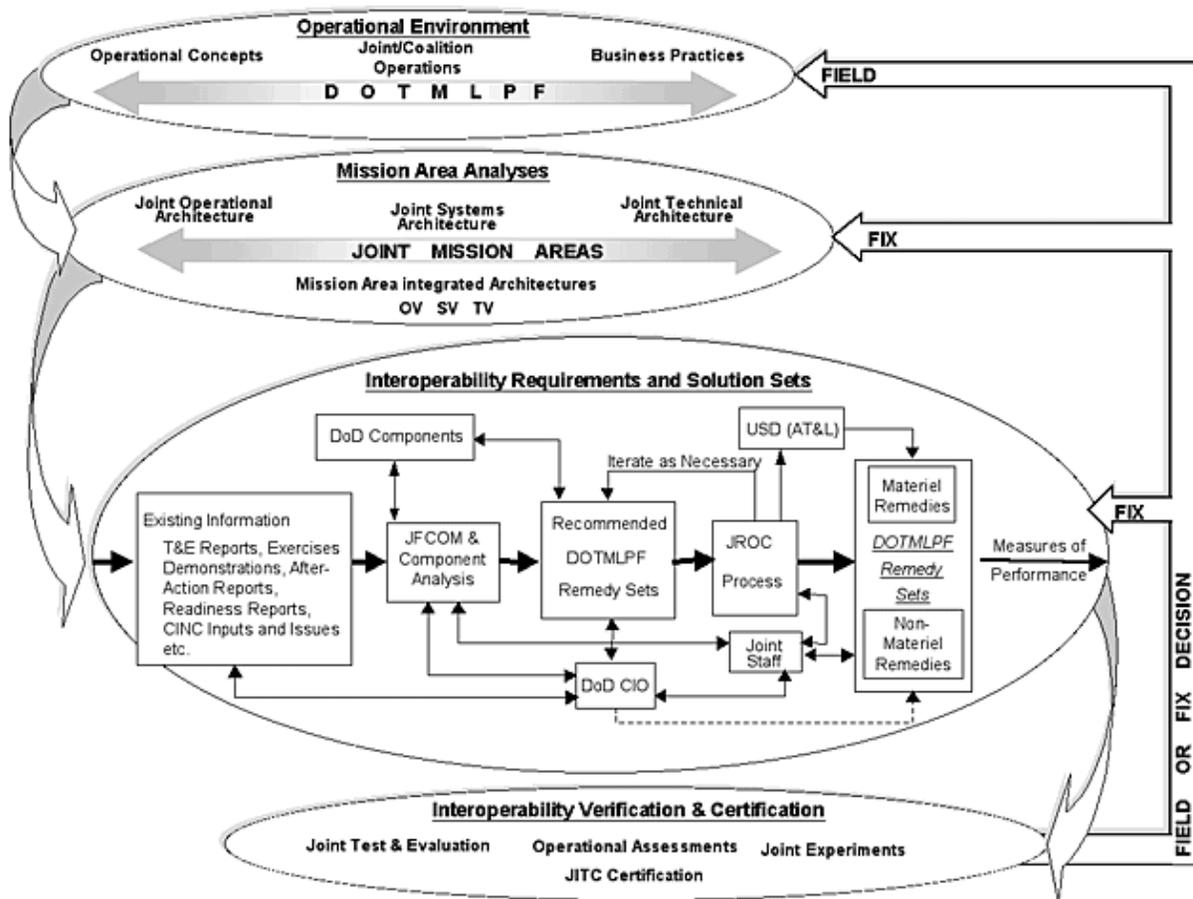
approve the management/support plan and forward any critical interoperability or supportability issues to the DoD CIO for review.

6.4.2.3. 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 will be accomplished and identify measurable, performance-based criteria that will be used to verify overall IT and NSS interoperability and supportability. The scope of test or demonstration plans 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.

6.4.3. 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 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 offices of the USD(AT&L), the DoD CIO, the DOT&E, and the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command) may be placed on the IWL to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

6.5. Fielded IT and NSS Interoperability Process. The following diagram depicts the outcome-based interoperability process for addressing operational warfighting interoperability and supportability issues for fielded IT and NSS.

Figure F5. Fielded (Legacy Systems) IT and NSS Interoperability Process



6.5.1. Fielded IT and NSS Interoperability Process Overview

6.5.1.1. The Unified Command Plan - 99 (UCP-99) assigns the U.S. Joint Forces Command an expanded role as Joint Forces Integrator responsible for combining DoD Component capabilities to enhance interoperability and joint, combined, and coalition capabilities by recommending changes in doctrine, organizations, training and education, materiel, leader development, and personnel. UCP-99 also requires the U.S. Joint Forces Command to support the development and integration of fully interoperable systems and capabilities, including Command, Control, Communications, Computers, and Intelligence, Surveillance, and Reconnaissance (C4ISR) for joint warfighting.

6.5.1.2. The U.S. Joint Forces Command (JI&I) shall identify interoperability and supportability shortfalls for fielded Joint Task Force IT and NSS by assessing the current operational force capability against the requirements and

determining the impact on warfighting readiness. This assessment shall provide the "state of joint force IT and NSS interoperability."

6.5.1.3. The U.S. Joint Forces Command (JI&I), 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 U.S. Joint Forces Command (JI&I) shall document and track these remedy sets.

6.5.1.4. The U.S. Joint Forces Command (JI&I), with the USD(AT&L), the DoD CIO, 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.

6.5.1.5. The USD(AT&L), the DoD CIO, and the DOT&E shall provide policy and oversight for the mission-related, outcome-based interoperability and supportability process; and with the Chairman of the Joint Chiefs of Staff and the U.S. Joint Forces Command, 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.

6.5.2. Fielded IT and NSS Interoperability Shortfalls and DOTMLPF Remedies

6.5.2.1. The U.S. Joint Forces Command (JI&I) shall leverage existing 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 U.S. Joint Forces Command, 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 verification 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 Component and an assessment of the AoA interoperability issues from either the USD(C)/CFO or the responsible CAE to examine the range of materiel and non-materiel solutions.

6.5.2.2. 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 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.emsp; Transition funds shall not be applied to National Foreign Intelligence Program (NFIP)-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 Congress.

6.5.3. Interoperability Verification/Certification. All proposed materiel and non-materiel remedies for fielded IT and NSS capabilities shall be verified by the cognizant authority 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 JITC interoperability testing or other test results, and certify materiel 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 offices of the USD(AT&L), the DoD CIO, the DOT&E, and the Chairman of the Joint Chiefs of Staff) may be placed on the IWL to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

6.6. IT and NSS Standards Development and Prescription

6.6.1. As the DoD CIO's Executive Agent, DISA is responsible for coordinating and integrating all DoD IT and NSS standards activities. DISA shall propose, coordinate among the DoD Components, and promulgate via the JTA, IT, and NSS standards that apply across the Department of Defense.

6.6.2. The DoD JTA improves FoS/SoS interoperability and supportability by identifying IT and NSS standards that facilitate exchange of IT services among systems, units or forces, to operate effectively together. DISA shall coordinate the development and periodically update the DoD JTA to reflect the most current IT and NSS standards adopted for DoD use.

6.6.2.1. JTA 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.

6.6.2.2. The DoD Components' use of JTA-mandated standards must consider the cost, schedule, or performance impacts. If the use of a JTA-mandated

standard will negatively impact cost, schedule, or performance, a DoD CAE or cognizant official may grant a waiver from use. Waivers from JTA use shall not be used to waive Defense Information Systems Network or Defense Enterprise Computing Center usage. Waivers for non-ACAT programs require the concurrence of the DoD CIO/ASD(C3I) and the USD(AT&L). For mission-critical or mission-essential ACAT-designated programs, all granted waivers shall be submitted through the DoD CIO to the USD(AT&L) for review. In either case, concurrence can be assumed if no response is received within 2 weeks of the date of receipt. To ensure proper and timely consideration, all requests for a waiver shall state the cost, schedule, and performance impacts that will occur if the waiver is not granted, and any resulting operational limitations.

6.6.2.3. DISA shall assess whether FoS/SoS components conform to DoD JTA standards and shall regularly report the results to the USD(AT&L), the DoD CIO, the DOT&E, the Chairman of the Joint Chiefs of Staff, and the U.S. Joint Forces Command. The documentation of all standards used in the development of FoS/SoS components is also required for mission area integrated architecture development of technical architecture views.

6.6.2.4. Each DoD Component CAE is responsible for DoD JTA implementation, including compliance, planning, programming, and budgeting.

6.6.3. DISA shall review and assess all DoD Component-approved requirements documents, test plans, and C4I Support Plans 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. 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, DoD AIC, DoD CIO Executive Board, MCEB, or MIB) during the program decision process. The following shall be considered during this assessment:

6.6.3.1. 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.

6.6.3.2. Standards implementation for Communications Security (COMSEC), especially in cases of combined interoperability, shall be carefully considered.

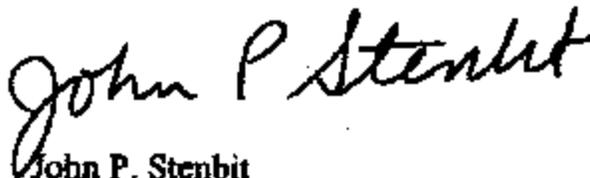
6.6.3.3. Adherence to U.S. Federal and DoD standards, U.S.-ratified NATO STANAGS, and other international standards accepted for U.S. use.

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 5.9.5, DoD Component C4I Support Plans required by subparagraph 6.3.2.5., and the periodic updates to the DoD IWL are exempt from licensing according to paragraph C4.4.2 of DoD 8910.1-M (reference (o)).

8. EFFECTIVE DATE

This Instruction is effective immediately.



John P. Stenbit

**Assistant Secretary of Defense for Command,
Control, Communications and Intelligence**

Enclosures - 3

- E1. References, continued
- E2. Definitions
- E3. Acronyms

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Section 133 of title 10, United States Code
- (f) [DoD Directive 5000.1](#), "The Defense Acquisition System," January 4, 2001
- (g) [DoD Instruction 5000.2](#), "Operation of the Defense Acquisition System," October 23, 2000
- (h) [DoD Regulation 5000.2-R](#), "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," June 10, 2001
- (i) [DoD Directive 4650.1](#), "Management and Use of the Radio Frequency Spectrum," June 24, 1987
- (j) National Security Telecommunications and Information System Security Policy (NSTISSP) No. 8, "National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments," February 13, 1997
- (k) National Security Telecommunications and Information System Security Policy (NSTISSP) No. 11, "National Information Assurance Acquisition Policy," January 2000
- (l) [DoD Instruction 5200.40](#), "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
- (m) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (n) Sections 2223 and 2224 of title 10, United States Code
- (o) [DoD 8910.1-M](#), "DoD Procedures for Management of Information Requirements," June 30, 1998

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. DoD 5000.2-R, Part 1, (reference (h)) 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 need described in the requirements 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. C4I Support Plan. A mechanism to identify and resolve implementation issues related to an acquisition program's C4ISR infrastructure support and IT and NSS interface requirements. It identifies IT and NSS needs, dependencies, and interfaces for programs in all acquisition categories, focusing attention on interoperability, supportability, and sufficiency concerns.

E2.1.7. Capstone Requirements Document (CRD). A document that contains capabilities-based requirements that facilitate and guide the development of individual ORDs by providing a common framework and operational concept. It is an oversight tool for overarching requirements for a system-of-systems or family-of-systems.

E2.1.8. Certification (Certify). A formal statement of adequacy provided by a responsible Agency attesting that a system has met its interoperability and supportability requirements.

E2.1.9. Common Operating Environment (COE). The COE establishes an 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.

E2.1.10. Conformance Testing. Testing the extent to which a system or subsystem adheres to or implements a standard.

E2.1.11. Defense Agencies. All agencies and offices of the Department of Defense, including the Ballistic Missile Defense Organization, 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 Imagery and Mapping Agency, National Reconnaissance Office, and National Security Agency.

E2.1.12. 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 within the Department of Defense.

E2.1.13. DoD 5000 Series. Refers collectively to DoD Directive 5000.1, DoD Instruction 5000.2, and DoD 5000.2-R.

E2.1.14. Electromagnetic Environmental Effects (E3). 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.

E2.1.15. 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.

E2.1.16. Family-of-Systems (FoS). A set or arrangement of independent systems that can be interconnected or related in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities that depend on the situation.

E2.1.17. 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.

E2.1.18. Information Exchange Requirements (IERS). The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as why the information is necessary, and how it will be used.

E2.1.19. Information Superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

E2.1.20. Information Systems Security (INFOSEC). The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, against the denial of service to authorized users, or against the provision of service to unauthorized users. It includes those measures necessary to detect, document, and counter such threats.

E2.1.21. 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 Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS).

E2.1.22. Information Technology Architecture (ITA). An integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the Agency's strategic goals and information resources management goals.

E2.1.23. Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, systems view, and technical view) that facilitates integration and promotes interoperability across FoS/SoS and compatibility among related mission area architectures.

E2.1.23.1. The operational architecture view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a warfighting function.

E2.1.23.2. The systems architecture view is a description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions.

E2.1.23.3. The technical architecture view 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.

E2.1.24. 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.

E2.1.25. Joint Mission Areas (JMAs). JMAs represent a functional group of joint tasks and activities that share a common purpose and facilitate joint force operation and interoperability. JMAs provide a logical way to organize the JOA and provide the context for defining FoS/SoS relationships sharing a common mission area.

E2.1.26. Joint Operational Architecture (JOA). Description of tasks and activities, operational elements, and information flows required to accomplish or support military operations; defines the types and frequency of information exchanged, which tasks and activities are supported by information exchanges, and nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

E2.1.27. Joint Systems Architecture (JSA). The identification and description of all DoD systems and their interconnections necessary to accomplish the tasks and activities described in the Joint Operational Architecture.

E2.1.28. Joint Technical Architecture (JTA). The JTA consists of 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. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems, and its adoption is mandated for the management, development, and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense.

E2.1.29. Key Performance Parameter (KPP). Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet a KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a Capstone Requirements Document KPP threshold can be the cause for the FoS/SoS concept to be reassessed or the contributions of the individual systems to be reassessed.

E2.1.30. Materiel Solution. Correction of a deficiency, satisfaction of a need, 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.

E2.1.31. Milestones. Major decision points that separate the phases of an acquisition program.

E2.1.32. Milestone Decision Authority (MDA). The individual designated according to criteria established by the USD(AT&L) or by the ASD(C3I) for IT and NSS acquisition programs to approve entry of an acquisition program into the next phase.

E2.1.33. Military Department. A DoD Component headed by a civilian Secretary that the President appoints, including a Military Service (e.g., the Department of the Navy includes two Services).

E2.1.34. Mission Area Integrated Architectures. Mission area integrated architectures are the common foundation for mission area focused, outcome-based IT

and NSS interoperability and supportability processes. Mission area integrated architectures (consisting of operational, systems, and technical views) are derived from JMAs (i.e., subordinate/supporting missions to the JMAs) and/or business/administrative mission areas. Mission area integrated architectures can cover organizational entities (e.g., Joint Task Force, Navy Battle Group or Army Brigade). The Joint Operational Architecture (JOA), the Joint Systems Architecture (JSA), and the Joint Technical Architecture (JTA) serve as the basis for developing mission area integrated architectures.

E2.1.35. Mission Critical Information System (MCIS). A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act (reference (c)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission critical should be made by a Component Head, a CINC or their designee.) A Mission Critical Information Technology System has the same meaning as a Mission Critical Information System.

E2.1.36. Mission Essential Information System (MEIS). A system that meets the definition of "information system" in the Clinger-Cohen Act (reference (c)), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission critical should be made by a Component Head, a CINC or their designee.)

E2.1.37. 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.

E2.1.38. Mission Need Statement (MNS). A formatted non-system-specific statement, written in broad operational terms, that describes operational capability needs, required operational capabilities, and constraints to be studied during the Concept Exploration and Definition Phase.

E2.1.39. National Security System (NSS). Any telecommunications or information system operated by the United States Government, the function, operation, or use of which:

E2.1.39.1. Involves intelligence activities.

E2.1.39.2. Involves cryptologic activities related to national security.

E2.1.39.3. Involves command and control of military forces.

E2.1.39.4. Involves equipment that is an integral part of a weapon or weapons system.

E2.1.39.5. 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).

E2.1.40. Non-Materiel Solution. Changes in doctrine, organization, training, leadership, personnel or facilities that satisfies identified mission needs.

E2.1.41. Operational Concept. An end-to-end stream of activities that defines how force elements, systems, organizations, and tactics combine to accomplish a military task.

E2.1.42. Operational Requirements. A system capability or characteristic required to accomplish approved mission needs. Operational (including supportability) requirements are typically performance parameters, but they may also be derived from cost and schedule. For each parameter, an objective and threshold value must also be established.

E2.1.43. Operational Requirements Document (ORD). A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or users representative at each milestone beginning with Milestone A.

E2.1.44. Outcome-Based Interoperability. An interoperability process that:

E2.1.44.1. Includes experts from the operational community to identify, consolidate, and prioritize mission needs and interoperability deficiencies; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities.

E2.1.44.2. Characterizes IT and NSS interoperability requirements in a family-of-systems or system-of-systems mission area context and relates IT and NSS through integrated architectures derived from the Joint Operational Architecture and associated Joint Mission Areas.

E2.1.44.3. Precisely defines operational user requirements to include interoperability as a Key Performance Parameter.

E2.1.44.4. Incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organizational, training, leadership, personnel, or facilities) solutions.

E2.1.44.5. Verifies solutions sets in formal tests or operational exercises.

E2.1.44.6. Continuously evaluates interoperability Key Performance Parameters and verifies overall IT and NSS interoperability throughout a system's life.

E2.1.45. Oversight. Senior executive-level review of programs to ensure compliance with policy and attainment of broad program goals.

E2.1.46. Requirement. The need of an operational user initially expressed in broad operational capability terms in the format of a MNS. It progressively evolves to system-specific performance requirements in the ORD.

E2.1.47. Signals Intelligence (SIGINT). A category of intelligence comprising, either individually or in combination, all Communications Intelligence (COMINT), Electronics Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).

E2.1.48. Spectrum Supportability. The assurance that the necessary frequencies and bandwidth are available to military systems in order to maintain effective interoperability in the operational electromagnetic environment. It includes spectrum certification, host nation coordination, frequency assignment, and electromagnetic compatibility.

E2.1.49. Standards Compliance. Confirmation that IT and NSS has undergone standards testing and exhibits a specified degree of standards conformity.

E2.1.50. Standards Conformance Certification. Confirmation by DISA that an IT and NSS has undergone information technology standards testing and exhibits IT standard base implementation. IT standards include standards for information processing, information content (such as standard data definitions), information formats, and information transfer.

E2.1.51. Supportability. The ability of existing and planned IT, including NSS, systems and infrastructure components to aid, protect, complement, and sustain development or operation of the system being acquired.

E2.1.52. System-of-Systems (SoS). A set or arrangement of systems that are related or connected to provide a given capability. The loss of any part of the system degrades the performance or capabilities of the whole.

E2.1.53. System Standards Profile. A system-specific list of all technical standards and guidelines for their use. To meet IT and NSS interoperability requirements, the system standards profile should be built from applicable standards drawn from the DoD Joint Technical Architecture.

E2.54. Tactical SIGINT System. All SIGINT systems developed for use by U.S. Forces.

E2.1.55. Test and Evaluation (T&E). 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.

E2.1.56. Universal Reference Resource (URR). Reference models and information standards that serve as sources for guidelines and attributes that must be consulted while building integrated architecture products. The following are the currently listed URRs: DoD Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework; C4ISR Core Architecture Data Model; Defense Data Dictionary, Levels of Information Systems Interoperability; Universal Joint Task List; Joint Operational Architecture; Technical Reference Model; Defense Information Infrastructure Common Operating Environment; Shared Data Environment; and the DoD Joint Technical Architecture.

E2.1.57. Validation. An authoritative act or process of supporting or corroborating whether IT and NSS interoperability and supportability requirements are appropriate.

E2.1.58. Verification. The act of establishing whether IT and NSS interoperability requirements are accurate, measurable, supportable, and adequately reflected in a system or family of systems' acquisition strategy, test and evaluation plan, or in non-materiel or non-traditional acquisition IT and NSS interoperability plans.

E3. ENCLOSURE 3

ACRONYMS

E3.1.1. <u>ACAT</u>	Acquisition Category
E3.1.2. <u>AIC</u>	Architecture Implementation Council
E3.1.3. <u>ACTD</u>	Advanced Concept Technology Demonstration
E3.1.4. <u>ASD(C3I)</u>	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
E3.1.5. <u>ATD</u>	Advanced Technology Demonstration
E3.1.6. <u>C3I</u>	Command, Control, Communications, and Intelligence
E3.1.7. <u>C4</u>	Command, Control, Communications, and Computers
E3.1.8. <u>C4I</u>	Command, Control, Communications, Computers, and Intelligence
E3.1.9. <u>CAE</u>	Component Acquisition Executive
E3.1.10. <u>C4ISR</u>	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
E3.1.11. <u>CINCs</u>	Commander in Chiefs
E3.1.12. <u>CIO</u>	Chief Information Officer
E3.1.13. <u>CM</u>	Configuration Management
E3.1.14. <u>COE</u>	Common Operating Environment
E3.1.15. <u>COMINT</u>	Communications Intelligence
E3.1.16. <u>COMSEC</u>	Communications Security
E3.1.17. <u>COTS</u>	Commercial-Off-the-Shelf
E3.1.18. <u>CRD</u>	Capstone Requirements Document
E3.1.19. <u>DAB</u>	Defense Acquisition Board
E3.1.20. <u>DAR</u>	DoD Architecture Repository
E3.1.21. <u>DoD CIO</u>	Department of Defense Chief Information Officer
E3.1.22. <u>DIA</u>	Defense Intelligence Agency
E3.1.23. <u>DII</u>	Defense Information Infrastructure
E3.1.24. <u>DISA</u>	Defense Information Systems Agency
E3.1.25. <u>DoD</u>	Department of Defense
E3.1.26. <u>DoD CFO</u>	DoD Chief Financial Officer
E3.1.27. <u>DoD CIO</u>	DoD Chief Information Officer
E3.1.28. <u>DoDIIS</u>	Department of Defense Intelligence Information Systems
E3.1.29. <u>DOT&E</u>	Director Operational Test & Evaluation
E3.1.30. <u>DOTMLPF</u>	Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities
E3.1.31. <u>DSPO</u>	Defense Standardization Program Office
E3.1.32. <u>DT</u>	Developmental Testing
E3.1.33. <u>ELINT</u>	Electronics Intelligence
E3.1.34. <u>E3</u>	Electromagnetic Environmental Effects
E3.1.35. <u>FISINT</u>	Foreign Instrumentation Signals Intelligence
E3.1.36. <u>FoS</u>	Family of Systems
E3.1.37. <u>GOTS/NDI</u>	Government-Off-the-Shelf/Non-Developmental Items

E3.1.38. <u>IA</u>	Information Assurance
E3.1.39. <u>IC CIO</u>	Intelligence Community Chief Information Officer
E3.1.40. <u>IER</u>	Information Exchange Requirement
E3.1.41. <u>INFOSEC</u>	Information Security
E3.1.42. <u>ISRP</u>	Interoperability Senior Review Panel
E3.1.43. <u>IT</u>	Information Technology
E3.1.44. <u>ITA</u>	Information Technology Architecture
E3.1.45. <u>IWL</u>	Interoperability Watch List
E3.1.46. <u>JCAS</u>	Joint Close Air Support
E3.1.47. <u>JI&I</u>	Joint Interoperability and Integration
E3.1.48. <u>JMA</u>	Joint Mission Area
E3.1.49. <u>JOA</u>	Joint Operational Architecture
E3.1.50. <u>JROC</u>	Joint Requirements Oversight Council
E3.1.51. <u>JSA</u>	Joint Systems Architecture
E3.1.52. <u>JTA</u>	Joint Technical Architecture
E3.1.53. <u>JTADG</u>	JTA Development Group
E3.1.54. <u>JTAMD</u>	Joint Theater Air Missile Defense
E3.1.55. <u>JT&E</u>	Joint Test and Evaluation
E3.1.56. <u>JWID</u>	Joint Warfighter Interoperability Demonstration
E3.1.57. <u>KPP</u>	Key Performance Parameter
E3.1.58. <u>MAIS</u>	Major Automated Information System
E3.1.59. <u>MCEB</u>	Military Communications-Electronics Board
E3.1.60. <u>MCIS</u>	Mission Critical Information System
E3.1.61. <u>MDA</u>	Milestone Decision Authority
E3.1.62. <u>MDAP</u>	Milestone Defense Acquisition Program
E3.1.63. <u>MEIS</u>	Mission Essential Information System
E3.1.64. <u>MIB</u>	Military Intelligence Board
E3.1.65. <u>MNS</u>	Mission Need Statement
E3.1.66. <u>NATO</u>	North Atlantic Treaty Organization
E3.1.67. <u>NFIP</u>	National Foreign Intelligence Program
E3.1.68. <u>NSA</u>	National Security Agency
E3.1.69. <u>NSS</u>	National Security System
E3.1.70. <u>OA</u>	Operational Assessment
E3.1.71. <u>ORD</u>	Operational Requirements Document
E3.1.72. <u>OSD</u>	Office of the Secretary of Defense
E3.1.73. <u>OT</u>	Operational Testing
E3.1.74. <u>OTA</u>	Operational Test Authority
E3.1.75. <u>OT&E</u>	Operational Test and Evaluation
E3.1.76. <u>OTRR</u>	Operational Test Readiness Review

E3.1.77. <u>PM</u>	Program Manager
E3.1.78. <u>POM</u>	Program Objective Memorandum
E3.1.79. <u>PSA</u>	Principal Staff Assistant
E3.1.80. <u>SoS</u>	System of Systems
E3.1.81. <u>SIGINT</u>	Signals Intelligence
E3.1.82. <u>STANAG</u>	Standardization Agreement (NATO)
E3.1.83. <u>STAR</u>	System Threat Assessment Report
E3.1.84. <u>TEMP</u>	Test and Evaluation Master Plan
E3.1.85. <u>T&E</u>	Test and Evaluation
E3.1.86. <u>USD(AT&L)</u>	Under Secretary of Defense for Acquisition, Technology, and Logistics
E3.1.87. <u>USCINCFCOM</u>	Commander-in-Chief, U.S. Joint Forces Command
E3.1.88. <u>USD(C)</u>	Under Secretary of Defense (Comptroller)
E3.1.89. <u>USIGS</u>	U.S. Imagery and Geospatial Service
E3.1.90. <u>USSOCOM</u>	U.S. Special Operations Command