October 17, 2002

Acquisition

Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems
(D-2003-011)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
17 Oct 2002	N/A	-

Title and Subtitle Acquisition: Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Report Number** D-2003-011
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 100	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
CRD	Capstone Requirements Document
DISA	Defense Information Systems Agency
GIG	Global Information Grid
JCPAT	Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool
JITC	Joint Interoperability Test Command
KPP	Key Performance Parameter
ORD	Operational Requirements Document
TEMP	Test and Evaluation Master Plan
USJFCOM	U.S. Joint Forces Command

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

October 17, 2002

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
COMMANDER, U.S. JOINT FORCES COMMAND
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, JOINT STAFF
CO-CHAIR, INTEROPERABILITY SENIOR REVIEW PANEL

SUBJECT: Report on the Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems (Report No. D-2003-011)

We are providing this report for review and comment. This report is the first in a series of reports that discuss the overall implementation of interoperability and information assurance policies for the acquisition of DoD systems. This report addresses the implementation of those policies within the Office of the Secretary of Defense and the Defense agencies. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. As a result of management comments, we revised Recommendations 1., 3.a., and 4.b. We redirected Recommendations 1., 2., 3.a., 3.b., 4.a. and 4.b. to clarify our intention and request comments on how management plans to implement the recommendations. Therefore, we request that the Co-Chair, Interoperability Senior Review Panel provide comments by December 16, 2002.

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. John E. Meling at (703) 604-9091 (DSN 664-9091) (jmeling@dodig.osd.mil) or Mr. Jack D. Snider at (703) 604-9087 (DSN 664-9087) (jsnider@dodig.osd.mil). See Appendix J for the report distribution. The team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2003-011 **October 17, 2002**
(Project No. D2002AE-0009)

Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems

Executive Summary

Who Should Read This Report and Why? Policy makers, milestone decision makers, combat and materiel developers, and testers responsible for interoperability and information assurance requirements of DoD weapon systems should be interested in this report. This report addresses the importance of adhering to DoD interoperability and information assurance policies to reduce the risk of DoD weapon systems not being interoperable and able to exchange information in a secure manner with other DoD and allied systems.

Background. This report is the first in a series of reports on the implementation of interoperability and information assurance policies for the acquisition of DoD weapon systems. Other reports in the series will address how effectively the Army, Navy, Air Force, and Unified Commands implement those policies. Interoperability and information assurance policies include the Joint Vision 2020 and the Global Information Grid capstone requirement document.

Results. The Department faces a difficult challenge in achieving interoperability between DoD systems and needs congruent and effective mechanisms to measure and oversee its progress. Without consistent guidance that makes combat and materiel developers analyze programs using an operational architecture view, the DoD is at risk of developing systems that operate independently of other systems and of not fully realizing the benefits of interoperable DoD systems to satisfy the needs of the warfighter as outlined in Joint Vision 2020. Implementing a process that timely integrates revisions for interoperability and information assurance policies into the applicable DoD and Chairman of the Joint Chiefs of Staff interoperability and information assurance policies; establishing criteria and procedures for placing DoD systems on the Interoperability Watch List; comparing the operational requirements documents (ORDs) of proposed DoD systems against the other ORDs in the related mission area architecture; updating the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool (JCPAT) database and controlling user access; and defining and implementing a plan to test critical operational issues for DoD systems in the Global Information Grid should better enable DoD to implement interoperability and information assurance policies. (See the Finding section of this report for the detailed recommendations.)

Management Comments and Audit Response. We received comments from the Director, Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Director, Architecture and Interoperability, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C3I]); the Inspector General, Office of the Commander, U.S. Joint

Forces Command (USJFCOM); the Director, Operational Test and Evaluation; the Inspector General, Defense Information Systems Agency (DISA); the Director, Joint Staff; and the Co-Chair, Interoperability Senior Review Panel.*

The Director, Interoperability neither concurred nor nonconcurred with the recommendation concerning timely revisions of interoperability and information assurance policies; however, he suggested revisions to the recommendation, which we made. The Director, Architecture and Interoperability concurred with the recommendation concerning timely revisions of interoperability and information assurance policies and neither concurred nor nonconcurred with the recommendation concerning the implementation of the Interoperability Watch List. The Inspector General, USJFCOM stated that USJFCOM neither concurred nor nonconcurred with the recommendation concerning the comparison of ORDs; however, he suggested revisions to the recommendation, which we made. The Inspector General added that the USJFCOM is currently not funded or resourced to perform the in-depth review of the ORD, as recommended. The Director, Operational Test and Evaluation partially concurred with the recommendations concerning the implementation of the Interoperability Watch List and the testing of critical operational issues. The Director, Joint Staff concurred with the report, subject to the incorporation of his comments on the recommendations concerning interoperability and information assurance policies, the Interoperability Watch List, and limiting JCPAT access. The Director also stated that the DoD is not effectively structured to effect the organizing, training, and equipping of joint capabilities. Further, he stated that a joint process was not established to delineate who is responsible and accountable for developing and acquiring joint command and control systems and integrating capabilities. The Co-Chair, Interoperability Senior Review Panel agreed with the need for timely revisions of interoperability and information assurance policies, the implementation of the Interoperability Watch List, the comparison of ORDs, the use of qualification analysis and predictive tools, and the testing of critical operational issues. Further, the Co-Chair supported the position of the Joint Staff regarding the JCPAT. (See the Finding section of this report for a discussion of the management comments and the Management Comments section of the report for the complete text of the comments.)

Because we received varied comments from the senior leadership of the Interoperability Senior Review Panel to the recommendations, often without a coordinated corrective action plan, we redirected those recommendations to the Co-Chair, Interoperability Senior Review Panel and request that he comment on how the Panel will implement a process that timely integrates revisions for interoperability and information assurance policies; will establish a clearly defined process and criteria for the Interoperability Watch List; will employ a process and resources, including quantification analysis and predictive tools, to compare the ORDs of proposed DoD systems against the other ORDs in the related mission area architecture; will update or archive JCPAT documents; and will limit JCPAT access. Therefore, we request that the Co-Chair, Interoperability Senior Review Panel provide comments on this final report by December 16, 2002.

*The Interoperability Senior Review Panel is composed of senior leaders from the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C^3I); the Joint Staff; the USJFCOM; the Director for Programs, Analysis, and Evaluation; and the Director, Operational Test and Evaluation.

Table of Contents

Background

This report is the first in a series of reports on the implementation of interoperability and information assurance policies for the acquisition of DoD weapon systems. This report addresses the implementation of those policies by the Office of the Secretary of Defense and Defense agencies, the interoperability requirements process, and the oversight thereof. Subsequent reports will discuss the adequacy of interoperability key performance parameters (KPPs) and the interoperability certification process for DoD systems, including national security systems in the Army, Navy, Air Force, and unified combatant commands. Appendix B provides definitions of technical terms used in this report.

Chairman of the Joint Chiefs of Staff Testimony on the President's Proposed Defense Program for FYs 2003 to 2007. On February 5, 2002, General Myers, the Chairman of the Joint Chiefs of Staff, testified before the U.S. Senate Committee on Armed Services on interoperability. General Myers described how Navy, Air Force, and Marine Corps systems shared information to execute combat operations in Afghanistan. He testified that:

> To fulfill our range of commitments and protect our global interests, we must make the investments necessary to maintain the quality of our force while preparing for future challenges of the 21st century. The best means of accomplishing these goals, in my mind, are to, one, improve our joint war-fighting capabilities, and two, to transform the armed forces of America into a 21st century force.

General Myers further testified that DoD should conceive, design, and produce new systems with joint warfighting requirements in mind. DoD needs to view new systems as interchangeable modules that can be used in any situation and in any command arrangement. General Myers believed the area with the greatest potential is in command, control, communications, computers, intelligence, surveillance and reconnaissance.

Quadrennial Defense Review. On September 2001, the Quadrennial Defense Review report stated that achieving the objectives of the defense strategy requires the transformation of the U.S. Armed Forces. Two of the six critical operational goals for the DoD transformational efforts relate to information assurance and interoperability.

- Assuring that, in the face of attack, information systems conduct effective information operations.

- Leveraging information technology and innovative concepts to develop interoperable, joint command, control, communications, computers, intelligence, surveillance, and reconnaissance architectures and capability that includes a tailorable joint operational picture.

Additionally, as stated in the Quadrennial Defense Review report,

> To support joint and combined command and control and to enable a common relevant operational picture of the battlespace, the Department will enhance end-to-end interoperable communications for secure planning and operations. These communications will provide shared situational awareness and integration of joint fires, maneuver, and intelligence. They must be interoperable across all components and tailorable for coalition operations with other countries.

Joint Vision 2020. On May 30, 2000, the Chairman of the Joint Chiefs of Staff signed Joint Vision 2020, which addressed the concept, design, and production of systems with joint warfighting requirements. Joint Vision 2020 describes in broad terms a future joint force whose operational capabilities will be required to succeed across the full range of military operations and accomplish missions in the year 2020 and beyond. Joint Vision 2020 states that interoperability is a mandate for the future joint force especially for communications, common logistics items, and information sharing. Information systems and equipment that enable a common, relevant operational picture must work from shared networks that can be accessed by any appropriately cleared participant. As an example, Appendix C details the action plan that the Director for Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics is planning to execute for command and control systems.

Another tenet of Joint Vision 2020 is to attain information superiority. Information superiority gets the right information to the right people, at the right time, and in the right format, resulting in a vastly improved shared understanding of the situation. Joint Vision 2020 emphasizes the following information superiority goals:

- implement effective programming for establishing information assurance and critical infrastructure protection, and

- build a coherent Global Information Grid (GIG).

Global Information Grid. In November 1999, the Joint Chiefs of Staff assigned the Commander, U.S. Joint Forces Command (USJFCOM) the task of preparing the capstone requirements document (CRD) for the GIG. On August 30, 2001, the Joint Requirements Oversight Council approved the CRD, which describes the overarching information capability requirements for a globally interconnected, end-to-end, interoperable, and secured system-of-systems that would support the Secretary of Defense, warfighters, DoD personnel, the intelligence community, policy makers, and non-DoD users at all levels involved in military and nonmilitary operations. Appendix D provides a detailed description of the GIG.

Common Interoperable and Secure Systems. To attain Joint Vision 2020 and GIG compliance and reduce the risk of building stand-alone or "stovepipe" systems, the Defense agencies and the Military Departments are required to develop and retrofit DoD systems into common interoperable and secure systems. Information assurance is required to protect, defend, and ensure the

availability of information and information systems. Interoperability is required to provide the ability of systems to exchange data effectively. Together, information assurance and interoperability comprise the basis for achieving network centric warfare, information superiority, decision superiority, and full spectrum dominance, as defined in Joint Vision 2020. The DoD faces a complex challenge in achieving an effective coexistence between interoperability and information assurance within the context of Joint Vision 2020 and the GIG. Appendix E shows the multiple factors affecting the implementation of interoperability requirements in the weapon system development process.

Objectives

The primary audit objective was to evaluate whether the Office of the Secretary of Defense and the Defense agencies were effectively implementing DoD interoperability and information assurance policies. Subsequent reports will discuss the adequacy of interoperability KPPs and the interoperability certification process for DoD systems, including national security systems in the Army, Navy, Air Force, and unified combatant commands. See Appendix A for a discussion of the audit scope and methodology, and prior coverage related to the audit objectives.

Adequacy of the Interoperability and Information Assurance Process

The Department faces a difficult challenge in achieving interoperability between DoD systems and needs congruent and effective mechanisms to measure and oversee its progress. The Department did not have fundamental mechanisms that are consistently applied or established because:

- The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C3I]) had interoperability policies in the 1992 version of DoD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems," that were inconsistent with Chairman of the Joint Chiefs of Staff Instruction 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology Systems," May 8, 2000. During the audit, on May 2, 2002, DoD updated DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),"[1] to rectify the policy implementation inconsistencies in the earlier version.

- The Commander, USJFCOM did not analyze interoperability and information assurance requirements in the operational and system architectures for DoD systems as part of the interoperability certification process[2] for operational requirements documents (ORDs).[3]

- The Director, Command, Control, Communications, and Computers Systems Directorate (J-6) (the Joint Staff J-6) had not updated the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool (JCPAT) database to include all interoperability certifications; Test and Evaluation Master Plans (TEMPs); and Command, Control, Communications, Computers, and Intelligence (C4I) support plans for DoD systems.

[1]Title of instruction changed as a result of the update.

[2]Two interoperability certifications exist; the first for requirements and supportability documents and the second for interoperability certification testing. The Chairman of the Joint Chiefs of Staff (J-6) and the Joint Interoperability Test Command are responsible for requirements and supportability document certification and for interoperability certification testing, respectively.

[3]The updated DoD Instruction 4630.8 assigned USJFCOM with the responsibility to collect, consolidate, and prioritize the information technology and national security systems' interoperability and supportability requirements for emerging and fielded Joint Task Force systems using input from Defense agencies and Military Departments.

- The Chairman of the Joint Chiefs of Staff; the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); and the Commander, U.S. Joint Forces Command, in coordination with the Director, Operational Test and Evaluation, had not established criteria for the Defense agencies and the Military Departments to place DoD systems on the Interoperability Watch List.

- The Director, Operational Test and Evaluation had not completed a plan to include testing of critical operational issues addressing interoperability and information assurance in the Global Information Grid.

Without consistent guidance that makes combat and materiel developers analyze programs using an operational architecture view, the DoD is at risk of developing systems that operate independently of other systems and of not fully realizing the benefits of interoperable DoD systems to satisfy the needs of the warfighter as outlined in Joint Vision 2020. However, the recent DoD revisions of policies in achieving transformation through interoperability may have consolidated some fragmented activities.

Interoperability and Information Assurance Policies

The following provides an overview of DoD and Joint Staff policies concerning interoperability and information assurance. Appendix F provides a detailed discussion of the policy.

Interoperability Policy. The DoD and Joint Staff established policy guidance concerning interoperability during the requirements and acquisition processes.

DoD Policy. The policy requires that joint, combined, coalition, and interagency missions must be supported through interoperable information technology and national security systems in global operations across the peace-conflict spectrum. All information technology and national security systems for U.S. Forces use are to be considered for use by joint, allied, and other U.S. Government departments and agencies. Information technology and national security systems' interoperability and supportability requirements are to be identified through the mission area integrated architectures. Interoperability requirements are required to be managed, evaluated, and reported throughout the life of the system. All DoD acquisition category programs will use a C4I Support Plan to document interoperability requirements. Additionally, interoperability and supportability requirements are required to be balanced with the need for information assurance.

Joint Staff Policy. The policy states that interoperability KPPs in an ORD define the level of interoperability for the proposed system and that ORDs must be certified before each milestone, regardless of acquisition category, for conformance with joint national security systems and interoperability standards.

Failure to meet a KPP can be cause for the system to be reevaluated or the program to be reassessed or terminated. In addition, USJFCOM is to provide comments to the Joint Staff J-6 on interoperability issues for all acquisition category programs to ensure that each ORD contains information exchange requirements and operational views. Combatant commanders,[4] Military Departments, and DoD agencies are to incorporate interoperability testing into their overall testing plans in coordination with DISA and the Joint Interoperability Test Command (JITC). Further, JITC is to certify test results for all interoperability system tests. The Joint Staff J-6 issues an interoperability system validation memorandum based on the testing reports from the JITC.

Information Assurance Policy. The DoD and Joint Staff established policy guidance concerning information assurance during the acquisition process.

DoD Policy. The policy established the DoD Information Technology Security Certification and Accreditation Process (the Process) for security certification and accreditation of unclassified and classified information technology. The Process sets forth the activities and management structure to certify and accredit information technology systems that will maintain the security posture of the Defense Information Infrastructure. Further, the Director, Operational Test and Evaluation is not to approve test plans unless they contain a well-defined strategy for addressing information assurance concerns.

Joint Staff Policy. The policy states that information assurance is required for all DoD systems that are used to enter, process, store, display, or transmit DoD information, regardless of classification or sensitivity. Information assurance requirements are to be codeveloped and coevolved with those for information interoperability. The policy also states that information assurance is critical to the military's ability to conduct warfare and is the responsibility of all modern warfighters; a risk assumed by one organization, at any organization level, can be a risk imposed on all organizations. Therefore, the requirement for implementing information assurance applies at all DoD organization levels. Further, information assurance for DoD information systems and networks requires a strategy that integrates the capabilities of people, operations, and technology to ensure survivability and mission accomplishment.

Evaluation of Interoperability and Information Assurance Policy

The ASD(C3I) had interoperability policies that were inconsistent with those of the Chairman of the Joint Chiefs of Staff. Appendix F identifies the interoperability and information assurance policies that the Defense agencies and the Military Departments must implement. Appendix G provides a flow chart of the interoperability requirements review process for DoD weapon systems.

[4]Formerly commanders-in-chief.

Inconsistent Policy. DoD had issued at least six separate policy documents for interoperability and at least three separate policy documents for information assurance because DoD dispersed authority for interoperability and information assurance policy to various organizations within the Office of the Secretary of Defense. Specifically, directorates in the offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Director, Operational Test and Evaluation; and the Joint Staff had established interoperability and information assurance policies and instructions that apply to DoD. The DoD interoperability and information assurance policies and instructions describe processes for reviewing system interoperability requirements during the requirement generation stage and require that the interoperability of system architectures be tested to ensure that information technology and national security systems communicate.

During the audit, ASD(C3I) updated DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" and DoD Instruction 4630.8 on January 11 and May 2, 2002, respectively, because the outdated DoD Directive and Instruction had not been updated for 10 years. Both updated policies canceled the previous versions signed in 1992. Updates in 2002 to the DoD Instruction resolved the inconsistencies and synchronized policies and instructions for the first time.

Information Assurance Policy. The level of information assurance controls varied throughout the DoD because no standard methodology existed to measure the progress of information assurance, and no DoD-wide information security plan was implemented to protect and defend the DoD systems and networks, according to prior Inspector General of the Department of Defense reviews. The Inspector General of the Department of Defense in Report No. D-2001-182, "Information Assurance Challenges," stated that until DoD implements a consolidated policy approach to information assurance and fully incorporates information assurance requirements into its ongoing architectural efforts, security policies and procedures will continue to be fragmented, and DoD Components will continue to provide varied and inconsistent levels of information assurance. Consolidating information assurance policy would eliminate the need to keep all other DoD information assurance policies updated. We will review specific requirements in upcoming audits, as discussed in Appendix A, "Other Matters of Interest."

Revisions to Guidance. When the Chairman of the Joint Chiefs of Staff revised interoperability policies, those revisions were not immediately reflected in DoD Instruction 4630.8. However, during this audit, DoD updated the policies to reduce inconsistent attributes that would confuse those who will be required to implement interoperability and information assurance policies. Furthermore, the Office of the Secretary of Defense, in conjunction with the Chairman of the Joint Chiefs of Staff, should implement a process that timely updates all interoperability and information assurance policies when interoperability or information assurance policy revisions occur.

Interoperability Requirements

Public Law. Section 922, Public Law 105-261, "Strom Thurmond National Defense Authorization Act for Fiscal Year 1999," expressed the sense of Congress concerning joint warfighting experimentation. In that provision, Congress discussed the designation of a commander of a combatant command to have the mission of joint warfighting experimentation, as a key step in exploiting advanced technologies, new organizational structures and new joint operational concepts to transform the conduct of military operations by the U.S. Armed Forces. Congress also expressed its sense that such a commander should be provided with appropriate and sufficient resources for joint warfighting experimentation and listed the responsibilities and authorities that should accompany that designation, including improving interoperability; reducing unnecessary redundancy; synchronizing technology fielding; and making recommendations to the Chairman of the Joint Chiefs of Staff on mission needs statements and operational requirements documents. Section 485, title 10, United States Code, was added by section 923 of Public Law 105-261 to provide for an annual reporting requirement from the combatant commander to the Secretary, and then to the Congress, on the joint experimentation efforts for each preceding fiscal year.

Comparison of ORDs to Joint Mission Architectures. The DoD designated the Commander, USJFCOM as the DoD Joint Force Integrator.[5] However, the USJFCOM did not compare ORDs to joint mission architectures before system development started. This condition occurred because the USJFCOM, although responsible for conducting interoperability analysis, was not assessing the interoperability requirements within a joint mission architecture and because it did not have the necessary analytical or quantitative modeling and simulation tools. In comments to the report, ASD(C3I) stated that the Joint Staff must refine the joint mission architectures and the subordinate mission areas before USJFCOM can conduct an effective comparative analysis of operational requirements.

Interoperability Analysis. Chairman of the Joint Chiefs of Staff Instruction 6212.01B requires the USJFCOM to provide comments to the Joint Staff J-6 on interoperability issues for all acquisition category programs so that each ORD contains interoperability KPPs and information exchange requirements. However, the USJFCOM did not analyze the ORD requirements of a proposed DoD system within the context of ORD requirements of other systems with which a proposed DoD system must interoperate and exchange information. Instead of analyzing the ORDs that the system will interoperate with, the USJFCOM stated that it reviews ORDs within the context of CRDs and measures interoperability and integration requirements against ORDs that

[5]DoD Instruction 4630.8 states that the USJFCOM, in an expanded role as the DoD Joint Force Integrator, is responsible for enhancing interoperability and joint, combined, and coalition capabilities by recommending changes in doctrine, organizations, training and education, materiel, leader development, and personnel.

relate to CRDs and against other known DoD systems outside the CRDs. The updated DoD Instruction 4630.8 assigns the USJFCOM with the responsibility to collect, consolidate, and prioritize the information technology and national security systems interoperability and supportability requirements for emerging and fielded Joint Task Force systems using input from Defense agencies and Military Departments. Additionally, the Instruction requires that USJFCOM participate in the requirements validation process for information technology and national security systems by reviewing and confirming that the interoperability information exchange requirements and KPPs are sufficient for requirements documents. This assessment is based on the warfighter's perspective using joint mission area integrated architectures.

Interoperability Review Assessment. To provide interoperability comments, USJFCOM subject-matter experts analyze ORD requirements against qualitative criteria established in Joint Staff policy after receiving the ORD from the Joint Staff J-6. However, the subject-matter experts do not compare the proposed system ORD against the ORDs of the systems it must be interoperable with, even if required, because they do not have the necessary analytical or quantitative modeling and simulation tools to determine whether the ORD is appropriate for the operational or systems architecture. As a result, the subject-matter experts consider a system interoperable if the ORD contains interoperability information exchange requirements and KPPs, but they do not determine whether the proposed DoD system's requirements are interoperable with other systems in their intended mission architectures. Therefore, the subject-matter experts conduct only a stand-alone qualitative assessment of the ORD. The updated DoD Instruction 4630.8 requires that the development of mission area integrated architectures be consistent with the products required by the C4I Surveillance and Reconnaissance Architecture Framework. The ASD(C3I) stated that the updated DoD Instruction 4630.8, combined with guidance in the DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," April 5, 2002, that requires working level integrated product teams to develop ORDs and C4I support plans, will assist the USJFCOM in the ORD analysis.

Tools. Modeling, simulations, or relationship databases may provide USJFCOM with the means to synchronize interoperability requirements before beginning system developmental work. Matching ORD interoperability and information assurance requirements at the beginning is necessary for later specifications, standards, and interfaces to be written in acquisition document plans. Without conducting upfront interoperability requirements analysis of individual systems in mission architectures, DoD may be at greater risk of developing systems that do not communicate with each other. The Automated Commander-in-Chief Integrated System Tool (the Tool) is a DoD initiative under development that could assist the USJFCOM in evaluating interoperability requirements in proposed ORDs during the review process. The Tool is an automated process intended to enable combat developers to build testable and measurable requirements, develop joint information exchange requirements, identify operational architectures, and build system architectures based on operational needs. The Tool could be a mechanism to provide a single,

integrated, and coherent view of interoperability requirements for the Joint Staff, the Military Departments, and the combatant commands. Accordingly, the USJFCOM could use the Tool or similar mechanism to review the ORD for interoperability requirements within the context of mission architectures. However, all Defense agencies and Military Departments would have to agree to use the Tool or a similar tool as the standard format for requirements sent to USJFCOM.

Tracking Requirements. The Joint Staff J-6 did not have an updated Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool (JCPAT) database to maintain interoperability certifications, TEMPs, C4I support plans, and approved ORDs for DoD systems. Further, after users were granted access to the JCPAT, they had unlimited read access to all information, which raises concerns about the need to know.

Maintenance of the Database. In May 1999, the Joint Staff established the JCPAT on the Secret Internet Protocol Router Network for DoD organizations to use for tracking and staffing comments while reviewing the requirements during the interoperability certification process, as required in the Chairman of the Joint Chiefs of Staff Instruction 6212.01B. The Joint Staff J-6 relies on the DISA to maintain up-to-date documents that contain interoperability and information assurance requirements for DoD systems. The documents maintained include ORDs, CRDs, C4I support plans, and TEMPs. As a result, the JCPAT is a historical database that lists all DoD systems undergoing interoperability requirements certification or that have been certified for interoperability. Further, the JCPAT contains comments made on DoD systems about interoperability concerns.

When searching for interoperability certified documents in the JCPAT, a user could not be assured that the document located was the most recently certified document. More importantly, the Defense agencies and Military Departments did not forward approved documents, such as the ORD, CRDs, C4I support plans, or TEMP, for inclusion in the JCPAT database. The final approved documents were not consistently maintained in the JCPAT because the Joint Staff J-6 depends on the Joint Requirements Oversight Council and milestone decision authorities to execute the requirement for Stage Three in the requirement certification process.[6] Therefore, the DISA and the USJFCOM cannot compare new proposed ORDs to approved ORDs to provide meaningful comments to the Joint Staff J-6 on the proposed ORDs.

For the JCPAT to be useful, final versions of the documents must be submitted and included in the JCPAT. Further, outdated versions of documents should be archived so that users can locate and obtain the most up-to-date approved documents for making interoperability determinations for DoD systems.

[6]The Chairman of the Joint Chiefs of Staff Instruction 6212.01B requires posting the document into the JCPAT within 15 days after the Joint Requirements Oversight Council or the milestone decision authority approves the mission need statement, CRD, or ORD.

Access to Database. Appendix H identifies 50 DoD organizations that have access to the JCPAT. In those 50 DoD organizations, 756 users were given access to the JCPAT through a secure network. DISA identified 756 total users; however, it could not designate whether those users were DoD or contractor personnel. As a result, contractors have read-only access to program documentation for which they may not have a need to know.

Oversight of Significant Interoperability Deficiencies

Interoperability Watch List. DoD policy on the Interoperability Watch List (Watch List) did not define a significant interoperability deficiency that would cause the Office of the Secretary of Defense, the Joint Staff, the Defense agencies, and the Military Departments to place a DoD system on the Watch List.

Policy. DoD Regulation 5000.2-R states that all major DoD acquisition programs, programs on the Office of the Secretary of Defense Test and Evaluation Oversight list, legacy systems, and all programs and systems that must interoperate with them are subject to interoperability evaluations throughout their life cycles to validate their ability to support mission accomplishment. At their discretion, the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Director, Operational Test and Evaluation; and the Joint Staff (the four signatories) decide, based on the Interoperability Senior Review Panel's[7] recommendations, to place programs and systems deemed to have significant interoperability deficiencies on the Watch List. DoD systems are to remain on the Watch List until program managers take corrective actions to address identified interoperability deficiencies. The Interoperability Senior Review Panel is required to prepare quarterly reports summarizing the activities of DoD systems and programs on the Watch List.

Inclusion of DoD Systems with Significant Interoperability Deficiencies on the Watch List. Although the policy applies to all programs and systems, as of July 2002, no programs had been or are on the Watch List.[8] Further, the Interoperability Senior Review Panel did not prepare any quarterly reports that addressed DoD systems with interoperability testing concerns during FY 2001.

[7]The Interoperability Senior Review Panel is composed of senior leaders from the Offices of the Under Secretary of Defense for Acquisition Technology and Logistics; the ASD(C^3I); the Joint Staff; the USJFCOM; the Director for Programs, Analysis, and Evaluation; and the Director, Operational Test and Evaluation.

[8]The Director, Operational Test and Evaluation stated that the original intent was for organizations, such as the Military Communication and Electronics Board, the USJFCOM, and others, to identify DoD systems for the Watch List. The Interoperability Senior Review Panel has discussed criteria. One criteria is the overall impact the lack of interoperability has on a mission area. The Interoperability Senior Review Panel has considered the U.S. Air Force Situational Awareness Date Link as a candidate for placement on the Watch List; however, the Interoperability Senior Review Panel has been unable to reach consensus on the placing the Situational Awareness Date Link on the Watch List.

However, the Director, Operational Test and Evaluation cited interoperability testing concerns for 21 DoD systems in the FY 2001 Annual Test Report to Congress, as shown in the following table.

Programs with Interoperability Deficiencies in the FY 2001 Annual Test Report

Military Department	Number of DoD Systems
Army	8
Navy	7
Air Force	5
Other DoD	1
Total	**21**[9]

The Director, Operational Test and Evaluation stated that identifying interoperability deficiencies in the FY 2001 Annual Report is a positive sign that DoD policies are working and that program managers are now obligated to address the Director, Operational Test and Evaluation concerns before progressing with development and production. Furthermore, the Director, Operational Test and Evaluation stated that many of the systems shown in the table will be tested and validated over a series of already scheduled test events outlined in the applicable system's TEMP. However, some of the programs were not mature enough in development to address interoperability issues, while other systems were having to "catch up" to recent policies, because the policies were not in existence in the system's early development phase.

DoD Regulation 5000.2-R states that DoD systems that have a significant interoperability deficiency may be added to the Watch List. Because the phrase significant interoperability deficiency is ambiguous, a more concise definition is required to determine when a DoD system should be added to the Watch List. The Interoperability Senior Review Panel could use the requirements in DoD Regulation 5000.2-R on interoperability and information assurance as

[9]Of the 21 programs, 9 are Acquisition Category I, 8 are Acquisition Category II, and 4 are Acquisition Category III. Those programs are on the Director, Operational Test and Evaluation's Oversight Watch List. The Director, Operational Test and Evaluation stated that, because those programs were on the Oversight Watch List, many of the system level issues would be resolved at the milestone decision reviews. However, he stated that the concern was with the systems not on the Oversight Watch List, such as Acquisition Category III and IV systems, transitioning advanced concept technology demonstrations, and fielded legacy systems.

criteria for determining inclusion of systems on the Watch List. DoD Regulation 5000.2-R requires that DoD system program offices have:

- an interoperability certification from the Joint Staff J-6,
- approval of the C4I support plan and information assurance strategy from the chief information officer,
- verification that the program manager used the Joint Technical Architecture standards and guidelines in system development, and
- an approved Systems Security Authorization Agreement.

By actively using the Watch List, the DoD would have a method of ensuring compliance with the interoperability and information assurance based on DoD Regulation 5000.2-R requirements. The updated DoD Instruction 4630.8 reinforces the establishment of the Watch List.[10] However, the revised instruction does not state specific criteria for systems to be included on the Watch List. The phrase "critical for mission effectiveness" allows a broad interpretation.

Measuring Progress. DoD Regulation 5000.2-R states that when a DoD system is placed on the Watch List, the program office is to provide periodic updates of current status towards correcting identified deficiencies to the Interoperability Senior Review Panel. The program manager, or other cognizant official, and the responsible test organization, in conjunction with JITC, provide those updates. Those updates support an assessment as to whether interoperability issues are being adequately addressed, and whether a status change is warranted; specifically, whether the program or system should be removed from the Watch List, kept on the Watch List, or proposed for test and evaluation oversight. Staff members of the Interoperability Senior Review Panel are to conduct quarterly reviews to determine the program manager's progress towards addressing identified interoperability deficiencies.

To strengthen the review process for measuring corrective actions to mitigate the deficiencies, program office corrective actions taken on Acquisition Category I programs and less than Acquisition Category I programs on the Watch List should be discussed in the Defense Acquisition Executive Summary reporting process and during program reviews, respectively.

Defense Acquisition Executive Summary. DoD Regulation 5000.2-R states that the Defense Acquisition Executive Summary is a multi-part document, which reports program information and assessments; program

[10]DoD Instruction 4630.8 requires that the Director, Operational Test and Evaluation establish, in conjunction with the Under Secretary of Defense for Acquisition, Technology, and Logistics; the DoD Chief Information Officer; the Chairman of the Joint Chiefs of Staff; and the USJFCOM, an Interoperability Watch List to provide DoD oversight for those systems that interoperability is deemed critical to mission effectiveness, but is not being adequately addressed. Systems considered for the Interoperability Watch List may be preacquisition systems, acquisition programs (any acquisition category), already fielded systems, or combatant command-unique procurements.

manager, program executive officer, and Component acquisition executive comments; and cost and funding data primarily for Acquisition Category I programs. The Defense Acquisition Executive Summary is an early warning report to the Under Secretary of Defense for Acquisition, Technology, and Logistics and the ASD(C3I), which describes actual program problems, warns of potential program problems, and describes mitigating actions taken. At a minimum, the Defense Acquisition Executive Summary reports program assessments, including interoperability, unit costs, and current estimates, and the status of exit criteria and vulnerability assessments. The Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); Director, Operational Test and Evaluation; the Cost Analysis Improvement Group in the Office of the Secretary of Defense; the Component acquisition executives; and the program executive officers review or assess the Defense Acquisition Executive Summary reports. During those reviews or assessments, we believe those groups should determine whether the program has:

- shown significant interoperability deficiencies,
- been placed on the Watch List, and
- made progress towards correcting the significant interoperability deficiencies to be removed from the Watch List.

By reviewing significant interoperability deficiencies during the review process, the Defense Acquisition Executive Summary review groups may have focused additional attention on the nine Acquisition Category I programs that have interoperability testing concerns in the FY 2001 Annual Test Report to Congress.

Program Reviews. At milestone and appropriate program reviews, the milestone decision authority should be focusing additional attention on programs that are on the Watch List to determine whether the program offices are making satisfactory progress towards correcting significant interoperability deficiencies.

Testing Interoperability and Information Assurance Requirements in the Global Information Grid

On March 31, 2000, the Deputy Secretary of Defense directed the Director, Operational Test and Evaluation to include critical operational issues addressing interoperability and information assurance in the GIG operational test and evaluation.

The GIG is not one system, but an end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communication and computing systems, services, software, data, security services, national security systems, and associated services necessary to achieve

Information Superiority. In this regard, the Director, Operational Test and Evaluation plans to eventually create a joint network to simulate the GIG consisting of equipment at Military Department test facilities.[11] That simulated network would show how DoD systems will communicate in a joint and allied environment. However, the Director, Operational Test and Evaluation had not formalized a plan that discusses the required resources needed to construct the network.

Military Departments, system designers, and system testers need to coordinate their resources to adequately test interoperability and information assurance among DoD systems in the GIG and determine their mission capability in a joint environment. System testers design operational tests around critical operational issues that are derived from operational requirements in the ORD. However, the GIG is based on many DoD systems that work together as an architecture of a mission area. Therefore, testing of interoperability and information assurance in individual DoD systems that are part of the GIG must be included as critical operational issues so that testers will fully test the operational effectiveness and suitability of the individual systems as they operate in the GIG. The Director, Operational Test and Evaluation stated that the challenge is to identify the appropriate architecture and the ability to execute a test that takes into account the scope of that architecture.

Conclusion

Without consistent guidance that makes combat and materiel developers analyze programs using an operational architecture view, the DoD is at risk of developing systems that operate independently of other systems and of not fully realizing the benefits of interoperable DoD systems to satisfy the needs of the warfighter as outlined in Joint Vision 2020. DoD interoperability and information assurance requirements must become more streamlined and easier to implement. Further, information assurance must be implemented appropriately and commensurate to the level of interoperability required to avoid fielding DoD systems that do not ensure the availability, integrity, authenticity, confidentiality, and nonrepudiation of information. To achieve this objective, combat developers[12] must have the capability to conduct analyses of operational requirements at the beginning of a system to determine the interoperability and information assurance effects of new and legacy systems on mission area architectures.[13] Without this capability, the combat developers cannot determine which systems need to operate together and whether those systems will be suitable for the warfighter.

[11]DoD has funded the development of the Joint Distributed Engineering Plant to coordinate resources for testing. The Director, Operational Test and Evaluation stated that, as the Joint Distributed Engineering Plant matures, he will use it for integration testing to provide that larger environment represented by the GIG.

[12]A combat developer is the command or agency that formulates doctrine, concepts, organization makeup, materiel requirements, and objectives. Generically, it represents the user community role in the materiel acquisition process.

[13]The ASD(C^3I), the Director, Operational Test and Evaluation, and the USJFCOM stated that the Chairman of the Joint Chiefs of Staff completing joint mission area architectures is critical to achieving interoperability.

Management Comments on the Finding and Audit Response

Summaries of management comments on the finding and audit responses are in Appendix I.

Recommendations, Management Comments, and Audit Response

Redirected and Revised Recommendations. In response to most of the recommendations, we received varied management comments to the same recommendation, often without a coordinated corrective action plan. Therefore, to collectively resolve the recommendations and to obtain succinct and attainable corrective action, we are redirecting Recommendations 1., 2., 3.a., 3.b., 4.a., and 4.b. to the Co-Chair, Interoperability Senior Review Panel, which consists of senior leaders from the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Joint Staff; the USJFCOM; the Director for Programs, Analysis, and Evaluation; and the Director, Operational Test and Evaluation. Further, in response to comments by the Director, Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Inspector General, USJFCOM; and the Director, Joint Staff, we revised Recommendations 1., 3.a., and 4.b., respectively, so that:

- the revision process for interoperability and information assurance policies will be jointly implemented instead of coordinated among the applicable organizations;
- the Commander, USJFCOM will compare the ORDs of proposed DoD systems with joint mission area architectures, as they are completed, against the ORDs in the related joint mission area architecture to verify the completeness of stated interoperability requirements; and
- JCPAT access will be limited to users who have a need to know.

1. We recommend that the Co-Chair, Interoperability Senior Review Panel, in concert with the applicable membership of the Interoperability Senior Review Panel, implement a process that timely integrates revisions for interoperability and information assurance policies into the applicable DoD and Chairman of the Joint Chiefs of Staff interoperability and information assurance policies.

Director, Architecture and Interoperability, Office of the ASD(C3I), Comments. The Director concurred, stating that his office will work with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Joint Staff to implement a process for timely revision and

synchronization of DoD interoperability and information assurance policies. Further, the Director stated that the Interoperability Senior Review Panel will be used to:

- coordinate the annual review and synchronization and review, if required, for the following policies and implementing instructions that affect interoperability: DoD Directive 4630.5; DoD Instruction 4630.8; Chairman of the Joint Chiefs of Staff Instruction 3170.01B, "Requirements Generation System," April 15, 2001; and Chairman of the Joint Chiefs of Staff Instruction 6212.01B; and

- ensure consistency of those policies and implementing instructions with the 5000 series policy documents for acquisition; DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997; and Chairman of the Joint Chiefs of Staff Instruction 6510.01C, "Information Assurance and Computer Network Defense," May 1, 2001.

For the complete text of the Director's comments, see the Management Comments section of the report.

Director, Joint Staff Comments. The Director concurred, subject to the inclusion of his comments, and suggested adding the following to the recommendation:

> We also recommend the implementation of a process which addresses, funds, and implements aspects of joint battle management command and control interoperability and connectively; validation and/or allocation of resources to acquire Joint systems and create offices supporting integration of materiel and non-materiel solutions for broad mission capability areas.

The Director stated that he made the suggestion because the report did not address the issue that DoD was not effectively structured to organize, train, and equip joint capabilities. Further, he stated that a joint process was not established to delineate who is responsible and accountable for developing and acquiring joint command and control systems and integrating capabilities. For the complete text of the Director's comments, see the Management Comments section of the report.

Director, Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Comments. The Director neither concurred nor nonconcurred; however, he stated that the wording "in coordination with" could be construed to give the ASD(C3I) primacy over the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Joint Staff in integrating revisions to all documents related to interoperability. Further, he stated that each of those organizations is responsible for one or more of those documents. Therefore, the Director recommended that the phase "in coordination with" be changed to "jointly with" or that the first four lines be

rewritten to read, "We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Chairman of the Joint Chiefs of Staff jointly implement…." For the complete text of the Director's comments, see the Management Comments section of the report.

Co-Chair, Interoperability Senior Review Panel Comments. The Co-Chair agreed, stating that the Interoperability Senior Review Panel will work with the Joint Staff to implement a process for timely revision and synchronization of DoD policies regarding interoperability and information assurance. In addition, he provided comments similar to those made by the Director, Architecture and Interoperability, Office of the ASD(C3I). For the complete text of the Co-Chair's comments, see the Management Comments section of the report.

Audit Response. The comments by the Director, Architecture and Interoperability, Office of the ASD(C3I); and the Director, Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics were responsive. In response to the Director, Interoperability, we revised the recommendation as suggested. Further, the suggestion by the Director, Joint Staff concerning the issue of organizing, training, and equipping joint capabilities was outside the audit scope.

Because the respondents have not yet established a process for timely revision and synchronization of DoD policies regarding interoperability and information assurance, we redirected the recommendation to the Co-Chair, Interoperability Senior Review Panel, whose membership consists of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Joint Staff; the USJFCOM; the Director for Programs, Analysis, and Evaluation; and the Director, Operational Test and Evaluation, and request that the Co-Chair provide additional comments on how and when the Interoperability Senior Review Panel will establish a timely revision and synchronization process.

2. We recommend that the Co-Chair, Interoperability Senior Review Panel, in concert with the applicable membership of the Interoperability Senior Review Panel, define the term significant interoperability deficiency, and establish criteria and procedures for placing a DoD system with a significant interoperability deficiency on the Interoperability Watch List.

Director, Joint Staff Comments. The Director concurred, subject to the inclusion of his comments, and suggested adding the following subparagraphs to the recommendation:

> a. Develop Joint Mission Area Architectures based on currently available DoD assets and based on those assets needed to provide the capabilities for the future.
>
> b. Provide an analysis branch within each JMA [Joint Mission Area] to assess Requirement Document relevance against known architecture needs.

c. Develop compliant, certified, and standard analysis and predictive tools, such as models or simulations, to assist in verifying the completeness of stated interoperability requirements in mission area architectures.

Director, Architecture and Interoperability, Office of the ASD(C3I), Comments. The Director neither concurred nor nonconcurred; however, he stated that his office is working with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Director, Operational Test and Evaluation; and the Joint Staff to develop procedures for addressing interoperability deficiencies within existing processes. Further, he stated that his office will continue to work with the Interoperability Senior Review Panel to refine the process for identifying programs with interoperability deficiencies and for nominating those programs as candidates for the Interoperability Watch List. The Director stated that, because the Interoperability Watch List is a relatively new oversight tool, the development of appropriate criteria and procedures for placing programs on the Interoperability Watch List is still in the formative stages.

In addition, the Director stated that the Air Force's Situational Awareness Data Link program was pursued as an initial pilot case for nomination to the Interoperability Watch List. He stated that the lessons learned from that pilot case will be applied as other programs are explored for Interoperability Watch List consideration.

Director, Operational Test and Evaluation Comments. The Director partially concurred, stating that, as a member of the Interoperability Senior Review Panel, his office continues to work with the other members on refining the Interoperability Watch List processes. Further, he stated that the Interoperability Watch List is one of many tools available within DoD to address interoperability problems. The Director also stated that the Interoperability Watch List policy states that the list will be used for those systems with interoperability issues that are not being adequately addressed by other forums.

The Director stated that the Interoperability Senior Review Panel has served a valuable role over the last 18 months by coordinating interoperability policies and actions across DoD and by working within existing forums to solve issues. For example, the Interoperability Senior Review Panel worked with the Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics to ensure that interoperability is stressed within advanced concept technology demonstrations to avoid problems in the transition of these experimental items to the force.

In addition, the Director stated that the criteria for Interoperability Watch List candidates suggested by the report were certainly a start and that his office and the Interoperability Senior Review Panel would use those criteria to evaluate future candidates. He also stated that the report cited the Director, Operational Test and Evaluation's Annual Report to Congress as a source of systems for the Interoperability Watch List.

In conclusion, the Director stated that, although he believed that those systems in the Annual Report already received adequate attention through test and evaluation oversight and other acquisition review processes, he would bring programs under test and evaluation oversight that were not adequately addressing interoperability to the attention of the Interoperability Senior Review Panel for its consideration.

Co-Chair, Interoperability Senior Review Panel Comments. The Co-Chair stated that the Interoperability Senior Review Panel will continue to refine the process and procedures to implement the Interoperability Watch List. Further, he stated that the Interoperability Senior Review Panel's pilot case in 2001 was the Air Force's Situational Awareness Data Link program. The Co-chair stated that the Interoperability Senior Review Panel determined that the Situational Awareness Data Link had significant interoperability issues. In addition, he stated that the visibility, which the Interoperability Senior Review Panel placed on the Situational Awareness Data Link, caused the Air Force to design an interoperable solution for its close air support aircraft.

The Co-Chair stated that the Interoperability Senior Review Panel continues to investigate other programs for the Interoperability Watch List and will work to find solutions within established processes of the Offices of the Joint Staff; the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); and the Director, Operational Test and Evaluation before placing a system on the Interoperability Watch List.

Audit Response. The comments of the Director, Joint Staff; the Director, Architecture and Interoperability, Office of the ASD(C3I); and the Director, Operational Test and Evaluation were responsive. However, the suggestion that the Director, Joint Staff made concerning the subparagraphs to the recommendation should be proposed to the Interoperability Senior Review Panel for defining criteria, processes, and procedures for the Interoperability Watch List.

Even though the Director, Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Inspector General, USJFCOM did not comment on the recommendation, the comments by the Co-Chair, Interoperability Senior Review Panel satisfied the requirement to comment because those offices are represented on the Interoperability Senior Review Panel.

In addition to investigating other programs for the Interoperability Watch List and working to find solutions within established processes before placing a system on the Interoperability Watch List, the Interoperability Senior Review Panel should have a clearly defined process and criteria for the Interoperability Watch List to work effectively. The specific criteria, processes, and procedures should be included in DoD instructions so that combat and materiel developers understand the ramifications of their systems not being interoperable. Therefore, we redirected the recommendation to the Co-Chair, Interoperability Senior Review Panel, and request that he provide additional comments on how

and when the Interoperability Senior Review Panel will establish a clearly defined process and criteria for placing DoD weapon systems in the development phase of the acquisition process on the Interoperability Watch List.

3. We recommend that the Co-Chair, Interoperability Senior Review Panel, in concert with the applicable membership of the Interoperability Senior Review Panel, ensure that the Commander, U.S. Joint Forces Command, pursuant to DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002, and the Chairman of the Joint Chiefs of Staff Instruction 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology Systems," May 8, 2000, as part of the operational requirements document interoperability certification process:

a. Compares the operational requirements documents of proposed DoD systems with joint mission area architectures, as they are completed, against the other operational requirements documents in the related joint mission area architecture to verify the completeness of stated interoperability requirements.

Inspector General, USJFCOM Comments. The Inspector General neither concurred nor nonconcurred; however, he stated that the recommendation is not achievable without the Joint Staff's completion of the joint mission area architectures. Further, he stated that USJFCOM recognizes that the development of the joint mission area architectures is critical when comparing requirements across programs and will continue to pursue this need separately and collectively in all available forums. In addition, the Inspector General recommended that the recommendation be changed for accuracy to read:

> Compare the operational requirements documents of proposed DoD systems with JMA [Joint Mission Area] architectures, as they are completed, against the other operational requirements documents in the related joint mission area architecture to verify the completeness of stated interoperability requirements.

The Inspector General suggested this new recommendation because USJFCOM was not resourced to execute Recommendations 3.a. and 3.b.

Director, Joint Staff Comments. The Director stated that the USJFCOM was required to review only operational requirements documents as standalone documents for compliance with capstone requirements documents. Further, he stated that USJFCOM does not have the authority or resources to provide a more in-depth review of operational requirements documents for interoperability within the respective family of systems. Further, the Director suggested that the recommendation be changed for accuracy to read:

> Compare all relevant requirements documents of proposed DoD IT [Information Technology] and NSS [National Security System] (to include SAP [Special Access Program]) systems with JMA [Joint Mission Area] architectures, as they are completed, against all other

> operational requirements documents in the related joint mission area architecture to verify the completeness of stated interoperability requirements.

Director, Architecture and Interoperability, Office of the ASD(C3I), Comments. The Director agreed with the underlying premise of the recommendation. However, the Director believes that the recommendation should have indicated that, before the Joint Forces Command can conduct an effective comparative analysis of operational requirements:

- the Joint Staff must first define the joint mission areas and subordinate supporting mission areas and
- the DoD Components must develop mission area integrated architectures.

Further, the Director stated that DoD Instruction 4630.8 assigns to the Joint Staff the responsibility to:

> Ensure mission area integrated architectures, strategies, concepts, and visions of the DoD Components are synchronized to support IT [Information Technology] and NSS [National Security System] interoperability requirements and identify opportunities for, and impediments to, interoperability.

The Director also stated that, once joint mission and subordinate mission areas are defined, the Joint Staff must coordinate with the DoD Components to ensure that DoD develops a consistent and integrated set of mission area integrated architectures across the Military Departments and Defense agencies. He proposed that a recommendation be made in the report for the Joint Staff to further refine existing joint mission areas and to define applicable subordinate mission areas to serve as a basis for the DoD Components to develop mission area integrated architectures.

Co-Chair, Interoperability Senior Review Panel Comments. The Co-Chair agreed with the concept of the recommendation, stating that the Interoperability Senior Review Panel recognizes that the development of the joint mission area architectures is critical to the comparison of requirements across programs. Further, he stated that Interoperability Senior Review Panel will continue to emphasize this need separately and collectively in all available forums. However, the Co-Chair stated that the recommendation, as drafted, is not actionable by the Joint Forces Command without Joint Staff completion of the joint mission area architectures.

Audit Response. The Inspector General, USJFCOM comments were responsive to the intent of our recommendation. In response to those comments, we revised the recommendation as suggested by the Inspector

General, USJFCOM. Further, we redirected the recommendation to the Co-Chair, Interoperability Senior Review Panel, and request that he provide additional comments on:

- the interim process that the Interoperability Senior Review Panel and USJFCOM will employ to compare the ORDs of proposed DoD systems against the other ORDs in the related mission area architecture to verify the completeness of stated interoperability requirements until the joint mission area architectures are completed; and

- the resources that the Interoperability Senior Review Panel and USJFCOM require to implement the recommendation.

In response to the Director, Joint Staff comments that USJFCOM does not have the authority or resources to provide a more in-depth review of operational requirements documents, Congress expressed its sense in Section 922, Public Law 105-261, that the commander of a combatant command should be provided with appropriate and sufficient resources for joint warfighting experimentation. It listed the responsibilities and authorities that should accompany that designation, including improving interoperability and making recommendations to the Chairman of the Joint Chiefs of Staff on mission needs statements and ORDs. Accordingly, if USJFCOM believes that resources are insufficient, it should request the resources needed to fulfill the congressional intent.

b. Uses quantification analysis and predictive tools, such as models or simulations, to assist in verifying the completeness of stated interoperability requirements in mission area architectures.

Inspector General, USJFCOM Comments. The Inspector General neither concurred nor nonconcurred; however, he stated that the recommendation was not fully achievable at this time. Further, he stated that, although the software tools referenced in the report are under USJFCOM assessment and show potential, the software tools must be officially accredited by the Office of the Secretary of Defense and the Joint Staff for the verification of joint interoperability requirements in mission area architectures.

Co-Chair, Interoperability Senior Review Panel Comments. The Co-Chair agreed with the concept of the recommendation and provided comments similar to those submitted by the Inspector General, USJFCOM.

Audit Response. The Inspector General, USJFCOM comments were responsive to the intent of our recommendation. However, because the software tools referenced in the report are under USJFCOM assessment and show potential, but have not yet been accredited, we redirected the recommendation to the Co-Chair, Interoperability Senior Review Panel and request that he provide additional comments on:

- when the accreditation process for the software tools will be completed, and

- when the software tools will be made available for the DoD Components to verify joint interoperability requirements of planned weapon systems in mission area architectures.

4. We recommend that the Co-Chair, Interoperability Senior Review Panel, in concert with the applicable membership of the Interoperability Senior Review Panel:

a. Update or archive, as applicable, outdated operational requirements documents maintained in the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool database.

Director, Joint Staff Comments. The Director concurred, subject to the inclusion of his comments, and suggested that the recommendation be redirected to the ASD(C3I); the Director, DISA; and the Commander, USJFCOM, in addition to the Director, Command, Control, Communications, and Computers Systems Directorate (J-6), Office of the Chairman of the Joint Chiefs of Staff. He stated that the reason for redirecting the recommendation was because:

- JCPAT access and archiving are functional responsibilities of the Defense Information Systems Agency;

- the Office of the ASD(C3I) also uses the JCPAT; and

- as the warfighters advocate for interoperability and integration, USJFCOM should participate in the architecture process to ensure that warfighter needs and interests are met.

Co-Chair, Interoperability Senior Review Panel Comments. The Co-Chair stated that the Interoperability Senior Review Panel supports the position of the Joint Staff regarding this recommendation. Specifically, the responsibility for the JCPAT goes beyond the Joint Staff; therefore, the recommendation should be addressed to all departments, agencies, and directorates that use or control access, or both, to the JCPAT. Further, he stated that the Interoperability Senior Review Panel will review the policy and guidance associated with the JCPAT and make recommendations to appropriate organizations.

Audit Response. The Director, Joint Staff comments were responsive to the intent of our recommendation. In response to those comments, we redirected the recommendation as suggested by the Director, Joint Staff. However, because the Offices of the Chairman of the Joint Chiefs of Staff; the ASD(C3I); the Commander, USJFCOM; and the Director, DISA are represented on the Interoperability Senior Review Panel, we redirected the recommendation to the Co-Chair, Interoperability Senior Review Panel and request that he provide comments on how those represented offices will update or archive, as applicable, outdated ORDs maintained in the JCPAT database.

b. Limit Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool access to users who have a need to know.

Director, Joint Staff Comments. The Director concurred, subject to the inclusion of his comments, and suggested that the recommended corrective action to limit JCPAT access to users who have a need to know be coordinated among the ASD(C3I); the Director, DISA; and Joint Staff directorates. He stated that the reason for coordinating the corrective action was because the JCPAT is a collaborative database used by the organizations listed in his suggested redirection of the recommendation, as discussed above in Recommendation 4.a.

Co-Chair, Interoperability Senior Review Panel Comments. The Co-Chair's comments to Recommendation 4.a. also applied to this recommendation.

Audit Response. The Director, Joint Staff comments were responsive to the intent of our recommendation. In response to those comments, we revised and redirected the recommendation as he suggested. Therefore, because the Offices of the Chairman of the Joint Chiefs of Staff; the ASD(C3I); the Commander, USJFCOM; and the Director, DISA are represented on the Interoperability Senior Review Panel, we redirected the recommendation to the Co-Chair, Interoperability Senior Review Panel and request that he provide comments on how those represented offices will limit JCPAT access to users having a need to know.

5. We recommend that the Director, Operational Test and Evaluation define and implement a plan to test critical operational issues, including interoperability and information assurance requirements, for DoD systems in the Global Information Grid.

Director, Operational Test and Evaluation Comments. The Director partially concurred, stating that testing of interoperability and information assurance takes on more critical status as we continue to transform into a network centric force. Further, he stated that his office already ensures that interoperability is tested to support the assessment of key performance parameters provided in the operational requirements documents and published policy in 1999 for testing information assurance.

In addition, the Director stated that his office conducted an assessment in 2000 to determine requirements for interoperability testing of systems within the scope of a larger networked system of systems linked over the Global Information Grid. As a result of this effort and similar initiatives by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Joint Staff, DoD funded an initial capability called the Joint Distributed Engineering Plant in the FY 2002 Program Objectives Memorandum. The Director believes that the objective of the Joint Distributed Engineering Plant capability will permit his office to do the testing called for in this recommendation. However, expanded funding for the Joint Distributed Engineering Plant beyond that recommended in the Program Objectives

Memorandum is required before the Plant will provide the full scope called for in this recommendation. Further, he stated that interoperability and information assurance are key enablers for the future.

Co-Chair, Interoperability Senior Review Panel Comments. The Co-Chair agreed, providing comments similar to those by the Director, Operational Test and Evaluation concerning testing of interoperability and information assurance and testing to support the assessment of key performance parameters provided in the operational requirements documents. Further, he stated that the Interoperability Senior Review Panel supports the development of necessary test capabilities to represent relevant aspects of the Global Information Grid that will allow programs to test in a system of systems environment. The Co-Chair also stated that the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); and the Director, Operational Test and Evaluation support expanded funding in the upcoming Program Objectives Memorandum for the Joint Distributed Engineering Plant, which will allow cost-effective testing of critical operational issues, including interoperability and information assurance requirements, for DoD systems in the Global Information Grid.

Appendix A. Scope and Methodology

We reviewed documentation dated from March 1992 to July 2002. During the audit policies continued to be updated. To accomplish the audit objective, we:

- interviewed and obtained documentation from the staffs of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the Director, Operational Test and Evaluation; the Office of the Joint Chiefs of Staff; the U.S. Joint Forces Command; the Defense Information Systems Agency; and the Joint Interoperability Test Command.

- reviewed the processes that the Office of the Secretary of Defense, the Office of the Chairman of the Joint Chiefs of Staff, and the Defense agencies used for certifying DoD systems for interoperability and information assurance and whether those processes were effectively implementing DoD information interoperability and information assurance policies.

Subsequent reports will discuss the adequacy of interoperability key performance parameters in operational requirements documents and the certification process for DoD system interoperability within the Army, the Navy, the Air Force, and the unified combatant commands.

We performed this audit from September 2001 through July 2002 in accordance with generally accepted government auditing standards. We did not review the management control program because the audit focused on interoperability and information assurance requirements and review processes; therefore, our scope was limited to those specific requirements and processes.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the DoD weapon systems acquisition high-risk area.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit.

Use of Technical Assistance. A computer specialist from the Technical Assessment Division, Office of the Assistant Inspector General for Auditing of the Department of Defense, assisted the auditors in reviewing information assurance requirements.

Prior Coverage

During the last 5 years, the General Accounting Office (GAO), the Inspector General of the Department of Defense (IG DoD), and the Defense Science Board have issued five reports addressing interoperability and information assurance requirements for Defense systems. Unrestricted General Accounting Office and Inspector General of the Department of Defense reports can be accessed at http://www.gao.gov and http://www.dodig.osd.mil/audit/reports, respectively.

General Accounting Office

GAO Report No. NSIAD-98-73, "Joint Military Operations: Weakness in DoD's Process for Certifying C4I Systems' Interoperability," March 1998

Inspector General of the Department of Defense

IG DoD Report No. D-2001-176, "Survey of Acquisition Manager Experience using the DoD Joint Technical Architecture in the Acquisition Process," August 22, 2001

IG DoD Report No. D-2001-121, "Use of the DoD Joint Technical Architecture in the Acquisition Process," May 14, 2001

IG DoD Report No. 98-023, "Implementation of the DoD Joint Technical Architecture," November 18, 1997

Defense Science Board

Defense Science Board Task Force, "Protecting the Homeland, Report of the Defense Science Board Task Force on Defensive Information Operations, 2000 Summer Study, Volume II," March 2001

Other Matters of Interest

Key Performance Parameter. Although information assurance is not required to be a KPP in operational requirements documents, without them, milestone decision authorities increase the risk that weapon systems program managers will not achieve secure information exchanges before planned production decisions. We suggested to the Joint Staff (J-8) that information assurance be established as mandatory KPP. The J-8 responded that interoperability was the only mandatory KPP and that KPPs were driven by the capabilities deemed most essential by the warfighter and validated by the requirements authority in accordance with guidance in Chairman of the Joint Chiefs of Staff Instruction 3170.01B, "Requirements Generation System," April 15, 2001.

Furthermore, the J-8 stated that the Chairman of the Joint Chiefs of Staff Instruction 3170.01B does require information assurance for most information technology systems and, in some cases, information assurance has been made a KPP. For example, the Global Information Grid Capstone Requirement Document requires information assurance as a KPP. Therefore, ORDs for programs operating within the GIG must have information assurance requirements, including designating information assurance as a KPP, as appropriate.

Information Assurance Strategies. DoD policy requires chief information officers to review and confirm that the information assurance strategy is consistent with DoD policies, standards, and architectures. The ASD(C3I) is required to review the information assurance strategy for all major DoD systems before the milestone decision authority approves the DoD system for entry into the next acquisition phase. The ASD(C3I) uses a checklist based on the Defense Information Technology Security Certification Accreditation Process to review information assurance strategies.

Over the past 2 years, the ASD(C3I) has reviewed and had input on approximately 40 programs. The ASD(C3I) could not provide the number of information assurance strategies that had been disapproved, but commented that the goal was to work with program managers toward successful information assurance strategies. For non-acquisition DoD systems such as those developed from advanced concept technology demonstrations, the designated milestone decision authority is required to certify that the system complies with the Defense Information Technology Security Certification Accreditation Process procedures before approving the system for fielding. Accordingly, chief information officers, program managers, and testers must be knowledgeable of those procedures. However, a requirement did not exist for the ASD(C3I) to provide oversight for those non-acquisition DoD systems to verify that the systems had an information assurance strategy and were accredited.

Beginning in July 2002, the National Security Telecommunication and Information Systems Security Policy requires that all U. S. Government departments limit the acquisition of commercial off-the-shelf information assurance and information assurance-enabled products to those that have been evaluated and validated in accordance with the:

- Common Criteria,
- National Information Assurance Partnership Evaluation and Validation Program, and
- Federal Information Processing Standards Publications Validation Program.

The ASD(C3I) stated that chief information officers, program managers, and testers in Defense agencies and Military Departments will have to execute the policy.

Appendix B. Definitions of Technical Terms

Acquisition Category. An acquisition category determines an acquisition program's level of review, decision authority, and applicable procedures. The acquisition categories consist of I, major Defense acquisition programs; IA, major automated information systems; II, major systems; III, programs not meeting the criteria for acquisition categories I, IA, or II; and IV, programs designated as such by the Army, Navy, and Marine Corps.

Advanced Concept Technology Demonstration. An advanced concept technology demonstration is used to determine the military utility of proven technology and to develop the concept of operations that will optimize effectiveness. Advanced concept technology demonstrations are not themselves acquisition programs, but are designed to provide a residual, usable capability upon completion, and possibly transition into acquisition programs. Funding is programmed to support the demonstration for up to 2 years in the field.

Architecture. An architecture is the structure of components, their interrelationships, and the principal guidelines governing their design and evolution over time.

Capstone Requirements Document. A capstone requirements document is a document that contains capabilities-based requirements for developing individual ORDs by providing a common framework and operational concept to guide their development. It is an oversight tool containing overarching requirements for a system-of-systems or family-of-systems.

Combat Developer. A combat developer is the command or agency that formulates doctrine, concepts, organization makeup, materiel requirements, and objectives. Generically, it represents the user community role in the materiel acquisition process.

Command, Control, Communications, Computers, and Intelligence Support Plan. A C4I support plan describes system dependencies and interfaces in sufficient detail to enable program managers and operational testers to test interoperability key performance parameters derived from information exchange requirements.

Command, Control, Communications, Computers, and Intelligence Surveillance and Reconnaissance Architecture Framework. The C4I surveillance and reconnaissance architecture framework provides rules, guidance, and product descriptions for developing and presenting different architectural views of a given system to ensure a common denominator for understanding, comparing, and integrating architectures across DoD.

Critical Operational Issue. A critical operational issue is a key operational effectiveness issue or operational suitability issue that must be examined in the operational test and evaluation to determine the system's capability to perform its mission.

Defense Acquisition Executive Summary. The Defense Acquisition Executive Summary is a multi-part document, which reports program information and assessments; program manager, program executive office, and Component acquisition executive comments; and cost and funding data primarily for Acquisition Category I programs.

Defense-in-Depth. Defense-in-depth integrates the capabilities of people, operations, and technology to establish multi-layer, multi-dimension protection of networked systems. The concept is to deploy defenses at multiple locations in successive layers in the protected information environment. Defense–in–depth focuses on the local computing environments (or enclaves), enclave boundaries, networks that link enclaves, and supporting infrastructures.

Developmental Test and Evaluation. Developmental test and evaluation is any engineering type of test used to verify the status of technical progress, verify that design risks are minimized, substantiate achievement of contract technical performance, and certify readiness for initial operational testing. Generally, those tests are instrumented and measured by engineers, technicians, or soldier operator-maintainer test personnel in a controlled environment to facilitate failure analysis.

Global Information Grid. The Global Information Grid provides the foundation for network-centric warfare, information superiority, decision superiority, and ultimately, full spectrum dominance. The GIG includes any system, equipment software, or service that transmits information to, receives information from, routes information among or interchanges information among other equipment, software, and services. Non-GIG Information Technology is stand-alone, self-contained, or embedded information technology that is not or will be connected to the enterprise network.

Information Assurance. Information assurance is information operations that protect and defend the information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and nonrepudiation. Information assurance provides for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Exchange Requirements. Information exchange requirements characterize the information exchanges to be performed by a proposed system and identify who exchanges what information with whom, why the information is necessary, and how the users will employ that information.

Information Technology. Information technology includes any equipment or interconnected system or subsystem of equipment that is used in automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, software, firmware, ancillary equipment and similar procedures, services, and related resources.

Information Warfare. Information warfare is used to achieve information superiority by affecting adversary information, information-based processes,

information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.

Interoperability. Interoperability is the ability of systems, units, or forces to provide services to or accept services from other systems, units, or forces and to use the services so exchanged to operate effectively together.

Interoperability Certification Process. The interoperability certification process consists of two interoperability certifications; the first for requirements and supportability documents and the second for interoperability certification testing. The Chairman of the Joint Chiefs of Staff (J-6) and the Joint Interoperability Test Command are responsible for requirements and supportability document certification and for interoperability certification testing, respectively.

Interoperability Senior Review Panel. The Interoperability Senior Review Panel recommends programs and systems deemed to have significant interoperability deficiencies for the Interoperability Watch List. The Panel is composed of the staffs from the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Director, Operational Test and Evaluation; the USJFCOM, and the Joint Staff.

Joint Distributed Engineering Plant. The Joint Distributed Engineering Plant is a DoD-wide effort to link existing Defense agencies and Military Departments and joint combat system engineering and test sites (including design activities, software support activities, test and evaluation facilities, training commands, and operational units). The Joint Distributed Engineering Plant is designed to improve the interoperability of weapon systems and platforms through rigorous testing and evaluation in a replicated battlefield environment.

Joint Mission Area. A joint mission area is a functional group of joint tasks and activities that share a common purpose and facilitate joint force operations.

Joint Operational Architecture. A joint operational architecture describes tasks and activities, operational elements, and information flows required to accomplish or support military operations; defines types of information exchanged, frequency of exchange, which tasks and activities are supported by information exchanges, and nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

Joint Requirements Oversight Council. The Joint Requirements Oversight Council assists the Chairman of the Joint Chiefs of Staff in identifying and assessing the priority of joint military requirements (including existing systems and equipment) to meet the national military strategy. The council, chaired by the Vice Chairman of the Joint Chiefs of Staff and consisting of all the Vice Chiefs of the Military Departments including the Assistant Commandant of the Marine Corps, directly supports the Defense Acquisition Board through review, validation, and approval of key cost, schedule, and performance parameters at

the start of the acquisition process, before each milestone review, and as requested by the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Joint Systems Architecture. The joint systems architecture identifies and describes those DoD systems and their interconnections needed to accomplish the tasks and activities described in the Joint Operational Architecture.

Joint Technical Architecture. The joint technical architecture is a common set of mandatory information technology standards, which are primarily interface standards and guidelines to be used by all emerging systems and systems upgrades, including advanced concept technology demonstrations. The joint technical architecture can be used to establish a system's technical architecture, and is applicable to all C4I and automated information systems and the interfaces of other key assets, such as weapon systems and sensors, with C4I systems.

Key Performance Parameters. Key performance parameters are capabilities or characteristics so significant that failure to meet the threshold or minimum acceptable value can be cause for the concept or system selected to be reevaluated or for the program to be reassessed or terminated.

Measure of Effectiveness. A measure of effectiveness is the quantitative expression defined to measure operational capabilities in terms of engagement of battle outcomes.

Measures of Performance. Measures of performance measure a system's technical performance expressed as speed, payload, range, time on station, frequency, or other distinctly quantifiable performance features. Several measures of performance may be related to the achievement of a particular measure of effectiveness.

National Security System. A national security system is any telecommunication or information system operated by the United States Government, whose function, operation, or use involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon system, or is critical to the direct fulfillment of military or intelligence missions.

Network-Centric Warfare. Network-centric warfare[14] allows a warfighting force to achieve improved information positions in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power.

Operational Architecture View. The operational architecture view is a description of the tasks and activities, operational elements, and information

[14]An in-depth discussion of network-centric warfare is provided in the book, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), by David S. Alberts, John J. Garstka, and Frederick P. Stein, C4I Surveillance and Reconnaissance Cooperative Research Program, August 1999.

flows required to accomplish or support a military operation. This architecture view defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

Operational Effectiveness. Operational effectiveness is the overall degree of mission accomplishment of a system when representative personnel use the system in the environment planned or expected for operational employment of the system, considering organization, doctrine, tactics, survivability, vulnerability, and threat.

Operational Requirements Document. The operational requirements document states the user's objectives and minimum acceptable requirements for the operational performance of a proposed concept or system.

Operational Suitability. Operational suitability is the degree to which a system can be placed satisfactorily in field use with consideration being given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistic supportability, natural environmental effects, documentation, and training requirements.

Operational Test and Evaluation. Operational test and evaluation is field testing, under realistic conditions, of any item or component of weapons, equipment, or munitions to determine their effectiveness and suitability for use in combat by typical military users and the evaluation of the results of such tests.

Planning, Programming, and Budgeting System. The Planning, Programming, and Budgeting System is the primary resource allocation process of DoD. It is a formal, systematic structure for making decisions on policy, strategy, and the development of forces and capabilities to accomplish anticipated missions.

Program. A program is an acquisition funded by research, development, test and evaluation or procurement appropriations, or both, with the express objective of providing a new or improved capability in response to a stated mission need or deficiency.

Program Objectives Memorandum. The Program Objectives Memorandum is an annual memorandum, which the DoD Component Heads submit to the Secretary of Defense, that recommends the total resource requirements and programs within the parameters of the Secretary of Defense's fiscal guidance.

Risk. Risk is a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact.

System. A system is the organization of hardware, software, materiel, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of specified data, its processing, and delivery to users.

System-of-Systems. System-of-systems, also known as a family-of-systems, is several independent programs which, when integrated, form a system to meet the needs of a broad mission area such as missile defense. The performance of the individual component programs making up the system-of-systems is specified in the respective program ORDs; the overarching requirements for the system-of-systems is contained in a CRD.

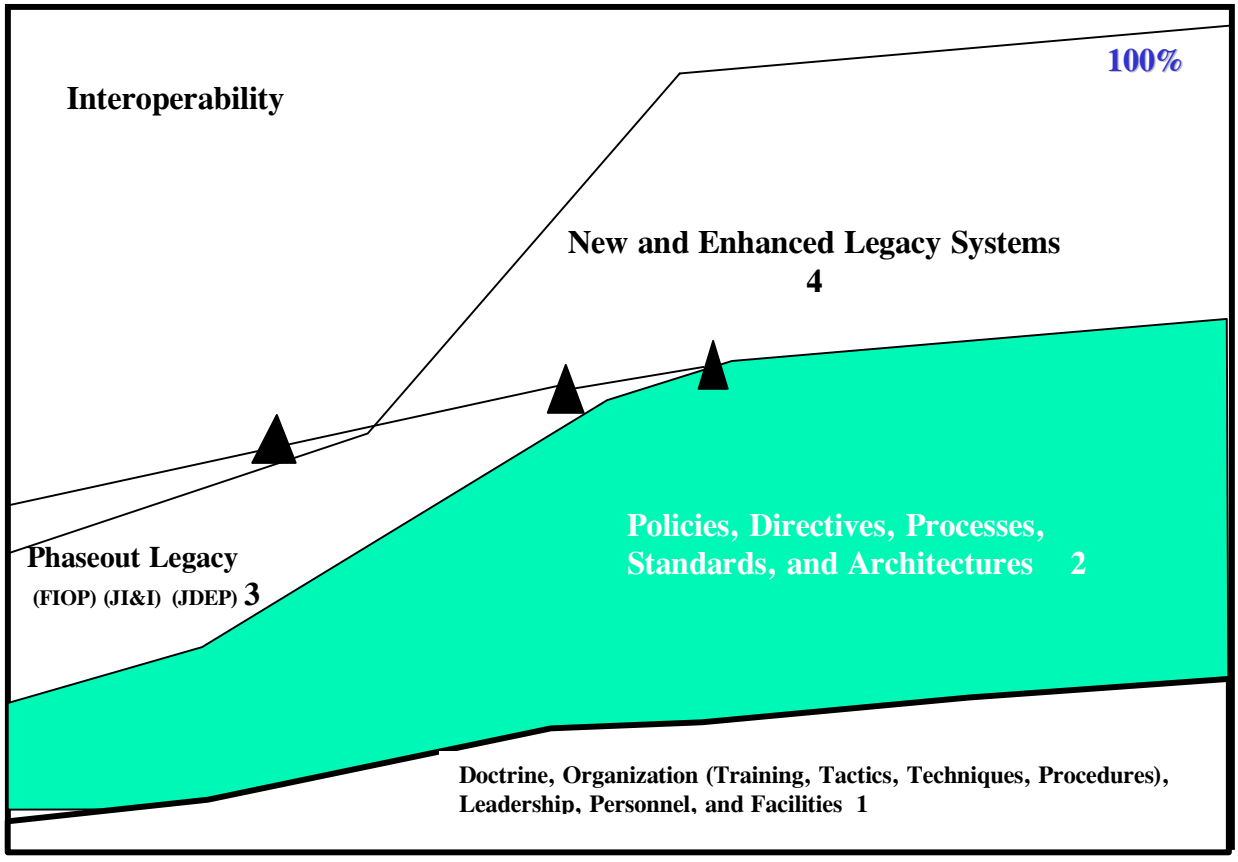
Systems Architecture View. The systems architecture view is a description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions. This architecture view associates physical resources and their performance attributes to the operational view and its requirements in accordance with standards defined in the technical architecture.

Technical Architecture View. The technical architecture view is the minimum 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. This architecture view includes a collection of the technical standards, conventions, rules, and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.

Test and Evaluation Master Plan. The test and evaluation master plan (TEMP) documents the overall structure and objectives of the test and evaluation program. It provides a framework within which to generate detailed test and evaluation plans and it documents schedule and resource implications associated with the test and evaluation program. The TEMP identifies the necessary developmental test and evaluation, operational test and evaluation, and live-fire test and evaluation activities. Further, the TEMP relates program schedule, test management strategy and structure, and required resources to critical operational issues, critical technical parameters, objectives and thresholds documented in the operational requirements document, evaluation criteria, and milestone decision points.

Test Integration Working Group. The Test Integration Working Group facilitates the integration of test requirements through close coordination between the materiel developer, combat developer, logistician, and developmental and operational testers to minimize development time and cost, and preclude duplication between developmental and operational testing.

Appendix C. Interoperability Action Plan of the Under Secretary of Defense for Acquisition, Technology, and Logistics for Command and Control Systems[15]



2001: Policy modifications and transition plans in place

2003: Overarching battle management/ command and control begin to take effect

2005: "Readily Resolvable" interoperability problems solved for legacy command and control systems

2008: Legacy command and control interoperability problems resolved; Interoperability institutionalized in processes and Architectures

[15]The numbers in the diagram relating to the elements required to achieve interoperability are described on the next page.

According to the Director of Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the following four major elements are needed to achieve interoperability for command and control systems.

1. Doctrine, organization, training, tactics, techniques and procedures, leadership, personnel, facilities, which form the foundation for any military operation.

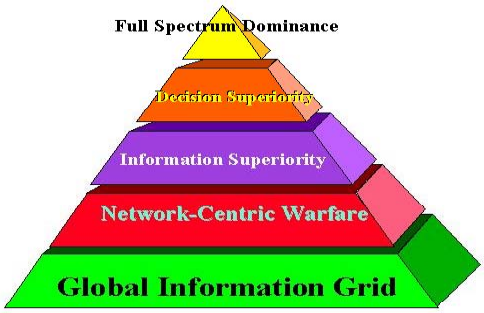
2. Policies, directives, processes, standards, and architectures without which real progress is impossible. Policies are necessary; however they are not sufficient.

3. To transition from legacy DoD systems to the future vision, overarching battle management command and control programs are necessary to provide for legacy DoD systems' integration and transition to the desired interoperability state. Those overarching programs are:
   - The Family of Interoperable Operational Pictures (FIOP), which will provide for systems engineering solutions for achieving interoperability of more than 30 critical battle management command and control systems (fielded and in development), within appropriate "communities of shared interest," from the combatant commander to the soldier, sailor, marine, airman, and coalition partners, including the seams between the Single Integrated Air Picture, a Single Integrated Ground Picture, a Single Integrated Maritime Picture, and the Common Operational Picture/Common Tactical Picture.
   - The Joint Interoperability and Integration (JII) reviews legacy and future systems' interoperability requirements in the total context of doctrine, operations, training, materiel, logistics, personnel, and facilities, and is tied to an "Interoperability Transition Fund" intended to focus on priority interoperability fixes.
   - The Joint Distributed Engineering Plant (JDEP) is designed to improve interoperability through distributed testing and evaluation involving the Services, DoD Components, and eventually industrial and allied resources.
4. New systems such as the Joint Tactical Radio System will contribute to the interoperability solution. Many marginally interoperable legacy systems will be phased out. The Quadrennial Defense Review and the normal Planning, Programming, and Budgeting System process should be used to determine priorities and funding for those systems.

The Under Secretary of Defense for Acquisition, Technology, and Logistics, estimates that if the overarching programs did not transition from the legacy to the future vision, the time to achieve the desired interoperability state would most likely double.

Appendix D. Global Information Grid

Global Information Grid. The GIG provides the foundation for network-centric warfare, information superiority, decision superiority, and ultimately full spectrum dominance as depicted below.



Global Information Grid as the Foundation for Achieving Full Spectrum Dominance

Source: Capstone Requirements Document for the GIG

The concept of the GIG evolved from concerns about the interoperability and end-to-end integration of automated information systems. Issues such as streamlined management and improved information infrastructure investment also contributed to the heightened interest in a GIG. However, the real demand for a GIG originates from the requirement for information and decision superiority to achieve full spectrum dominance, as expressed in Joint Vision 2020. The ability to achieve shared situational awareness and knowledge among all elements of a joint force, including allied and coalition partners, is increasingly viewed as a cornerstone to transform future warfighting capabilities.

Network-Centric Warfare. The GIG capstone requirement document states that network-centric warfare allows a warfighting force to achieve improved information positions in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power.

Information Superiority. Information superiority 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. Information superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve

operational objectives. Information superiority provides the joint force with a competitive advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to take advantage of superior information converted to superior knowledge to achieve "decision superiority."

Decision Superiority. Decision superiority is to arrive at better decisions and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission. Decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary.

Full Spectrum Dominance. The transformation of the joint force to reach full spectrum dominance rests upon information superiority as a key enabler and our capacity for innovation. The label full spectrum dominance implies that U.S. Forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all domains: space, sea, land, air, and information. Additionally, given the global nature of our interests and obligations, the United States must maintain its overseas presence forces and the ability to rapidly project power worldwide in order to achieve full spectrum dominance.

Appendix E. Multiple Factors Affecting the Implementation of Interoperability Requirements in the Weapon System Development Process

The following diagram shows the complex relationships governing the development of an interoperable system. The diagram shows four relationships for achieving interoperability.

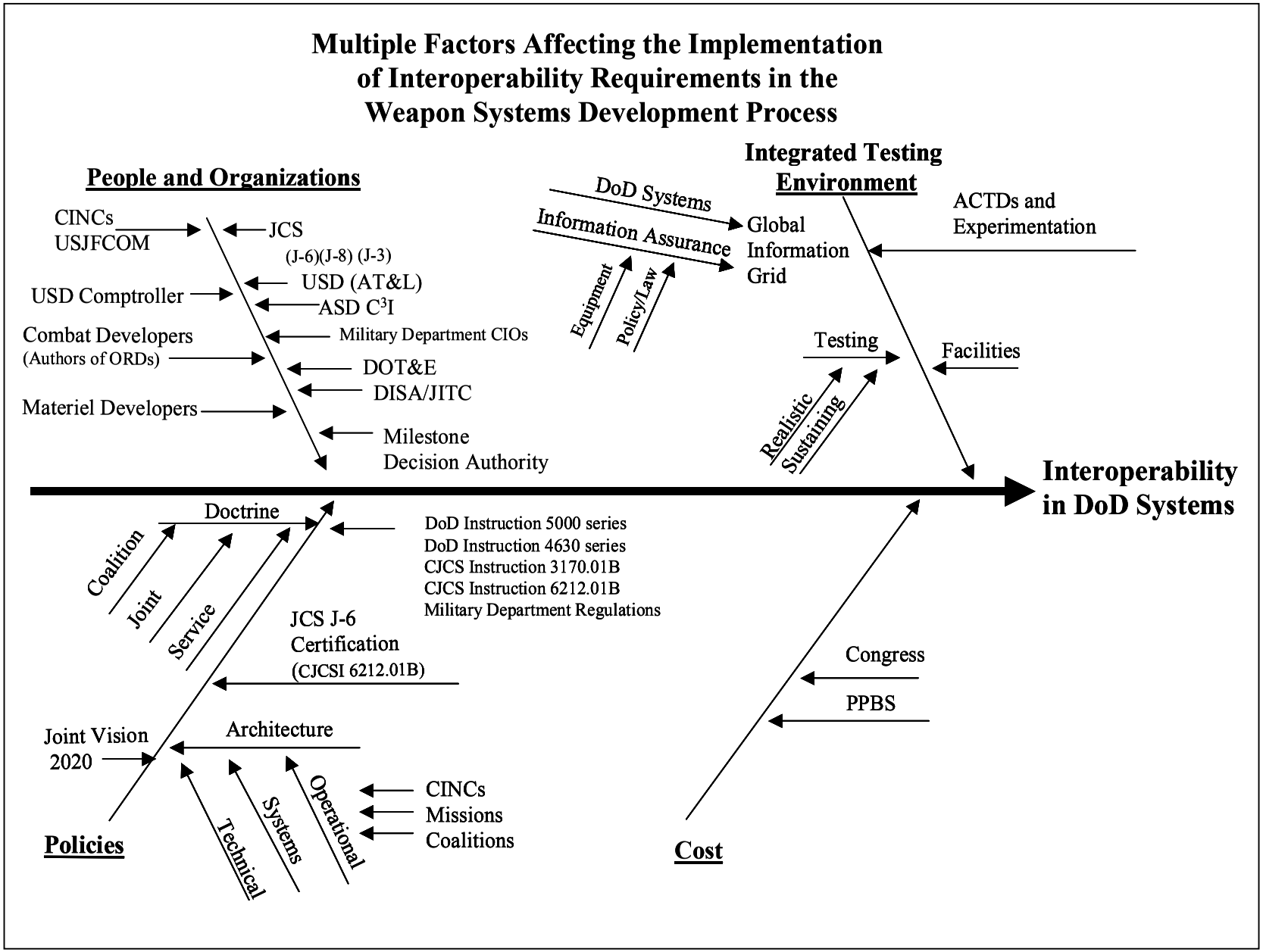
- **People and Organizations.** Organizations with responsibility for verifying and validating interoperability requirements before production decisions are shown in the diagram. Milestone decision authorities can not approve DoD systems for production before interoperability requirements are determined and tested.

- **Policies.** Program managers of DoD systems need to comply with numerous policies, doctrines, and architectures that define how the systems must operate in different environments and circumstances around the world. Therefore, combat developers must clearly depict the doctrine, training, organizations, soldiers, facilities, and relationship of the system to joint and allied systems before developing and acquiring a system.

- **Integrated Testing Environments.** Military Departments need test facilities and equipment to test the achievement of interoperability requirements for a DoD system in development. To realistically test how a system will interoperate in a joint and allied environment as envisioned in the GIG and Joint Vision 2020, additional equipment and resources may be required or shared with integrated testing environments.

- **Cost.** The Planning, Programming, and Budgeting System is a structured process that results in funding for DoD systems. Materiel developers of DoD systems attempt to maintain the planned acquisition strategy. If the acquisition strategy is not maintained, adjustments to the funding process should be made that are not always possible because of other DoD funding priorities.

All of the relationships must be met for a DoD system to meet the user's requirement for interoperability.


Multiple Factors Affecting the Implementation of Interoperability Requirements in the Weapon Systems Development Process
People and Organizations
CINCs USJFCOM
JCS
(J-6)(J-8) (J-3)
USD (AT&L)
USD Comptroller
ASD C3I
Military Department CIOs
Combat Developers (Authors of ORDs)
DOT&E
DISA/JITC
Materiel Developers
Milestone Decision Authority
Integrated Testing Environment
DoD Systems
Information Assurance
Global Information Grid
Equipment
Policy/Law
ACTDs and Experimentation
Testing
Facilities
Realistic
Sustaining
Interoperability in DoD Systems
Doctrine
Coalition
Joint
Service
DoD Instruction 5000 series
DoD Instruction 4630 series
CJCS Instruction 3170.01B
CJCS Instruction 6212.01B
Military Department Regulations
JCS J-6 Certification (CJCSI 6212.01B)
Joint Vision 2020
Architecture
Technical
Systems
Operational
CINCs
Missions
Coalitions
Policies
Cost
Congress
PPBS

Acronyms

ACTD	Advanced Concept Technology Demonstration
CINC	Commander-in-Chief
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CIO	Chief Information Officer
DODI	Department of Defense Instruction
DOT&E	Director, Operational Test and Evaluation
JCS	Joint Chiefs of Staff
J-3	Director for Operations, Joint Chiefs of Staff
J-6	Director for Command, Control, Communications and Computers Systems, Joint Chiefs of Staff
J-8	Director for Force Structure, Resources, and Assessments, Joint Chiefs of Staff
JITC	Joint Interoperability Test Command
PPBS	Planning, Programming, and Budgeting System
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD (Comptroller)	Under Secretary of Defense (Comptroller)/Chief Financial Officer
USJFCOM	U.S. Joint Forces Command

Appendix F. Interoperability and Information Assurance Policies

The following discusses relevant DoD and Joint Staff policies on interoperability and information assurance.

Interoperability Policy. DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" January 11, 2002; DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002; DoD Instruction 5000.2, "Operation of the Defense Acquisition System," April 5, 2002; DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," April 5, 2002; Chairman of the Joint Chiefs of Staff Instruction 3170.01B, "Requirements Generation System," April 15, 2001; and Chairman of the Joint Chiefs of Staff Instruction 6212.01B, "Interoperability and Supportability of National Security Systems, and Information Technology Systems," May 8, 2000, provide policy on interoperability.

DoD Directive 4630.5. DoD Directive 4630.5 requires that information technology and national security systems' interoperability and supportability needs be identified through the requirements definition and validation process, during the acquisition process, and updated as necessary throughout the system's life. Those requirements will be specified to a level of detail that allows verification of interoperability throughout a system's life. Also, those requirements will be characterized through operational mission area integrated architectures, operational concepts, and capstone requirements documents (CRDs) derived from joint mission areas and business and administrative mission areas. The joint operational architecture, the joint systems architecture, and the joint technical architecture serve as the foundation for development of operational mission area integrated architectures. Operational mission area integrated architectures connect information technology and the national security systems' interoperability and supportability requirements in a family-of-systems and system-of-systems context. Information technology and national security systems' information exchange requirements and associated interoperability key performance parameters (KPPs) are to be derived from the operational view of the mission area integrated architecture. Further, DoD is required to develop, acquire, and deploy C3I systems and equipment for U.S. Forces that are compatible with existing and planned C3I systems.

DoD Instruction 4630.8. DoD Instruction 4630.8 requires that joint, combined, coalition, and interagency missions must be supported through interoperable information technology and national security systems in global operations across the peace-conflict spectrum. All information technology and national security systems for U.S. Forces use are to be considered for use by joint, allied, and other U.S. Government departments and agencies. Information technology and national security systems' interoperability and

supportability requirements are to be identified through the mission area integrated architectures. Interoperability requirements are required to be managed, evaluated, and reported throughout the life of the system. All DoD acquisition category programs will use a C4I support plan to document interoperability requirements. Additionally, interoperability and supportability requirements are required to be balanced with the need for information assurance. The DoD Components are required to submit mission need statements, CRDs, ORDs, and C4I support plans for all information technology and national security system acquisitions or procurements to the Joint Staff for review to comply with joint policy, doctrine, and interoperability requirements. Additionally, requirements documents are to be reviewed by the Director, Defense Information Systems Agency for compliance with the DoD Joint Technical Architecture.

Furthermore, the Joint Staff is to develop, approve, and direct the use of the Joint Mission Area-based Joint Operational Architecture and direct its use when developing information technology and national security systems' interoperability requirements. The Instruction states that the Director, Operational Test and Evaluation is to develop policy and processes to test and evaluate information technology and national security systems in order to accurately assess the level of interoperability of the tested system with the intended family-of-systems with which it must operate. Additionally, the Director, Operational Test and Evaluation is required to confirm that the TEMP has identified information technology and national security systems' interoperability requirements for programs tested under the Director, Operational Test and Evaluation's oversight.

DoD Instruction 5000.2. DoD Instruction 5000.2 states that the user representative, with support from the operational test and evaluation community, develops the needs expressed in the mission need statement into requirements in the form of CRDs, if applicable, and ORDs. CRDs contain capabilities-based requirements to develop individual ORDs that provide a common framework and operational concept. The CRD is an oversight tool that establishes overarching requirements for a family of systems. Validated ORDs translate the mission needs statement and, if applicable, CRDs into broad, flexible, and time-phased operational goals that are further detailed and refined into specific operational capability requirements in the final ORD. The appropriate requirements authority validates all mission needs statements, CRDs, and ORDs.

DoD Regulation. DoD Regulation 5000.2-R states that, during the requirements generation process, users will develop interoperability KPPs for all CRDs and ORDs. In developing the ORD, the ORD sponsor considers using the products described in the C^4I Surveillance and Reconnaissance Architecture Framework and universal resources such as the joint technical architecture. The joint operational architecture and the joint technical architecture serve as the foundation for evolutionary development of those mission area integrated architectures. Mission area integrated architectures are to state information technology and national security systems' interoperability requirements in a family-of-systems mission area context. The user is to derive family-of-system

information technology and national security systems information exchange requirements from the operational information exchange requirements of the mission area integrated architecture.

Further, the regulation requires the overarching integrated product team to assess family-of-system or system-of-system capabilities for DoD systems within mission areas in support of mission area operational architectures developed by the Joint Staff before milestone decisions. Further, the ORD sponsor is to characterize information interoperability, as applicable, within a family-of-systems, a mission area, and a mission for all information technology and national security systems. Available mission area integrated architectures are to be used to develop information technology and national security systems' interoperability requirements. The regulation also states that the joint operational architecture and the joint technical architecture serve as the foundation for evolutionary development of mission area integrated architectures. The implementation of the joint technical architecture is required for all new, or changes to existing, information technology systems, including National Security systems.

The regulation also requires that all major Defense acquisition programs, programs on the Office of the Secretary of Defense Test and Evaluation Oversight list, legacy systems, and all programs and systems that must be interoperable with them be subject to interoperability evaluations throughout their life cycles to validate their ability to support mission accomplishment. At their discretion, the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Chairman of the Joint Chiefs of Staff ; the Commander, USJFCOM; and the Director, Operational Test and Evaluation can place programs and systems deemed to have significant interoperability deficiencies on the Interoperability Watch List (Watch List). Program managers with a program on the Watch List must take corrective actions to address identified interoperability deficiencies to remove their programs from the Watch List.

The regulation requires that, for programs on the Watch List, program managers will provide periodic updates of their status towards correcting identified deficiencies to senior representatives of Under Secretary of Defense for Acquisition, Technology, and Logistics; ASD(C3I); the Director, Operational Test and Evaluation; the USJFCOM; and the Joint Staff. The program managers of DoD systems, or other cognizant officials, and the responsible test organization (either developmental or operational), in conjunction with JITC, are to provide those updates. Those updates are to support an assessment on whether interoperability issues are being adequately addressed, and whether a status change is warranted; for example, whether the program or system should be removed from the Watch List, kept on the Watch List, or proposed for Director, Operational Test and Evaluation oversight. Staff members of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Director, Operational Test and Evaluation; the USJFCOM; and the Joint Staff are to prepare quarterly reports summarizing the activities of systems and programs on the Watch List.

Joint Staff Instruction 3170.01B. Chairman of the Joint Chiefs of Staff Instruction 3170.01B requires that the Joint Staff J-6 certify mission need statements, CRDs, and ORDs, regardless of acquisition category, for conformance with joint C4I policy and doctrine, technical architectural integrity, and interoperability standards. The Joint Staff J-6 is to review and comment on interoperability KPPs and coordinate C4I issues concerning mission need statements, capstone requirement documents, and ORDs with the appropriate agencies.

The Joint Staff J-6 is to forward for coordination the C4I interoperability requirements certification to the Joint Requirement Oversight Council for major DoD acquisition programs, major automated information systems, and special interest programs or to the sponsoring DoD Component for major systems and below programs. Failure for those systems to meet a KPP threshold in an ORD can be a reason for the system selection to be reevaluated or for the program to be reassessed or terminated.

Joint Staff Instruction 6212.01B. Chairman of the Joint Chiefs of Staff Instruction 6212.01B requires the USJFCOM to provide comments to the Joint Staff J-6 on interoperability issues for all acquisition category programs to ensure that each ORD contains interoperability KPPs and information exchange requirements. Furthermore, commanders of combatant commands, Military Departments, and Defense agencies are to incorporate interoperability testing into their overall testing plans in coordination with the Defense Information Systems Agency (DISA) and Joint Interoperability Test Center (JITC). In addition, JITC is to certify test results for all interoperability system tests.

DoD Chief Information Officer Memorandum. In DoD Chief Information Officer Guidance and Policy Memorandum No. 8-8001, March 31, 2000, the DoD Chief Information Officer authorizes the Director, Operational Test and Evaluation to include critical operational issues addressing interoperability and information assurance in the Global Information Grid operational test and evaluation.

Information Assurance Policy. DoD Regulation 5000.2-R, DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997; Chairman of the Joint Chiefs of Staff Instruction 3170.01B; Chairman of the Joint Chiefs of Staff Instruction 6510.01C, "Information Assurance and Computer Network Defense," May 1, 2001; and Director, Operational Test and Evaluation memorandum, "Policy for Operational Test and Evaluation of Information Assurance," November 17, 1999, provide policy on information assurance.

DoD Regulation. DoD Regulation 5000.2-R requires program managers to incorporate information assurance requirements into program design functions to ensure availability, integrity, authenticity, confidentiality, and nonrepudiation of critical system information. Further, program managers are to manage information systems using the best processes and practices to reduce security risks, including the risks to timely accreditation.

Furthermore, the regulation requires that information assurance testing be conducted on information systems to ensure that planned and implemented security measures satisfy ORD and System Security Authorization Agreement requirements when the system is installed and operated in its intended environment. The program manager, operational test and evaluation authority, and designated approving authority are to coordinate and determine the level of risk associated with operating the system and the extent of security testing required. Requirements to reconstitute or recover information system capabilities damaged by information assurance threat agents are also to be tested during operational test and evaluation.

The regulation requires that all weapon, command, control, communications, computers, intelligence, surveillance, and reconnaissance, and information programs that are dependent on external information sources, or that provide information to other DoD systems, be assessed for information assurance. The level of information assurance testing depends on the system risk and importance. Systems with the highest importance and risk are to be subject to penetration-type testing prior to the beyond low-rate initial production decision. Systems with minimal risk and importance are to be subject to normal National Security Agency security and developmental testing, but not subject to field penetration testing during operational test and evaluation.

DoD Instruction. DoD Instruction 5200.40 establishes the DoD Information Technology Security Certification and Accreditation Process for security certification and accreditation of unclassified and classified information technology. The Process sets forth the activities and management structure to certify and accredit information technology systems that will maintain the security posture of the Defense Information Infrastructure. The Process requires a System Architecture Analysis, which requires the system architecture to comply with the Systems Security Authorization Agreement architecture description. The interfaces between this and other systems are to be identified and the interfaces evaluated to assess their effectiveness in maintaining the security posture of the infrastructure.

Joint Staff Instruction 3170.01B. Chairman of the Joint Chiefs of Staff Instruction 3170.01B states that information assurance is required for all DoD systems that are used to enter, process, store, display, or transmit DoD information, regardless of classification or sensitivity. Information assurance requirements are to be codeveloped and coevolved with those for information interoperability.

Joint Staff Instruction 6510.01C. Chairman of the Joint Chiefs of Staff Instruction 6510.01C provides joint policy and guidance for information assurance and computer network defense operations. Information assurance is critical to the military's ability to conduct warfare and is the responsibility of all warfighters. Because of the universal nature of the Global Information Grid, a risk assumed by one organization, at any organization level, can be a risk imposed on all DoD organizations. Accordingly, the requirement for implementing information assurance is at all organization levels. The primary method of using information assurance is through the defense-in-depth strategy.

To prevent a potential breakdown of barriers and an invasion of the innermost or most valuable parts of the system, successive layers and safeguards must be constructed at different locations in the system. Those different locations are expressed as local computing networks, enclave boundaries, networks, and supporting infrastructures. Through a deliberate risk analysis process, program managers can make effective risk management decisions to ensure that the most effective defense-in-depth strategy, given the resources available, is deployed. Additionally, all DoD Components are required to establish an active risk management and mitigation program for information and information-based processes, and information systems, such as command, control, communications, and computer systems; weapon systems; and information infrastructures used by military forces. The associated information is to be protected based on the value of the information contained in the system and the risks associated with its compromise or loss.

Director, Operational Test and Evaluation Memorandum. The Director's memorandum establishes policy for operational test and evaluation of information assurance for all Director, Operational Test and Evaluation oversight programs, including weapon systems, C4I surveillance and reconnaissance systems, and information systems. The policy applies to acquisition programs that have not reached the production decision. The policy contains a four-step process to review information assurance during operational test and evaluation, as follows.

- **Requirements, Threat, and Test Documentation Review.** During this step, the Director, Operational Test and Evaluation determines the relevance of information-assurance testing based on requirements, and assesses vulnerabilities and the importance of program functions and missions.

- **Test Strategy Development.** For those programs that were not waived in the Step One review, the Director, Operational Test and Evaluation conducts a paper vulnerability assessment as part of the normal test strategy development using experts, program office personnel, operational test activity representatives, and users to define the degree to which operational information assurance testing is warranted. Test plans are not to be approved unless they contain a well-defined strategy for addressing information assurance concerns, adequate resources, and appropriate measures against which to test stated requirements. Those programs with operational test and evaluation waivers for information assurance are to note the waiver in their TEMP and test plan.

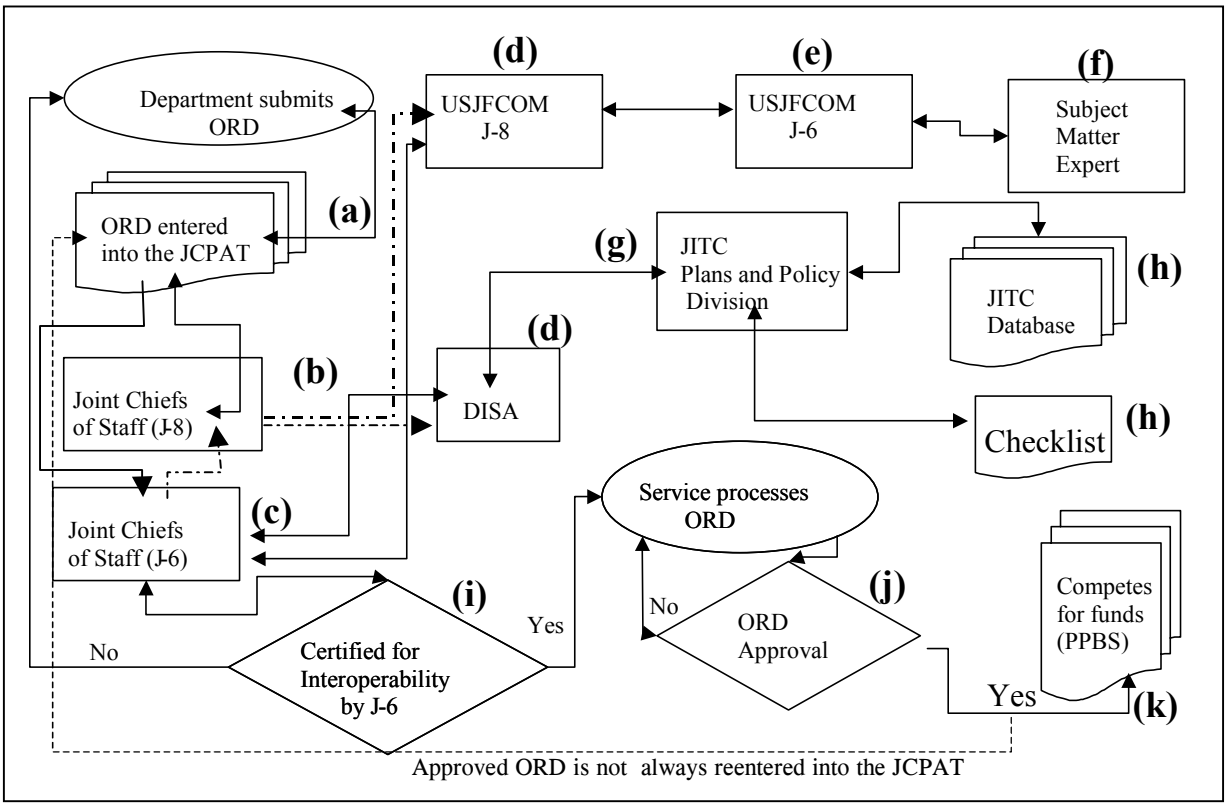
- **Review of Information Assurance Development Test and Evaluation and Computer Security Certification Results Before Entry into Operational Test and Evaluation.** For those systems considered to possess potentially high or unknown residual information assurance risk, the operational test activities are to examine development test and evaluation and Defense Information

Technology Security Certification Accreditation Process data, including any concurrent operational assessments that may have already occurred, in judging the effectiveness of that system.

- **Evaluation of Information Assurance Vulnerabilities During Operational Test.** Those programs that have undergone Steps One, Two, and Three and are still judged to have a high or unknown vulnerability are to be subject to field testing as part of the initial operational test and evaluation.

Appendix G. DoD System Interoperability Requirements Review Process

The C4I Surveillance and Reconnaissance Architecture Framework documents how architectures are created. Once an architecture is created, KPPs in the ORD are defined. The following flow chart shows the interoperability certification review process. The interoperability certification review process has three stages.



Stage One[16]

(a) The Defense agency or Military Department enters the ORD, regardless of the acquisition category, into the JCPAT.

(b) The acquisition category I ORD is forwarded the to the Force Structure, Resources, and Assessment Directorate J-8 (Joint Staff J-8), who staffs the requirement with the members of the Joint Requirement Oversight Council.

[16]Stage lasts 35 days.

(c) The acquisition category II and below ORD is staffed with the Command, Control, Communications, and Computers Systems Directorate J-6 (Joint Staff J-6).

(d) The Joint Staff J-6 staffs the acquisition category II and below ORD with DISA and the USJFCOM J-8.

(e) The USJFCOM J-8 staffs the document with the USJFCOM J-6

(f) The USJFCOM J-6 directs subject-matter experts review the ORD from a warfighter perspective to verify that GIG requirements are in the ORD. The USJFCOM J-6 receives comments from the subject-matter expert and then forwards those and any additional comments back through the chain to the Joint Staff J-6.

(g) DISA staffs the ORD through the Plans and Policy Division which then determines the lead JITC division. That division assigns a specific subject-matter expert to review the ORD from a technical perspective. After the review, the Plans and Policy Division consolidates comments on the ORD from the subject-matter expert with those from other JITC divisions.

(h) JITC subject–matter experts use a checklist to ensure that their mission need statements, CRDs, ORDs, C4I support plans, and TEMPs meet DoD policy requirements. Based on the results of the checklist review, comments are entered in the JITC database and forwarded to the Joint Staff J-6 through the DISA. The JITC database maintains historical data on documentation for DoD systems until operational testing is completed. JITC uses the data in its database and information from other sources such as symposiums, field demonstrations, or program managers to identify interoperability and information assurance requirements.

Stage Two[17]

(i) If the Joint Staff J-6 does not certify the ORD in stage one, the ORD, with comments, is returned to the Defense agency or Military Department for resolution of interoperability issues. After the issues identified in stage one are resolved, stage two, which is the same process as stage one, begins. If no deficiencies are found by the Joint Staff J-6, the ORD may be certified for interoperability.

(j) After certification for interoperability, the Joint Staff J-6 returns the ORD to the Military Department or the Defense agency, as applicable. The Military Department or the Defense agency is responsible for ORD approval.

[17]Stage two lasts 21 days.

(k) When the ORD is approved, the requirement competes for funding in the Planning, Programming, and Budgeting System process. However, no requirement exists for Military Departments or Defense agencies to submit the final approved ORD to be updated in the JCPAT.

Stage Three[18]

Stage III is the posting of the Acquisition Category II or III Milestone Decision Authority approved mission need statements, CRD, or ORD. Approved documents are filed in the JCPAT with the Joint Staff J-6 certification letter.

[18]Stage three suspense is 15 days after the Joint Requirements Oversight Council or the milestone decision authority approves the mission need statement, CRD, or ORD and posting the document into the JCPAT, according to the Chairman of the Joint Chiefs of Staff Instruction 6212.01B.

Appendix H. Organizations with Access to the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool

Office of the Secretary of Defense

Assistant Secretary of Defense (Command, Control, Communications, and Computers)
Inspector General of the Department of Defense

Joint Staff

Director for Intelligence (J-2)
Director for Operations (J-3)
Director for Logistics (J-4)
Director for Strategic Plans and Policy (J-5)
Director for Command, Control, Communications, and Computers (J-6)
Director for Operational Plans and Interoperability (J-7)
Director for Force Structure, Resources, and Assessment (J-8)

Department of the Army

Deputy Chief of Staff Operations and Plans, Headquarters Department of the Army
Commander, Communications and Electronics Command
Commander, Executive Agent Theater Joint Tactical Networks
Commander, Training and Doctrine Command

Department of the Navy

Deputy Assistant Secretary of the Navy
Deputy Chief of Naval Operations (Resources, Requirements, and Assessments)
Director, Equipment and Requirements Division, United States Marine Corps

Department of the Air Force

Deputy Chief of Staff for Air and Space Operations

Unified Commands

Commander, U.S. European Command
Commander, U.S. Pacific Command
Commander, U.S. Joint Forces Command
Commander, U.S. Southern Command
Commander, U.S. Central Command
Commander, U.S. Space Command
  North American Aerospace Defense Command
Commander, U.S. Special Operations Command
Commander, U.S. Strategic Command
Commander, U.S. Transportation Command

Other Defense Organizations

Director, Operational Test and Evaluation
Director, Defense Finance and Accounting Service
Director, Defense Intelligence Agency
Director, Defense Logistics Agency
Director, Defense Information Systems Agency
  Director for Operations
  Director for Acquisitions, Logistics, and Facilities
  Director for Strategic Plans and Policy
  Director for Engineering and Information
  Director for Joint Requirement Analysis and Integration
  Director for Command, Control, Communications, Computers and Intelligence
    Modeling, Simulation, and Assessment
  Director for Applications Engineering Directorate
    Program Planning Office
  Director for Interoperability
  Principal Director for Network Services
  Commander, Joint Interoperability Test Command
  Commander, Joint Spectrum Center
Commander, Joint Theater Air and Missile Defense Organization
Director, Joint Warfighting Capabilities and Assessment
Commander, Missile Defense Agency
Director, National Imagery and Mapping Agency
Director, National Reconnaissance Office
Director, National Security Agency

Appendix I. Response to Office of the Secretary of Defense and Defense Agency Comments Concerning the Report

Our detailed response to the comments from the Director, Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Director, Architecture and Interoperability, Office of the ASD(C3I); the Inspector General, Office of the Commander, USJFCOM; the Inspector General, DISA; the Director, Joint Staff; and the Co-Chair, Interoperability Senior Review Panel, on statements in the draft report follow. The complete text of those comments is in the Management Comments section of this report.

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments on Finding and Audit Response

The Director, Interoperability, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, commented on the implementation of information assurance and the term "combat developers.

Implementation of Information Assurance. The Director stated that the Conclusion section of the report states that, "…information assurance must be implemented whenever a system is deemed interoperable…," and that the statement is offered as a given. However, he believed that the statement may tend to imply equality of the two related measures. The Director stated that an appropriate qualification might be, "Information assurance must be implemented appropriately and commensurate to the level of interoperability required."

Audit Response. We revised the report as suggested.

Combat Developers. The Director stated that the term "combat developers" was used in the Conclusion section of the report without defining it.

Audit Response. The term "combat developers" was defined in Appendix B, "Definitions of Technical Terms," of the report. To clarify the Conclusion section, we added a footnote to also define the term, which refers to the requirements generation process.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments on Finding

The Director, Architecture and Interoperability, Office of the ASD(C3I) suggested some editorial changes that we considered and made where deemed appropriate.

U.S. Joint Forces Command Comments on Finding and Audit Response

The Inspector General, USJFCOM commented on analyzing interoperability and information assurance, conducting analytical or quantitative modeling and simulation, analyzing ORD requirements, comparing the proposed system ORD against the ORDs of the systems with which it must interoperate, providing a joint perspective concerning interoperability and integration, and comparing requirement documents of proposed DoD systems within joint mission area architectures.

Interoperability and Information Assurance Analysis. The Inspector General stated that the paragraph stating that "The Commander, USJFCOM did not analyze interoperability and information assurance requirements in the operational and system architectures for DoD systems as part of the interoperability certification process for ORDs" does not accurately reflect the requirements review process at the USJFCOM and the required actions as directed by Chairman of the Joint Chiefs of Staff Instructions 3170.01B and 6212.01B. Further, USJFCOM does analyze interoperability and information assurance. Without overarching joint mission area architectures, USJFCOM analyzes integration requirements in coordination with Chairman of the Joint Chiefs of Staff Instructions 3170.01B and 6212.01B from known and existing systems as they integrate with existing CRDs.

Audit Response. As stated in the finding, the analysis of interoperability and information assurance requirements that the USJFCOM subject-matter experts performed for proposed DoD system's requirements should be made to ORD requirements for other systems that the proposed system will be interoperable with in their intended mission architectures in addition to those requirements contained in existing CRDs.

Analytical or Quantitative Modeling and Simulation. The Inspector General stated that USJFCOM did not compare ORDs to joint mission architectures before system development started because it did not have the resources to conduct that level of review. Although USJFCOM strongly disagrees that the depth of the ORD review as outlined in the report is a USJFCOM mission, USJFCOM would like to be able to conduct the reviews as outlined in the report, including detailed analysis.

Audit Response. In Section 922, Public Law 105-261, Congress expressed its sense that the commander of a combatant command should be provided with appropriate and sufficient resources for joint warfighting experimentation. It listed the responsibilities and authorities that should accompany that designation, including improving interoperability and making recommendations to the Chairman of the Joint Chiefs of Staff on mission needs statements and ORDs. Accordingly, if USJFCOM believes that resources are insufficient, it should request the resources needed to fulfill the sense of Congress.

ORD Requirements. The Inspector General stated that the requirement to review ORDs in context with the existing family of systems is not a USJFCOM requirement. Further, the ORD review process, as outlined in Chairman of the Joint Chiefs of Staff Instructions 3170.01B and 6212.01B, was to ensure that the new ORDs were interoperable with the future family of systems as outlined or described in the CRDs. The CRD details the future system requirements for the family of systems that include the current and potential innovation resulting from technology to be added. USJFCOM works with the ORD authors to ensure that the new ORDs are compliant with the CRDs. Further, the role of the CRDs is to serve as the road map to future interoperability, which is why Chairman of the Joint Chiefs of Staff Instructions 3170.01B and 6212.01B require the traceability of ORD requirements to CRD requirements and not to the current or existing systems within the particular family of systems. In addition, USJFCOM does realize that additional efforts are required to ensure interoperability and, with additional resources, would want to participate in those efforts. Additionally, DoD lacks a reliable repository of all existing family of systems information.

Audit Response. USJFCOM had not documented that it lacked:

- resources needed to fulfill its responsibility for assessing interoperability requirements for proposed DoD weapon systems or
- a reliable repository of all existing family of systems information.

USJFCOM should be proactive in acquiring additional resources to ensure the interoperability of systems and to establish a reliable repository of all existing family of systems information, as specified in Section 922, Public Law 105-261, discussed above.

Proposed System ORD Comparison. The Inspector General stated that subject-matter experts were not required or authorized to compare the proposed system ORD against the ORDs of the systems with which it must interoperate. Further, the development of ORDs was the excusive role of the Military Departments and Defense agencies and, even though USJFCOM did have a role in the review process, approval was the responsibility of the Joint Requirements Oversight Council. The report misinterpreted what the actual role of USJFCOM was in the process and grossly overstated the requirements for USJFCOM. However, USJFCOM did concur that, with additional resources, it could improve the interoperability effort in many areas; however, those areas were not its assigned tasks and were unfunded.

Audit Response. The USJFCOM has the authority to obtain additional resources to improve interoperability throughout DoD. The Joint Staff's "Unified Command Plan 1999," emphasizes the role of USJFCOM as the chief advocate of jointness and the importance of enhancing jointness and interoperability throughout DoD. As part of its role in transforming U.S. Armed Forces to meet the security challenges of the 21st century, USJFCOM has the responsibility to support the development and integration of fully interoperable systems and capabilities, including C4I surveillance and

reconnaissance. Further, the sense of Congress, as expressed in Section 922, Public Law 105-261 encourages a combatant commander, such as USJFCOM, to be proactive in obtaining appropriate and sufficient resources to fulfill its responsibility for assessing interoperability requirements of proposed DoD weapon systems to enable the warfighter to have interoperable systems.

Joint Perspective. The Inspector General suggested that another recommendation be added to Recommendation 4. Specifically, he proposed that the Director, Command, Control, Communications, and Computers Systems Directorate (J-6), Office of the Chairman of the Joint Chiefs of Staff:

> Provide a joint perspective as the Chairman's advocate for interoperability and integration, to team with the Joint Warfighting Capability Assessments (JWCAs) in developing Joint Mission Area Architectures.

The Inspector General suggested the new recommendation because joint mission area architectures are key to determining the usefulness of systems within DoD. Further, as the warfighters advocate for interoperability and integration, USJFCOM should participate in the architecture process to ensure that warfighter needs and interests are met.

Audit Response. The report did not address the merits of a joint perspective interaction with joint warfighting capability assessments when developing joint mission area architectures. However, we will consider addressing that joint perspective issue when reviewing interoperability and information assurance policies at the unified command level, in a subsequent audit.

Comparison of Requirement Documents. The Inspector General suggested that another recommendation be added to Recommendation 4. Specifically, he proposed that the Director, Command, Control, Communications, and Computers Systems Directorate (J-6), Office of the Chairman of the Joint Chiefs of Staff:

> Compare requirement documents of proposed DoD systems within JMA [joint mission area] Architectures, as they are completed, against the other requirement documents in their related Joint Mission Area Architecture to verify the completeness of stated interoperability requirements.

The Inspector General provided the same rationale for this recommendation as he gave for his recommendation to provide a joint perspective, as discussed above.

Audit Response. The report did not specifically address the comparison of requirement documents of proposed DoD systems within joint mission area architectures against the other requirement documents in their related joint mission area architecture(s). However, we will consider addressing that comparison issue when reviewing interoperability and information assurance policies at the unified command level, in a subsequent audit.

Defense Information Systems Agency Comments on Finding and Audit Response

The Inspector General, Defense Information Systems Agency commented on DoD interoperability policy, the Interoperability Watch List, inconsistent DoD policy, conformance with Joint Chiefs of Staff policy, interoperability analysis, access to the JCPAT database, and interoperability certification. In addition, the Inspector General suggested some editorial changes that we considered and made where deemed appropriate.

DoD Interoperability Policy. The Inspector General stated that DoD Directive 4630.5 and DoD Instruction 4630.8 establish DoD interoperability policy and that:

- the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics implemented its interoperability responsibilities in DoD Directive 4630.5 and DoD Regulation 5000.2-R, and

- the Joint Staff implemented its interoperability responsibilities in Chairman of the Joint Chiefs of Staff Instructions 3170.01B and 6212.01B.

Further, while ASD(C3I) was revising DoD Directive 4630.5, the Joint Staff rewrote Chairman of the Joint Chiefs of Staff Instruction 6212.01B, which incorporated the intended changes to DoD Directive 4630.5 before its release in January 2002. In addition, the ASD(C3I), as a staff element of the Office of the Secretary of Defense, should be a higher authority than the Joint Chiefs of Staff. Therefore, the Inspector General stated that the report criticism could be that DoD Directive 4630.5 and DoD Instruction 4630.8 were outdated because of developments in architecture frameworks and acquisition documents. Alternatively, one could say, with equal validity, that Chairman of the Joint Chiefs of Staff Instruction 6212.01B:

- was prematurely issued because it was in conflict with DoD Directive 4630.5 and DoD Instruction 4630.8 and

- lacked the authority of DoD Directive 4630.5 and DoD Instruction 4630.8 for the changes.

Audit Response. The Joint Chiefs of Staff were proactive. The Office of the ASD(C3I) guidance had not been updated for 10 years. As the Inspector General stated, DoD Directive 4630.5 and DoD Instruction 4630.8 were partially outdated because of developments in architecture frameworks and acquisition documents.

Interoperability Watch List. The Inspector General stated that DoD Instruction 4630.8 did not specifically require the Director, Operational Test and Evaluation to establish criteria for placing DoD weapon systems in the

development phase of the acquisition process on the Interoperability Watch List. Further, the Interoperability Senior Review Panel was addressing the process for the Interoperability Watch List and had identified a process for nominating systems to the list. The Inspector General also stated that systems had been nominated for the Interoperability Watch List, but none were actually put on the List to date.

Audit Response. As evidenced in the report, without specific criteria for placing DoD weapon systems on the Interoperability Watch List, the Office of the Secretary of Defense, the Joint Staff, the Defense agencies, and the Military Departments have not placed any DoD weapon systems on the List. This occurred even though the Director, Operational Test and Evaluation cited interoperability testing concerns for 21 DoD systems in the FY 2001 Annual Test Report.

Inconsistent DoD Policy. The Inspector General stated that the Defense Information Systems Agency did not believe that the DoD policy is inconsistent, but rather that the release dates for revision of the various documents were not as coordinated as possible. Further, the contents of the various documents were coordinated and are now synchronized and undergoing another review and update cycle.

Audit Response. Whether or not the release dates for revision of the various documents were coordinated, DoD Directive 4630.5 and DoD Instruction 4630.8 were outdated because of developments in architecture frameworks and acquisition documents over the 10-year period between document updates.

Conformance with Joint Chiefs of Staff Policy. The Inspector General stated that Joint Chiefs of Staff policy and instruction should conform to ASD(C3I) guidance, not the other way around.

Audit Response. We agree; however, the Joint Staff was proactive in implementing agreed-upon policy needed because of developments in architecture frameworks and acquisition documents.

Interoperability Analysis. The Inspector General recommended revising the report's statements about the interoperability process because the ORD review process requires the originator to identify a proposed system's interoperability requirements in the context of the other systems with which it must interoperate.

Audit Response. Combat developers have neither a complete database of all DoD requirement and acquisition documents nor access to all joint mission area architectures to use as a reference when developing ORD interoperability requirements. Accordingly, USJFCOM has an important role in ensuring that interoperability requirements are fully defined in the ORD review process.

Access to JCPAT Database. The Inspector General stated that the third sentence under the subheading, "Access to Database," indicated that of 756 users, 15 were contractor support personnel, and that the fourth sentence

indicated that DISA could identify the total number of users but could not distinguish DoD from contractor personnel. He concluded that both statements could not be correct.

Audit Response. The Inspector General was citing statements from the discussion draft of this report, not the draft report. We revised those statements before issuing the draft report.

Interoperability Certification. The Inspector General stated that the phrase, "interoperability certification," is ambiguous. Further, he stated that the Joint Staff issues interoperability certifications of requirements and supportability documents, which are two separate types of certifications, and issues system validation memoranda. He also stated that JITC issues system interoperability test certifications based on interoperability testing.

Audit Response. Page 4, Footnote 2, of the report discussed the two separate types of interoperability certifications. In response to the management comments, we added the term, "Interoperability Certification Process," to Appendix B, "Definitions of Technical Terms."

Joint Staff Comments on Finding and Audit Response

The Director, Joint Staff commented on analyzing interoperability and information assurance requirements; updating the Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool (JCPAT); conducting analytical or quantitative modeling and simulation; analyzing ORD requirements; comparing the proposed system ORD against the ORDs of the system with which it must interoperate; developing the Automated Commander-in-Chief Integrated System Tool; and maintaining the database. In addition, the Director suggested some editorial changes that we considered and made where deemed appropriate.

Interoperability and Information Assurance Analysis. The Director provided comments similar to those made by the Inspector General, USJFCOM, for which we previously provided an audit response.

JCPAT. The Director stated that the USJFCOM did not update the JCPAT database to include all interoperability certifications, TEMPs, and C4I support plans for DoD systems because those documents were in hard copy form and, therefore, impede interoperability certification. Further, the Director stated that the Joint Staff J-6 maintains a hard copy of programs and documents that predate the JCPAT.

Audit Response. As indicated in the finding, the older documents in the JCPAT should be archived and all applicable documents should be incorporated into the JCPAT. Archiving and incorporating documents is important because other organizations outside the Joint Staff use the JCPAT to ensure that all information exchange requirements are encompassed in ORDs. Therefore, the

JCPAT data need to be complete and accessible. The inclusion of C4I support plans and TEMPs in the JCPAT database would help combat developers to more fully review and determine system interoperability requirements.

Analytical or Quantitative Modeling and Simulation. The Director provided comments similar to those made by the Inspector General, USJFCOM, for which we previously provided an audit response.

ORD Requirements. The Director provided comments similar to those made by the Inspector General, USJFCOM, for which we previously provided an audit response.

Proposed System ORD Comparison. The Director provided comments similar to those made by the Inspector General, USJFCOM, for which we previously provided an audit response.

Automated Commander-in-Chief Integrated System Tool. The Director stated that the recommended Automated Commander-in-Chief Integrated System Tool was under development, and DoD had not accepted, approved, or certified it. Further, he stated that USJFCOM could evaluate the usefulness of this or any other tool that USJFCOM uses in the requirements process.

Audit Response. The report discusses the Automated Commander-in-Chief Integrated System Tool only as a possible automated process to assist USJFCOM in evaluating interoperability requirements in proposed ORDs.

Maintenance of the Database. The Director suggested revising the sentence that discusses searching for interoperability certification documents in the JCPAT database. He stated that the reason for the revision was because requirements documents were submitted at each milestone. Further, the Director stated that depending upon the milestone, a particular program may have more than one document. He also stated that a reviewer would have to be aware of the milestone and the date processed to determine the current document. However, the Director stated that the Joint Staff agreed that the user could not be assured that the document is the most recently approved or validated document for Acquisition Category II and below documents. Further, he stated that, because the Joint Requirements Oversight Council was a validating authority, the Director, Force Structure, Resources, and Assessment (J-8) post-validated Acquisition Category I or Joint Staff Issue programs to the J-8 tool. The Director also stated that the validated documents are available in both the J-6 and J-8 tools. In conclusion, he stated that recent changes to the J-6 JCPAT should alleviate the confusion concerning the availability of up-to-date program documentation in the JCPAT database.

Audit Response. Even though the Director stated that the validated documents are available in the J-6 and J-8 tools and that recent changes to the J-6 JCPAT should alleviate the confusion concerning the availability of up-to-date program documentation, the user needs assurance that the document located in the JCPAT database is the most recently certified document. Therefore, DISA

needs to archive outdated versions of documents so that users can locate and obtain the most up-to-date approved documents for making interoperability determinations for DoD systems.

Interoperability Senior Review Panel Comments on Finding and Audit Response

The Co-Chair, Interoperability Senior Review Panel stated that the Interoperability Senior Review Panel consists of senior leaders from the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the ASD(C3I); the Joint Staff; U.S. Joint Forces Command; the Director for Programs, Analysis, and Evaluation; and the Director, Operational Test and Evaluation. He recognized that the primary objective of this report was to evaluate the Office of the Secretary of Defense and the Defense agencies' implementation of DoD interoperability and information assurance policies, but he stated that the report did not address the issue that DoD is not structured to organize, train, and equip required joint capabilities. The Co-Chair also stated that the Military Departments determine requirements and then resource those requirements based on their individual priorities instead of joint priorities. Further, the Co-Chair stated that interoperability and information assurance for information technology and national security systems should be viewed in the wider context of doctrine, organization, training, material, leadership development, personnel, and facilities instead of only system of systems context or family of systems context, or both. He concluded that joint interoperability requires a synchronized effort and resources across the entire doctrine, organization, training, material, leadership development, personnel, and facilities spectrum.

Audit Response. As the Co-Chair noted, the report did not address whether DoD is structured to organize, train, and equip required joint capabilities. However, we will consider addressing that structuring issue in a subsequent audit when we review interoperability and information assurance policies at the unified command level. Because certain recommendations required a synchronized effort and resources, we redirected those recommendations to the Co-Chair to coordinate corrective actions to implement policies.

Appendix J. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Deputy Under Secretary of Defense (Acquisition Initiatives)
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff
    Director for Command, Control, Communications, and Computers Systems (J-6)
    Director for Force Structure, Resources, and Assessment (J-8)

Department of the Army

Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Unified Command

Commander, U.S. Joint Forces Command

Other Defense Organizations

Director, Defense Information Systems Agency
    Commander, Joint Interoperability Test Command

Non-Defense Federal Organization

Office of Management and Budget
Office of Information and Regulatory Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

Final Report Reference

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION, TECHNOLOGY AND LOGISTICS

August 14, 2002

MEMORANDUM FOR DOD INSPECTOR GENERAL
ATTN: AUDIT FOLLOW-UP

THROUGH: Director, Acquisition Resources and Analysis 8/20/02

SUBJECT: Draft Audit Report No. D2002AE-0009 "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapons Systems", July 19, 2002

This is in response to your memorandum dated July 19, 2002, requesting comments on the subject audit report.

- Conclusions, Page 15, Line 7:

  "…information assurance must be implemented whenever a system is deemed interoperable…."

  - is offered as a given; however, as stated without appropriate qualification, may tend to imply equality of the two related measures.

  - an appropriate qualification might be, "Information assurance must be implemented appropriately and commensurate to the level of interoperability required."

Revised Page 15

- Conclusions, Page 15, Line 11

  You have used the term "combat developers" without defining it. If you are referring to program managers, then the reference is incorrect. PMs should not interpret requirements. They are set by the Requirements Generation Process. If you are referring to the requirements groups in the services or Joint Staff, then the activity is already being accomplished.

Revised Page 15

- Recommendation 1, Page 16:

  The wording "in coordination with" can be construed to give the ASD(C3I) primacy over AT&L and the Joint Staff in integrating revisions to all documents related to interoperability (CJCSI 3170, 6212, DoD 5000 & DoD 4630.) Each of these organizations is responsible for one or more of these documents.

Revised Page 17

Therefore recommend the words "in coordination with" be changed to "jointly with", or rewrite the first four lines to read "We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence); the Under Secretary of Defense for Acquisition, Technology, and Logistics; and Chairman of the Joint Chiefs of Staff jointly implement…."

Dr. V. Garber
Director, Interoperability
OUSD(AT&L)

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

August 19, 2002

MEMORANDUM FOR THE DOD INSPECTOR GENERAL

SUBJECT: Management Comments to DOD IG Audit Report on "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems (Project No. D2002AE-0009)"

This office has reviewed the subject Audit Report and concurs overall with its findings and recommendations. The Audit report accurately assesses Department of Defense progress in implementation of interoperability and information assurance policies within the DoD. Provided below are our management comments regarding the specific findings and recommendations, relevant to the Assistant Secretary of Defense (Command, Control, Communications), for this audit:

Recommendation 1. This office concurs with this recommendation and will work with the Office of the Under Secretary of Defense for Acquisition Technology and Logistics (OUSD (AT&L)) and the Joint Staff to implement a process for timely revision and synchronization of DoD policies regarding interoperability and information assurance. We will use the Interoperability Senior Review Panel (ISRP) to coordinate the annual review, synchronization and revision, if required, for the following policies and implementing instructions impacting interoperability: DoDD 4630.5, DoDI 4630.8, CJCSI 3170.01, and CJCSI 6212.01. The ISRP will also be used to ensure consistency of the above interoperability/requirement policies with the 5000 series policy documents for acquisition; and DoDI 5200.40 and CJCSI 6510.01 policies for information insurance.

Recommendation 2. This office will continue to work with the ISRP membership to refine the process for identifying programs with interoperability deficiencies and their nomination as candidates for the Interoperability Watch List. As the IWL is a relatively new oversight tool, we are still in the formative stages of developing appropriate criteria and procedures for placing programs on the IWL. This last year, the Air Force's Situational Awareness Data Link (SADL) program was pursued as initial pilot case for nomination to the IWL. The lessons learned from this pilot will be applied as we to continue to explore other programs for IWL consideration. We are also working with OUSD (AT&L), DOT&E and the Joint Staff to develop procedures for addressing interoperability deficiencies within existing processes and fora prior to consideration by the ISRP for the IWL.

Recommendation 3. This office agrees with the underlying premise of this recommendation. However, we believe it misses the essential point that the Joint Mission Areas and subordinate supporting mission areas must first be defined by the Joint Staff and mission area integrated architectures developed by DoD Components before Joint Forces Command can conduct an effective comparative analysis operational requirements. Further, DoDI 4630.8 assigns the Joint

Staff the responsibility to "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." Once JMAs and subordinate mission areas are defined, the Joint Staff must coordinate with the DoD Components to ensure we develop a consistent and integrated set of mission area integrated architectures across DoD Services and Agencies. We propose that a specific recommendation be made in this audit report for the Joint Staff to further refine existing JMAs and define applicable subordinate mission areas to serve as the basis for development of mission area integrated architectures by DoD Components.

Attached are additional editorial comments to this audit report for your consideration. Should you have any questions regarding our response to this audit, please feel free to contact either Mr. Jack Zavin at (703) 607-0238 (jack.zavin@osd.mil) or Mr. Kris Strance at (703) 607-0249 (kris.strance@osd.mil).

John L. Osterholz
Director
Architecture & Interoperability

Attachment:
Additional Comments to Audit Report

Final Report Reference

DOD IG Audit Report on Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems (Project D2002AE-0009

#	Page	**Paragraph**	Component	**Critical Substantive Editorial**	Comments	Final Report Reference
1	i	Results	ASD (C3I) A&I Directorate	**Substantive**	Change wording in the second sentence from: "...using an architecture view..." to: "...using a mission area integrated architecture..."	Revised Page i
2	5	3	ASD (C3I) A&I Directorate	**Substantive**	Change wording in the last sentence from: "...through interoperability may have consolidated..." to: "...through interoperability appears to have consolidated...".	Page 5
3	8	2	ASD (C3I) A&I Directorate	**Substantive**	Add the following after the last sentence: "While the appropriate tools are necessary to conduct a credible assessment, the nature of the JMA's as defined by the Joint Staff in JROC Memo CM-1014-00, of 6 September 2000 are very high level and may contribute to the difficulties analyzing specific ORD interoperability requirements against joint mission architectures. The refinement of the JMAs and the definition by the Joint Staff of subordinate mission areas that support the high level JMAs is required to form a more complete mission area integrated architecture upon which to base ORD interoperability assessments."	Revised Page 8
4	12	2	ASD (C3I) A&I Directorate	**Substantive**	Delete the second sentence. And replace with the following: "The IWL is a relatively new oversight tool and appropriate criteria for nominations are being developed. The Interoperability Senior Review Panel has been working to develop procedures for addressing interoperability deficiencies within existing processes prior to consideration for potential IWL nomination.	Page 12
5	15	2	ASD (C3I) A&I Directorate	**Substantive**	Add the following after the last sentence: " Refining the JMAs, defining subordinate joint mission areas and consistent development and management of mission area integrated architectures by the DoD Components as described in the recently revised DoDD 4630.5 and DoDI 4630.8 represents a positive step by the Department of Defense in meeting this challenge"	Page 15

1

Final Report Reference

Page 22

#	Page	**Paragraph**	Component	**Critical Substantive Editorial**	Comments
6	16	3	ASD (C3I) A&I Directorate	**Substantive**	Insert a new paragraph after paragraph 2 as follows: "We recommend that the Chairman of the Joint Chiefs of Staff further refine existing JMAs and define applicable subordinate mission areas to serve as the basis for development of mission area integrated architectures by DoD Components".

2

U.S. Joint Forces Command Comments

DEPARTMENT OF DEFENSE
COMMANDER IN CHIEF
U.S. JOINT FORCES COMMAND
1562 MITSCHER AVENUE SUITE 200
NORFOLK, VA 23551-2488

IN REPLY REFER TO:

Ser J00IG/2U9750
19 Aug 02

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Subject: Report on the Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon System (Project No. D2002AE-0009)

1. The Draft DoD Inspector General Audit Report on Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapons System has been reviewed. U.S. Joint Forces Command does not concur with subject report. The attachment contains USJFCOM comments and recommended changes.

2. If you have questions, please contact my Audit Liaison, YN2 Thaddeus D. Spain at (757) 836-5940 or DSN 836-5940.

GERALD B. EVANS
Colonel, U.S. Air Force
Inspector General

Attachment:
Recommended changes to Report on the Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon System (Project No. D2002AE-0009)

Final Report Reference

Revised Page 21

Page 23

Page 4

Page 8

Recommended Changes to Report on the Implementation of the Interoperability and Information Assurance Policies of DoD Weapons System (Project No. D2002AE-009)

ORG	Page #	Para #	Line #	Class	Comments	A/R/P
JFCOM J86	GEN			U	**Critical:** Recommendation: As drafted, the DoD IG recommendation is not actionable without Joint Staff completion of the Joint Mission Area (JMAs) architectures. The JFCOM recognizes that the development of the Joint Mission Area Architectures is critical to compare requirements across programs. We will continue to press this need separately and collectively in all available forums. Further, the quantification analysis and predictive tools recommendation is also not fully actionable at this time. Although the software tools referenced in the report are under JFCOM assessment and show potential, it must be officially accredited by OSD and the JS for the verification of joint interoperability requirements in mission area architectures. Rationale: Correctness.	
JFCOM J6 & J86	4	Adequacy of the Interoperability and Information Assurance Process Sub- Paragraph 2		U	**Critical**: Recommendation: Change the paragraph as follows: "The Commander, USJFCOM ~~did not analyze information assurance requirements in the operations and system architectures for DoD systems as part of the interoperability certification process for operational requirements documents (ORDS)~~ does analyze interoperability and information assurance. However, without overarching Joint Mission Area architectures, integration requirements in coordination with CJCSI 3170.01 and CJCSI 6212.01B are analyzed from known and existing systems and as they integrate with existing CRDs." Rationale: The paragraph as written does not accurately reflect the requirements review process at JFCOM and the required actions as directed by CJCSI 3170.01 and CJCSI 6212.01.	
JFCOM J6	8	Interoperability Requirements		U	**Critical**: Recommendation: Change the paragraph as follows: " ...did not have the analytical or quantitative modeling and	

1

Attachment

Final Report Reference

Recommended Changes to Report on the Implementation of the Interoperability and Information Assurance Policies of DoD Weapons System (Project No. D2002AE-009)

& J86					simulation tools or the resources to conduct that level of review. USJFCOM does review the interoperability of individual system ORDs within the framework of Family of Systems in existing Capstone Requirements Documents and known systems outside of those ORDs in accordance with the requirements of CJCSI 3170.01 and CJCSI 6212.01." Rationale: Accuracy – while USFJCOM would like to be able to conduct the reviews as outlined in the existing paragraph (although we strongly disagree that the depth of the ORD review as outlined in the report is currently a USJFCOM mission) to include detailed analysis JFCOM does not have the resources (manpower and test bed) at this time to do that.	
JFCOM J6 & J86	8	Interoperability Analysis		**U**	**Critical**: Recommendation: Delete the following sentences: " ... contains interoperability KPPs and information exchange requirements. ~~However, the USJFCOM did not analyze the ORD requirements of a proposed DoD system within the context of ORD requirements of other systems with which a proposed DoD system must operate and exchange information. Instead of analyzing the ORDs that the system will interoperate with, the USJFCOM stated that it reviews ORDs within the context of CRDs and measures interoperability and integration requirements against ORDs that relate to CRDs and against other known DoD systems outside the CRDs.~~ ..." Rationale: Accuracy. The above requirement in the report, to review ORDs in context with the existing family of systems, **is not a JFCOM requirement**. The current ORD review process, as outlined in CJCSI 6212.01 and CJCSI 3170.01, is to ensure the new ORDs interoperability with the future family of systems as outlined/described in the CRDs (the CRD details the future system requirements for the family of systems that include the current and potential innovation resulting form technology to be added). JFCOM works with the ORD authors who come under the respective JFCOM CRDs to ensure that those ORDs are compliant, as appropriate and applicable, with the CRDs.	

Page 8

2

Attachment

Final Report Reference

Recommended Changes to Report on the Implementation of the Interoperability and Information Assurance Policies of DoD Weapons System (Project No. D2002AE-009)

					The report appears to not understand what the role of the CRDs is to serve as the road map to future interoperability (that is why CJCSI 3170.01 and CJCSI 6212.01 require the traceability of ORD requirements to the CRDs requirements) and not to the current/existing systems within the particular family of systems. JFCOM does realize that additional efforts are required to insure interoperability and, with additional resources, would want to participate in those efforts. However, currently **USJFCOM is accomplishing** what it is directed to do in CJCSI 3170.01 and CJCSI 6212.01. Additionally, the DoD lacks a reliable repository of all existing family of systems information.	
Page 9 JFCOM J6 & J86	9	Interoperability Review Assessment		**U**	**Critical:** Recommendation: Change the paragraph as follows: "... however, the subject -matter experts do not compare the proposed system ORD against the ORDs of the system it must be interoperable with, ~~even if required,~~ because they do not have the necessary analytical, quantitative modeling and simulation tools, personnel, or the authority to determine whether the ORD is appropriate for the operational or systems architecture. Rationale: There is no requirement for USJFCOM to do as the author recommends and there is no authority for JFCOM to do this. The development of ORDs is the solely the role of the services and agencies and while JFCOM does have a role in the review process (IAW CJCSI 3170.01 and CJCSI 6212.01) the approval rests with the JROC. The statement is overall is **very misleading** and does not in fact accurately represent this process. The author is again misinterpreting what the actual role of JFCOM is in the process and is grossly overstating the requirements for JFCOM. We again do concur that with additional resources there are many areas where JFCOM could improve the interoperability effort, but these are areas that are currently not our assigned tasks and are unfunded.	
Page 21 JFCOM	1	Recommendations		**U**	**Critical**: Recommendation: Add the new paragraph: " Joint	

3

Attachment

Final Report Reference

Recommended Changes to Report on the Implementation of the Interoperability and Information Assurance Policies of DoD Weapons System (Project No. D2002AE-009)

J6 & J86	6	New paragraph 3			Forces Command is currently only required and resourced to review ORDs as a standalone document for compliance with the CRDs and to provide a joint perspective. We recommend additional resources be provided to JFCOM to enable a more in depth review of the ORDs for their interoperability within their respective family of systems." Rationale: JFCOM is currently unfunded/resourced to execute either recommendation 3a or 3b.	
JFCOM J6	16	Recommendations Paragraph 3a		U	**Substantive**: Recommendation: Change the sentence as follows: Compare the operational requirements documents of proposed DoD systems within JMA architectures, as they are completed, against the other operational requirements documents in the related joint mission area architecture ..." Rationale: Accuracy	Revised Page 21
JFCOM J86	16	Recommendations Paragraph 4a		U	**Critical:** Recommendation: Add a new paragraph and make it paragraph 4a as follows: "Provide a joint perspective as the Chairman's advocate for interoperability and integration, to team with the Joint Warfighting Capability Assessments (JWCAs) in developing Joint Mission Area Architectures." Rationale: JMA Architectures are key to determining the utility of systems within DoD. As the Warfighters advocate for interoperability and integration, USJFCOM should participate in the architecture process to insure warfighter needs and interests are met.	Page 58
JFCOM	16	Recommendations Paragraph		U	**Critical:** Recommendation: Change paragraph 4a to paragraph 4b and change the wording to read, "Compare requirement documents of proposed DoD systems within JMA Architectures, as they are completed, against the other requirement documents in their related Joint Mission Area Architecture to verify the completeness of stated interoperability requirements." Rationale: JMA Architectures are key to determining the utility of systems within DoD. As the Warfighters advocate for interoperability and integration, USJFCOM should participate	Page 58

4

Attachment

Final Report Reference

Page 23

Recommended Changes to Report on the Implementation of the Interoperability and Information Assurance Policies of DoD Weapons System (Project No. D2002AE-009)

					in the architecture process to insure warfighter needs and interests are met.	
JFCOM	16	Recommendations Paragraph		U	**Critical:** Recommendation: Add the following language to the end of paragraph 5, "and the director, Intelligence, surveillance and Reconnaissance (J2):" Rationale: Completeness	

5

Attachment

Director, Operational Test and Evaluation, Comments

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST AND EVALUATION

AUG 2 3 2002

MEMORANDUM FOR THE DOD INSPECTOR GENERAL

SUBJECT: DoD IG Audit Report on "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems (Project No. D2002AE-0009)"

I appreciate the opportunity to review and comment on the subject report. It provides a fair representation of the challenges the Department of Defense faces in coordinating interoperability activities across the Office of the Secretary of Defense, the Joint Staff, and US Joint Forces Command. However, I would like to offer the following comments on the findings and recommendations.

Recommendation 2. Partially concur. As a member of the Interoperability Senior Review Panel (ISRP), DOT&E continues to work with the other members on refining the Interoperability Watch List (IWL) processes. The Watch List is one of many tools available within the Department to address interoperability problems. The IWL policy states the list will be used for those systems with interoperability issues that are not being adequately addressed by other forums. I believe the ISRP has served a valuable role over the last 18 months in coordinating interoperability policies and actions across the Department and working within existing forums to solve issues. For example, the ISRP worked with OUSD (AT&L) AS&C to ensure interoperability is stressed within ACTDs to avoid problems as these experimental items transition to the force. The interoperability concerns raised by the ISRP on the Air Force Situational Awareness Data Link were key inputs for the OASD (C3I) Joint Tactical Radio System waiver process. The criteria for IWL candidates suggested by the report are certainly a start, and DOT&E and the ISRP will use these as a means to evaluate future candidates. The report also cites the DOT&E Annual Report to Congress as a source of systems for the IWL. Although I believe these programs are already receiving adequate attention through T&E oversight and other acquisition review processes, if a program on T&E Oversight is not adequately addressing interoperability, I will bring it to the ISRP for consideration.

Recommendation 5. Partially concur. I agree that testing of interoperability and information assurance takes on more critical status as we continue to transform into a network centric force. The DOT&E already ensures interoperability is tested to support the assessment of Key Performance Parameters provided in the Operational Requirements Documents, and published policy in 1999 for testing information assurance. In 2000, DOT&E conducted an assessment in response to study recommendations by the Defense Science Board, to determine requirements for interoperability testing of systems within the scope of a larger networked system of systems linked over the Global Information Grid (GIG). As a result of this effort and similar initiatives by OUSD (AT&L) and the Joint Staff, the Department funded an initial capability called the Joint Distributed Engineering Plant (JDEP) in the FY02 POM. I believe the

objective JDEP capability will permit DOT&E to do the testing called for in this recommendation. However, expanded funding for JDEP is needed over the POM before it will provide the full scope called for in this recommendation.

Interoperability and information assurance are key enablers for the future. I look forward to working with you and your staff on the follow-on reports.

Thomas P. Christie
Director

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

IN REPLY
REFER TO: INSPECTOR GENERAL (IG) 19 August 2002

MEMORANDUM FOR Department of Defense Inspector General

SUBJECT: Draft Report, Audit of Implementation Interoperability and Information Assurance Policies for Acquisition of DOD Weapon Systems, D2002AE-0009, FOUO

1. The enclosed document provides the response from the Defense Information Systems Agency on the subject Draft report.

2. The points of contact for this action are Liz Lippmann, Audit Liaison, at 703.607-6306 or Teddie Steiner, Audit Liaison, at 703.607-6316.

FOR THE DIRECTOR:

Enclosure a/s

for RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

Final Report Reference

Page 4

Page 5

JITC COMMENTS ON D2002AE-0009

Document page 4, first bullet item:

Background: DoD Interoperability Policy is set by DoDD 4630.5 and DoDI 4630.8. DoD Regulation 5000.2-R implements the AT&L responsibilities of 4630 while CJCSI 6212 and 3170 implement the Joint Staff responsibilities. CJCSI 6212.01B was in re-write while 4630 was being revised and incorporated the intended changes to 4630 prior to its release in Jan 02.

Draft discussion says 1992 version of ASD(C3I) DODI 4630.8 was inconsistent with CJCSI 6212.01B. Appears to be attribution of inconsistency to the wrong source. ASD(C3I), as a staff element of OSD, should be a higher authority than the JCS. Hence, criticism could be that 4630 series were outdated, given developments in architecture frameworks and acquisition documents. Alternatively, one could with equal validity say that 6212.01B, in so far as it was in conflict with 4630 series, was prematurely issued, lacking the authority of the 4630 series for the changes.

Document page 5, fourth bullet item:

Technically, 4630.8 does not require DOT&E to establish criteria. Specifically, it states:

> "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."
>
> The IWL process is being addressed by the Interoperability Senior Review Panel (ISRP) and there is a process identified for nominating systems to the list. POC for the ISRP would be Ms. Susan Wright (Susan.Wright@osd.mil). Systems have been nominated for the list, but none have been actually put on the list to date.

Final Report Reference

Document page 5, 'Interoperability Policy':

Page 5

Recommend re-wording to "The DoD CIO established policy guidance concerning interoperability for requirements generation, acquisition and complete life-cycle of a system. USD (AT&L) established the implementation guidance for system acquisition and the Joint Staff established the implementation guidance for requirements certification, supportability certification and system interoperability test certification." Rationale: More complete.

Document page 5, 'Joint Staff Policy':

Revised Page 5

Last sentence: "Further, DISA and the JITC are to certify test results for all interoperability system tests." More correctly should be "DISA/JITC." JITC is to certify results, and is, in fact, designated sole certifier of such results for the DOD.

Document page 6, 'Inconsistent Policy':

Page 7

Sentence should be revised in line with the comments to page 4 and 5 above. We do not believe that the DoD policy is inconsistent, but rather that the revisions of various documents were not as coordinated with respect to their release dates as possible. The various documents were coordinated as to content. They are now in synchronization and are undergoing another review/update cycle.

Document page 7, 'Revisions to Guidance':

Page 7

Same problem as identified in first comment. JCS policy and instruction should conform to OSD guidance, not the other way around.

Document page 8, 'Interoperability Analysis':

Page 8

Recommend revising since the ORD review process does require the originator to identify the system's interoperability requirements in the context of other systems and thereby creates a review of system A requirements vs. system B, C and other requirements.

Document page 10, 'Maintenance of the Database':

Page 10

Final Report Reference

States that "...the JCPAT is a historical database that lists all DoD systems undergoing interoperability certification or that have been certified for interoperability." Recommend that this be revised to read "...the JCPAT is a historical database that lists all DoD systems undergoing interoperability requirements certification or that have had their interoperability requirements documents certified." Rationale: More accurate as the JCPAT is a repository of interoperability requirements documents.

Page 11

Document page 10, 'Access to Database':

Third sentence says 756 users, 15 contractor support personnel. Fourth sentence says DISA could identify total number of users, but could not distinguish DOD from contractor personnel. Both statements cannot be correct as they stand.

Revised Page 4

Document page 11, first bullet item:

Phrase 'interoperability certification' is ambiguous. The JS issues interoperability certifications of requirements and supportability documents (two separate types of certifications), and issues system validation memoranda. JITC issues system interoperability test certifications based on interoperability testing.

Page 29

Document page 18, last sentence:

Paragraph deals entirely with information assurance issues. End of last sentence reads: "... to verify that the systems had an information assurance strategy and were certified." Correct term to reflect approval is "...to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk" with respect to DITSCAP procedures is 'accredited' vice 'certified.'

Revised Page 64

Document page 48:

Distribution: Should read Commander, Joint Interoperability Test Command

Joint Staff Comments

THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-0300

DJSM-806-02
03 September 2002

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Subject: Report on the Implementation of Interoperability and Information Assurance Policies for Acquisition of DOD Weapon Systems (Project No. D2002AE-0009)

1. Thank you for the opportunity to review and comment[1] on the subject draft report. I concur subject to incorporation of the enclosed comments.

2. The Joint Staff point of contact is Lieutenant Colonel Scott Hoffman, 614-7004.

JOHN P. ABIZAID
Lieutenant General, USA
Director, Joint Staff

Enclosure

Reference:
1 DOD IG memorandum, 19 July 2002, "Report on the Implementation of Interoperability and Information Assurance Policies for Acquisition of DOD Weapon Systems (Project No. D2002AE-0009)"

Final Report Reference

ENCLOSURE

JOINT STAFF COMMENTS ON REPORT ON THE IMPLEMENTATION OF INTEROPERABILITY AND INFORMATION ASSURANCE POLICIES FOR ACQUISITION OF DOD WEAPON SYSTEMS (PROJECT NO. D2002AE-0009)

Page 4

1. Page 4, 2d bullett. Change as follows: "The Commander, USJFCOM ~~did not analyze interoperability and information assurance requirements in the operational and system architectures for DoD systems as part of the interoperability certification process[2] for operational requirements documents (ORDS)[3]~~ does analyze interoperability and information assurance. However, without overarching Joint Mission Area architectures, integration requirements in coordination with CJCSI 3170.01 and CJCSI 6212.01B are analyzed from known and existing systems as they integrate with existing CRDs."

REASON: The paragraph does not accurately reflect the requirements review process at USJFCOM and the required actions as directed by CJCSI 3170.01 and CJCSI 6212.01.

Page 4

2. Page 4, 3d bullet. Change as follows: "The Director, Command, Control, Communications, and Computer Systems Directorate (J-6) (the Joint Staff J-6) had not updated the Joint Command, Control, Communications, Computer, and Intelligence Program Assessment Tool (JCPAT) database ~~to include all interoperability certifications' Test and Evaluation Master Plans (TEMPs); and Command, Control, Communications, and Intelligence (C3I) support plans for DoD sytems~~ with documents that pre-date JCPAT. Because these documents are in hard copy form, they do not facilitate interoperability certification."

REASON: In response to the statement that JCPAT did not include all interoperability certifications, it should be noted that there are certified documents and programs that pre-date JCPAT. The Joint Staff J-6 maintains a hard copy of programs and documents that pre-date JCPAT.

Page 8

3. Page 8, Interoperability Requirements, 1st paragraph, second sentence. Change as follows: "...and making recommendations to the Chairman of the Joint Chiefs of Staff on ~~mission need statements and operational requirements documents~~ requirement documents."

REASON: These recommendations apply to all requirement documents. All references to operational requirements documents (ORDs) in this report should be changed to read requirement documents.

Enclosure

Final Report Reference

4. Page 8, Interoperability Requirements, 1st paragraph, last sentence. Change as follows: "...did not have the analytical or quantitative modeling and simulation tools or the resources to conduct that level of review. USJFCOM does review the interoperability of individual system ORDs within the framework of Family of Systems in existing Capstone Requirements Documents and known systems outside of those ORDs in accordance with the requirements of CJCSI 3170.01 and CJCSI 6212.01."

Page 8 Paragraph 2

REASON: Accuracy. While USFJCOM would like to conduct the reviews as outlined in the existing paragraph (USJFCOM disagrees that the depth of the ORD review as outlined in the report is currently a USJFCOM mission), to include detailed analysis, USJFCOM does not have the required resources (manpower and test bed).

5. Page 8, 2d paragraph. Change as follows: "...contains interoperability KPPs and information exchange requirements. ~~However, the USJFCOM did not analyze the ORD requirements of a proposed DoD system within the context of ORD requirements of other systems with which a proposed DoD system must operate and exchange information. Instead of analyzing the ORDs that the system will interoperate with, the USJFCOM stated that it reviews ORDs within the context of CRDs and measures interoperability and integration requirements against ORDs that relate to CRDs and against other known DoD systems outside the CRDs~~."

Page 8 Paragraph 3

REASON: Accuracy. The above requirement in the report, to review ORDs in context with the existing family of systems, is not a USJFCOM requirement. The current ORD review process, as outlined in CJCSI 6212.01 and CJCSI 3170.01, is to ensure the new ORDs interoperate with the future family of systems as outline and described in the CRDs (the CRD details the future system requirements for the family of systems that include the current and potential innovations resulting form technology to be added). USJFCOM works with the ORD authors to ensure that those ORDs are compliant, as appropriate and applicable, with the Capstone requirements documents (CRDs). The role of the CRDs is to serve as a road map to future interoperability (that is why CJCSI 3170.01 and CJCSI 6212.01 require the traceability of ORD requirements to CRDs requirements) and not to current and existing systems within the particular family of systems. USJFCOM does realize that additional efforts are required to insure interoperability and, with additional resources, would participate in those efforts. However, it is accomplishing what was directed under CJCSI 3170.01 and CJCSI 6212.01.

Final Report Reference

Page 9

6. Page 9, Interoperability Review Assessment, 2d sentence. Change as follows: "However, the subject matter experts do not compare the proposed system ORD against the ORDs of the system it must be interoperable with, ~~even if required,~~ because ~~they do not have~~ the necessary analytical, quantitative modeling and simulation tools have not been approved or provided. Although USJFCOM has the responsibility to recommend ORD changes that enhance interoperability, USJFCOM has neither the personnel or the authority to determine whether the ORD is appropriate for the operational or systems architecture.".

REASON: There is no requirement or authority for USJFCOM to do as the author recommends. The development of ORDs is solely the role of the Services and agencies. While USJFCOM does have a role in the review process (CJCSI 3170.01 and CJCSI 6212.01) the approval rests with the JROC. The statement as drafted is misleading and does not accurately represent the Joint Staff-supported process. The actual role of USJFCOM is only within the process.

Page 9

7. Page 9, Tools paragraph. Comment: The recommended tool is under development. It is not DOD accepted, approved or certified. USJFCOM could evaluate the utility of this or any other tool with respect to the role that USJFCOM performs in the requirements process prior to approving any language this specific.

Page 10

8. Page 10, Maintenance of the Database, 2d paragraph, 1st sentence. Change as follows: "When searching for ~~interoperability certification documents in the JCPAT,~~ ACAT II or below documents, a user ~~could not be assured that the document located~~ must be aware of the correct milestone for the program to determine the most ~~recently~~ recent certified document."

REASON: Requirements documents are submitted at each milestone. Depending upon the milestone, there may be more than one document on a particular program. A reviewer would have to be aware of the milestone and the date processed to determine the current document. We agree that the user cannot be assured that the document is the most recently approved or validated document. However, this is only true for ACAT II and below documents. Since the Joint Requirements Oversight Council is a validating authority, the J-8 post-validated ACAT I or JSI programs to the J-8 tool. Since both tools use the same repository, the validated documents are available in both the J-6 and J-8 tool. Recent changes to J6 JCPAT should alleviate confusion.

Page 17

9. Page 16, Recommendations, end of paragraph 1. Add: "We also recommend the implementation of a process which addresses, funds,

Final Report Reference

and implements aspects of joint battle management command and control interoperability and connectivity, validation and/or allocation of resources to acquire Joint systems and create offices supporting integration of materiel and non-materiel solutions for broad mission capability areas."

REASON: The IG report does not address the fundamental issue that the Department of Defense is not effectively structured to effect the "organizing, training, and equipping" of joint capabilities. There is no joint process responsible and accountable for developing and acquiring joint command and control systems and integrating capabilities.

10. Page 16, Recommendations, paragraph 2. Add the following subparagraphs: Page 18
"a. Develop Joint Mission Area Architectures based on currently available DOD assets and based on those assets needed to provide the capabilities for the future.
b. Provide an analysis branch within each JMA to assess Requirement Document relevance against known architecture needs.
c. Develop compliant, certified, and standard analysis and predictive tools, such as models or simulations, to assist in verifying the completeness of stated interoperability requirements in mission area architectures."

REASON: Completeness.

11. Page 16, Recommendations, paragraph 3. Comment: USJFCOM is currently required to only review ORDs as stand-alone documents for compliance with CRDs. The command does not possess the authority or resources to provide a more in-depth review of ORDs for interoperability with the respective family of systems. Page 21

12. Page 16, Recommendations, subparagraph 3a. Change as follows: Revised Page 21
"Compare all relevant ~~the operational~~ requirements documents of proposed DoD IT and NSS (to include SAP) systems within JMA architectures, as they are completed, against all other operational requirements documents in the related joint mission area architectures to verify the completeness of stated interoperability requirements."

REASON: Accuracy.

13. Page 16, Recommendations, paragraph 4. Change as follows: "We recommend that OASD, DISA, the Director, Command, Control, Communications, and Computer Systems Directorate (J-6), Office of the Chairman of the Joint Chiefs of Staff, and USJFCOM:". Revised Page 24

Final Report Reference

REASON: JCPAT access and archiving are functional responsibilities of DISA. JCPAT is also used by OSD. The recommendation should be addressed to all users, to include USJFCOM. JMA Architectures are the key to determining the utility of systems within the Department of Defense. As the warfighters advocate for interoperability and integration, USJFCOM should participate in the architecture process to insure warfighter needs and interests are met.

Revised Page 25

14. Page 16, Recommendations, subparagraph 4b. Change as follows: "In ~~conjunction with other~~ coordination between OASD, DISA and Joint Staff directorates, limit Joint Command, Control, Communications, Computers, and Intelligence Program Assessment Tool access to users who have a need to know."

REASON: JCPAT is a collaborative database used by at least four different executive directorates and agencies. (J-6/J-8/OASD/DISA). Since the J-6 tool is only one element of JCPAT, this statement should be directed to include all users.

Revised Page 50

15. Page 42, Appendix G. Change diagram as follows: Draw a line directly from JCPAT (a) to J-6 (b) and add a line between J-8 (a) and USJFCOM (d).

REASON: The diagram does not distinguish between ACAT I, JSI and ACAT II and below systems. The diagram also indicates that J-6 receives documents from J-8. This not true for ACAT II and below. ACAT II and below programs are staffed directly from JCPAT. Additionally, documents are forwarded to USJFCOM from both J-8 and J-6.

Interoperability Senior Review Panel Comments

OFFICE OF THE SECRETARY OF DEFENSE

1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

27 AUG 2002

MEMORANDUM FOR THE DOD INSPECTOR GENERAL

SUBJECT: DoD IG Audit Report on "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems (Project No. D2002AE-0009)"

The Interoperability Senior Review Panel (ISRP) has reviewed the subject report. The ISRP consists of senior leaders from the Office of the Under Secretary of Defense for Acquisition Technology and Logistics (OUSD (AT&L)), the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence (OASD (C3I)), the Joint Staff, Joint Forces Command, Office of the Director for Programs, Analysis and Evaluation (PA&E), and Director, Operational Test and Evaluation (DOT&E). Recognizing that the primary objective of the report was an evaluation of Defense and the Defense Agencies implementation of DoD interoperability and information assurance policies, the IG report does not address the fundamental issue that DoD is not currently structured to effect "organizing, training, and equipping" required joint capabilities. The Services determine requirements and resource those requirements based on individual Service vice Joint priorities. Further, IT and NSS interoperability and information assurance should be viewed in a wider context of Doctrine, Organization, Training, Materiel, Leadership Development, Personnel, and Facilities (DOTMLPF) instead of only system of system and/or family of systems. Viewed in this context joint interoperability requires a synchronized effort and resources across the entire DOTMLPF spectrum. The ISRP offers the following specific comments on the recommendations:

Recommendation 1. The ISRP concurs with this recommendation and will work with the Staff to implement a process for timely revision and synchronization of DoD policies regarding interoperability and information assurance. The ISRP membership will be used to coordinate the annual review, synchronization and revision, if required, for the following policies and implementing instructions impacting interoperability: DoDD 4630.5, DoDI 4630.8, CJCSI 3170.01, and CJCSI 6212.01. The ISRP will also coordinate with OUSD (AT&L), OASD (C3I), and the Joint Staff to ensure consistency of the above interoperability/requirements policies with the 5000 series policy documents for acquisition, and DoDI 5200.40 and CJCSI 6510.01 policies for information insurance.

Recommendation 2. The ISRP will continue to refine the process and procedures regarding implementation of the Interoperability Watch List. Our pilot case this past year was the Air Force Situational Awareness Data Link (SADL). SADL was based on a non-Joint Tactical Radio System compliant radio, using a non-standard air-to-air and air-to-ground tactical data link. The ISRP determined the interoperability issues were significant. The visibility the ISRP brought to the SADL allowed the existing OASD (C3I) JTRS Waiver process to proceed with the decision to disapprove the SADL request and have the Air Force design an interoperable

solution for its close air support aircraft. The ISRP continues to investigate other programs for the Interoperability Watch List and will work to find solutions within established processes of the Joint Staff, OUSD (AT&L), OASD (C3I), and DOT&E before placing a system on the List.

Recommendation 3. The ISRP concurs with the concept of the basic recommendation and recognizes the development of the Joint Mission Area Architectures is critical to compare requirements across programs. We will continue to press this need separately and collectively in all available forums. However, as drafted, the recommendation is not actionable by JFCOM without Joint Staff completion of the Joint Mission Area (JMAs) architectures. Further, the quantification analysis and predictive tools recommendation is also not fully actionable at this time. Although the software tools referenced in the report are under JFCOM assessment and show potential, it must be officially accredited by OSD and the JS for JFCOM to provide verification of joint interoperability requirements in mission area architectures.

Recommendation 4. The ISRP supports the position of the Joint Staff regarding this recommendation. The responsibility for JCPAT goes beyond the Joint Staff, so that the recommendation should be addressed to all departments, agencies, and directorates that either use or control access to JCPAT. Since many members of the ISRP benefit from JCPAT, the ISRP will look into the policy and guidance associated with JCPAT and make recommendations to appropriate organizations.

Recommendation 5. The ISRP agrees that testing of interoperability and information assurance takes on more critical status as we continue to develop and transform into a network centric force. The DOT&E currently tests interoperability to ensure the Key Performance Parameters within the Operational Requirements Documents are met, and has a policy for testing information assurance. The ISRP supports the development of necessary test capabilities to represent relevant aspects of the Global Information Grid that will allow programs to test in a system of systems environment. OUSD (AT&L), OASD (C3I), and DOT&E support expanded funding in the upcoming POM for the Joint Distributed Engineering Plant which will allow for a cost effective means to do this type of testing.

The ISRP point of contact is Ms Susan Wright, Executive Secretary, 703-681-1440 extension 115.

George G. Wauer
Co-Chair
Interoperability Senior Review Panel

Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Mary L. Ugone
John E. Meling
Jack D. Snider
Mark E. Stephens
Kevin W. Klein
Trisha L. Staley
Kelly R. Veith
Jacqueline N. Pugh